## CONTENTS

### 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
  - Determine the Scope of the Upgrade or Migration 15

### CHAPTER 4
- Requirements and Limitations 17
  - Requirements and Limitations 17
  - Hardware 18
  - Upgrade Considerations for Upgrades from 12.0(1) to 12.5(1) 18
  - Network Requirements 19
    - IP Address Requirements 19
Supported Upgrade and Migration Paths 33

Supported Versions 33

Supported Upgrade and Migration Paths 33

Applications Installed on Cisco Media Convergence Servers Hardware 34

Applications Installed on Virtual Machines 35

Deployment Types and Recommendations 37

Type of Deployment 37

Business Edition 6000 and Business Edition 7000 Deployments 37

Virtualized Deployments of Cisco Unified Communications Manager and IM and Presence Service 37
CHAPTER 7

Sequencing Rules and Time Requirements 39
  Upgrade Sequence and Time Requirements 39
  Recommended Sequence for the Least Time 39
  Recommended Sequence for the Least Impact 41
  Sequence Rules 44

Upgrade time requirements 45
  Factors that Affect Upgrade Time Requirements 45
  Estimating the Minimum Time Requirements 47

Examples 49
  Example: Time Requirements for a Standard Upgrade in the Least Time 49
  Example: Time Requirements for a Refresh Upgrade in the Least Time 50
  Example: Time Requirements for a Standard Upgrade with the Least Impact 51
  Example: Time Requirements for a Refresh Upgrade with the Least Impact 52

CHAPTER 8

Find all Required Upgrade Documentation 55
  Upgrade Documentation 55

PART III

Change the Virtualization Software 59

CHAPTER 9

Change the Virtualization Software 61
  Virtual Machine Configuration Tasks 61
    Install and Configure VMware vCenter 62
    Upgrade vSphere ESXi 63
    Download and Install OVA Templates 63
    Change Virtual Machine Configuration Specifications 64
    Migrate From Single to Multi-vDisk Virtual Machine 65

PART IV

Upgrade the Applications 67

CHAPTER 10

Pre-upgrade Tasks 69
  Pre-Upgrade Task Flow 69
  Generate a Database Status Report 75
  Check Database Replication 75
Before You Begin 98
Upgrade Task Flow 99
Upgrade the Applications 100
  Upgrade from a Local Source 101
  Upgrade from a Remote Source 104
  Upgrade from Local Filesystem 106
Version Switching 109
  Switch the Software Version 109
Cluster-Wide Reboot 110
  Switch to Previous Version 111
    Switch Cluster to Previous Version 111
    Switch Node to Previous Version 111
  Reset Database Replication 112
    Switch version back to Cisco Unified Presence 8.6(3) or earlier 112
Verify that Database Replication is Functioning 113
Verify that Database Replication is Complete 114
Upgrade Individual Cluster Nodes through CLI 114
Upgrade Cluster Through CLI 116

CHAPTER 12
Post-upgrade Tasks 119
Post-upgrade Task Flow 119
  Switch the Software Version 122
  Remove the Serial Port 123
  Restart Extension Mobility 123
  Restart TFTP Services 124
  Reset TFTP Parameters 124
  Restore Enterprise Parameters 124
  Reset High and Low Watermarks 125
  Updating VMware Tools 125
  Install Locales 126
  Restore the Database Replication Timeout 128
  Verify the Registered Device Count 128
  Verify Assigned Users 129
  Test Functionality 129
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade RTMT</td>
<td>130</td>
</tr>
<tr>
<td>Manage TFTP Server Files</td>
<td>131</td>
</tr>
<tr>
<td>Set Up a Custom Log-On Message</td>
<td>132</td>
</tr>
<tr>
<td>Configure IPSec Policies</td>
<td>132</td>
</tr>
<tr>
<td>Assign New Manager Assistant Roles</td>
<td>133</td>
</tr>
<tr>
<td>Verify IM and Presence Service Data Migration</td>
<td>133</td>
</tr>
<tr>
<td>Enable High Availability on Presence Redundancy Groups</td>
<td>134</td>
</tr>
<tr>
<td>Restart the IM and Presence Sync Agent</td>
<td>135</td>
</tr>
<tr>
<td>Restart CER Service</td>
<td>135</td>
</tr>
</tbody>
</table>

**PART V**

**Troubleshooting**

**CHAPTER 13**

**Troubleshooting**

- Dump a Log File After an Upgrade Failure                         139
- Troubleshooting Unified Communications Manager Upgrades          140
  - Upgrade Failure                                                140
  - Troubleshooting Simplified Upgrade Issues                      140
  - Upgrade Fails with Insufficient Disk Space                     142
  - Resuming a Failed Upgrade                                      143
  - Reduced Permissions for Access Control Groups                  143
  - Loss of Phone Settings                                          144
- Post-Upgrade Failure of Unified Communications Manager Publisher Node 144
- Post-Upgrade Failure of Unified Communications Manager Subscriber Nodes 144
- Troubleshooting IM and Presence Upgrades                         144
  - Upgrade Failure of IM and Presence Database Publisher Node      144
  - Upgrade Failure of IM and Presence Subscriber Node              145
  - Upgrade From Pre Release 8.6(4) Fails                          145
  - IM and Presence user phone presence problems                    146
  - Presence User Experiences Issues Obtaining Availability        146
  - Real-Time Monitoring Tool alert for Cisco SIP proxy service     146
  - Cannot find upgrade file on remote server                      146
  - Upgrade file checksum values do not match                      146
  - Database replication did not complete                           147
  - Cisco UP Presence Engine database does not restart              147
Version Errors 147
Failed refresh upgrade 148
Cancelled or failed upgrade 148
Directory Was Located and Searched but No Valid Options or Upgrades Were Available 148
Common Partition Full Upgrade Failure 149

PART VI

Appendix 151

CHAPTER 14
Frequently Asked Questions 153
Frequently Asked Questions 153

CHAPTER 15
Upgrading from Legacy Releases 157
Upgrading and Migrating from Legacy Releases 157

CHAPTER 16
Additional Upgrade Resources 159
Additional Upgrade Resources 159
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 IM and Presence Service. The table below outlines how to use this guide to plan and then perform an upgrade or migration.

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></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 59**  
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 67**  
Use the information in this section when you are ready to begin to upgrade or migrate the Unified Communications Manager and the IM and Presence applications.

• Complete the pre-upgrade tasks in this section that are identified for the type or upgrade or migration that you are doing.

• After you complete the pre-upgrade tasks, perform the upgrade or migration using the method and the documentation that you identified during the planning stage. For example, if you are performing a direct upgrade using the Cisco Unified CM OS Admin interface, follow the procedures in this guide. If you are performing a direct upgrade or a migration using Cisco Prime Collaboration Deployment (PCD), follow the procedures in the PCD documentation.

• Complete the post-upgrade tasks in this section for all upgrade and migration methods.

**Step 5**  
**Troubleshooting, on page 137**  
Use the information in this section to troubleshoot problems that occur during the upgrade process.

**Step 6**  
**Appendix, on page 151**  
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
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 IM and Presence Service 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 IM 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.
Once upgraded to 12.5 release or upgrade attempt to 12.5 release fails, if for any reason you decide to revert to prior software version, you can switch version to the older version of the software. After that, you cannot upgrade to any pre 12.5 (for example, 11.5(1), and 12.0(1)) releases. If the administrator really wants to upgrade to pre 12.5 version, PCD migration or cluster rebuild is necessary.

### Migrations

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

- your currently installed version is running on Cisco 7800 Series Media Convergence Server (MCS 7800) hardware and you are upgrading to release that will run on a virtual machine.
- your currently installed version is running on a virtual machine and you need to move to a new virtual machine.
- you are upgrading to 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 IM 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.
- **Command Line Interface (CLI)**:
  
  You can use the `utils system upgrade initiate` command under the admin CLI to initiate a direct upgrade.

### Export Restricted and Export Unrestricted Software

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

Unrestricted versions of software are intended only for a very specific set of customers who do not want various security capabilities; unrestricted versions are not intended for general deployments.
Export unrestricted versions differs from restricted versions as follows:

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

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

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

The following table describes the GUI items that are not available for the export unrestricted version of IM and Presence.

<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>This menu and its options are not available.</td>
</tr>
<tr>
<td>VPN Configuration</td>
<td>Advanced Features &gt; VPN</td>
<td>The Device Security Mode is set to Non Secure and is not configurable.</td>
</tr>
<tr>
<td>Phone Security Profile Configuration</td>
<td>System &gt; Security &gt; Phone Security Profile</td>
<td></td>
</tr>
<tr>
<td>Cisco Unified CM IM and Presence Administration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GUI Item</td>
<td>Location</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security Settings</td>
<td>System &gt; Security &gt; Settings</td>
<td>• You cannot check the <strong>Enable XMPP Client to IM/P Service Secure Mode</strong> setting.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• You cannot check the <strong>Enable XMPP Router-to-Router Secure Mode</strong> setting.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• You cannot check the <strong>Enable Web Client to IM/P Service Secure Mode</strong> setting.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The option to set <strong>SIP intra-cluster Proxy-to-Proxy Transport Protocol</strong> to TLS has been removed.</td>
</tr>
<tr>
<td>Service Parameter Configuration</td>
<td>System &gt; Service Parameters and choose Cisco SIP Proxy as the Service</td>
<td>• All TLS options have been removed for the <strong>Transport Preferred Order</strong> parameter.</td>
</tr>
<tr>
<td>for Cisco SIP Proxy service</td>
<td></td>
<td>• The TLS option has been removed from the <strong>SIP Route Header Transport Type</strong> parameter.</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 <strong>NO TLS</strong>.</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 33
- Deployment Types and Recommendations, on page 37
- Sequencing Rules and Time Requirements, on page 39
- Find all Required Upgrade Documentation, on page 55
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>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | Determine whether you need to update the following components:  
- Hardware, on page 18  
- Virtual Machine Configuration, on page 20 | Ensure that your system meets the requirements of the new release. |
| Step 2 | Verify the Supported Upgrade and Migration Paths, on page 33. | 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 37 | 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 39 | 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 | 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.

**Step 5** Find Upgrade Documentation, on page 55. | 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 IM and Presence Service.

Caution

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

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

Note

- By default, your system is in non-FIPS mode, you must enable it.
- Before you upgrade to FIPS, Common Criteria, or Enhanced Security mode on the cluster, ensure that the security password length is minimum of 14 characters and it needs to be updated even if the prior version was FIPS enabled.
Unified Communications Manager 12.5 requires minimum ESXi version of 6.5 U2 with minimum VM Hardware version of 13. For latest Unified Communications Manager ESXi version support, see http://www.cisco.com/go/virtualized-collaboration.

Note

The Simplified Upgrade (Cluster upgrade, reboot, and switch version) feature is supported only in Unified Communications Manager version 12.5 and higher.

Hardware

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

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

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

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

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

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

Note

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

Refresh upgrade from Unified Communications Manager 12.0.1. to 12.5 or from Unified Communications Manager previous release upgrade to 12.5 release:
Before you proceed with refresh upgrade, ensure that your system has sufficient free disk space. Perform the following steps to create free disk space:

- Install “ciscocm.free_common_space_<latest_version>.cop” on Unified Communications Manager Publisher and all Subscriber (including TFTP server) nodes.

- Delete the unused phone loads on the Unified Communications Manager TFTP subscriber nodes.

Network Requirements

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

IP Address Requirements

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

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

DNS requirements

Note the following requirements:

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

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

- If your deployment does not use DNS, will need to edit the following Host Name/IP Address fields:
  - Server—In the Cisco Unified CM Administration Server Configuration window, set IP addresses for your cluster nodes.
  - IM and Presence UC Service—In the Cisco Unified CM Administration UC Service Configuration window, create an IM and Presence UC service that points to the IP address of the IM and Presence database publisher node
  - CCMCIP Profiles—In the Cisco Unified CM IM and Presence Administration CCMCIP Profile Configuration window, point any CCMCIP profiles to the IP address of the host.
Multinode considerations—If you are using the multinode feature in IM and Presence, 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 Cisco Unified Communications versions, refer to the following URL:

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

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

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

You can find detailed information about the requirements for the virtualized environment by going to https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-sizing.html, where you can:

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

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

Table 2: Supported Browsers and Operating Systems

<table>
<thead>
<tr>
<th>You can use this browser...</th>
<th>...with one of these operating systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Chrome (latest browser version)</td>
<td>Microsoft Windows 10 (64 bit)</td>
</tr>
</tbody>
</table>
| Microsoft Internet Explorer 11 | • Microsoft Windows 10 (64 bit)  
   • Microsoft Windows 8.1 (64 bit)  
   • Microsoft Windows 7 (64 bit) |
| Microsoft Edge | Microsoft Windows 10 (32 bit/64 bit) |
| Mozilla Firefox (latest browser version) | Microsoft Windows 10 (64 bit) |
| Safari | Apple Mac OS 10.x (or newest OS release available) |

Licensing

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

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

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

- Direct—Unified Communications Manager sends usage information directly over the internet. No additional components are needed.

- Cisco Smart Software Manager satellite—Unified Communications Manager sends usage information to an on-premise Smart Software Manager. Periodically, an exchange of information is performed to keep the databases in synchronization. For more information on installation or configuration of the Smart Software Manager satellite, go to this URL: [www.cisco.com/go/smartsatellite](http://www.cisco.com/go/smartsatellite).

Note

Cisco Smart Software Manager satellite is an on-premises collector similar to standalone Prime License Manager.
• Proxy Server—Unified Communications Manager sends usage information over the internet through a proxy server.

Cisco Unified Communications Manager License Requirements

Cisco Smart Software Licensing is a new way of thinking about licensing. It adds flexibility to your licensing and simplifies it across the enterprise. It also delivers visibility into your license ownership and consumption.

Cisco Smart Software Licensing helps you to procure, deploy, and manage licenses easily where devices self-register and report license consumption, removing the need for product activation keys (PAK). It pools license entitlements in a single account and allows you to move licenses freely through the network, wherever you need them. It is enabled across Cisco products and managed by a direct cloud-based or mediated deployment model.

The Cisco Smart Software Licensing service registers the product instance, reports license usage, and obtains the necessary authorization from Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

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

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

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

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

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


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

Migration of PLM Licenses to Smart Entitlement

If you are eligible to upgrade to the Smart Licensing version of the product, then you are able to initiate the migration through the License Registration Portal or Cisco Smart Software Manager. You can self-initiate this process by downloading and installing the Smart Licensing version of the software and registering the device to a Smart Account using a Registration Token. The migration of any entitlements tracked by Cisco automatically migrates to the Customers Smart Account. You will also be able to initiate the migration of unused classic PAKs to Smart Accounts for future consumption by products in Smart Mode. This process is available through the License Registration Portal or Cisco Smart Software Manager.
Unified Communications Manager 9.0x and later version of 12.0(1)

- If you are holding an active Cisco Software Support Service (SWSS) contract, then you can convert the classic licenses to smart entitlements through the Cisco Smart Software Manager at https://software.cisco.com/#SmartLicensing-LicenseConversion.

- Two types of Migration are supported:
  - PAK based—Supported for already fulfilled, partially fulfilled and unfulfilled PAKs
  - Device based

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

Upgrade to Smart Entitlement

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

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


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

Specific License Reservation

Specific License Reservation (SLR) allows the customer to reserve licenses from their virtual account, tie them to a device's UDI and use their device with these reserved licenses in a disconnected mode. The customer reserves specific licenses and counts for a UDI from their virtual account. The following options describe the new functionality and design elements for Specific Reservation.

Table 3: Specific License Reservation Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>license smart reservation enable</td>
<td>Use this command to enable the license reservation feature.</td>
</tr>
<tr>
<td>license smart reservation disable</td>
<td>Use this command to disable the license reservation feature.</td>
</tr>
<tr>
<td>license smart reservation request</td>
<td>Use this command to generate reservation request code.</td>
</tr>
<tr>
<td>license smart reservation cancel</td>
<td>Use this command to cancel the reservation process before the authorization code is installed.</td>
</tr>
<tr>
<td>license smart reservation install &quot;&lt;authorization-code&gt;&quot;</td>
<td>Use this command to install the license reservation authorization-code generated on the Cisco Smart Software Manager.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>license smart reservation return</td>
<td>Use this command to remove the license reservation authorization code that is installed and list of reserved entitlements. The device transitions back to an unregistered state.</td>
</tr>
<tr>
<td>license smart reservation return-authorization &quot;&lt;authorization code&gt;&quot;</td>
<td>Use this command to remove the license reservation authorization code that is entered by the user.</td>
</tr>
</tbody>
</table>

Note If you are upgrading from 12.0 to higher versions and enable license reservation feature on upgraded server, you should download `ciscocm-ucm-resetudi.k3.cop.sgn` from CCO and install on the upgraded CUCM before enabling reservation feature.

**IM and Presence license requirements**

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

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

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

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

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

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

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

This section describes the limitations that apply when you install or upgrade Unified Communications Manager or the IM 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 IM and Presence nodes in a cluster is 6.

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

IP Subnet Mask

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

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

Support for Intercluster Peers

The IM and Presence Service supports intercluster peers to clusters that are running different software versions. To find the interdomain federations that are supported, see the "Supported Integrations" chapter in the Compatibility Matrix for Cisco Unified Communications Manager and IM and Presence Service for your release, at http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-device-support-tables-list.html.

Device Name for Cisco Unified Mobile Communicator

Ensure that the device name for the Cisco Unified Mobile Communicator device contains 15 or fewer characters. If the device name contains more than 15 characters for the Cisco Unified Mobile Communicator, the device does not migrate during the upgrade.
Upgrade from Unified Communications Manager version 9.x to higher version

Upgrade from Unified Communications Manager version 9.x to version 10.x or higher fails if you have a SIP Profile with any of the following names on version 9.x:

- Standard SIP Profile
- Standard SIP Profile For Cisco VCS
- Standard SIP Profile For TelePresence Conferencing
- Standard SIP Profile For TelePresence Endpoint
- Standard SIP Profile for Mobile Device

If you have a SIP Profile with any of these names, you need to rename or delete it before proceeding with the upgrade.

Deprecated Phone Models

As of Cisco Unified Communications Manager Firmware Release 14.0, the following phones are not supported:

- Cisco Unified SIP Phone 3911
- Cisco Unified SIP Phone 3951
- Cisco Unified IP Phone 6911
- Cisco Unified IP Phone 6921
- Cisco Unified IP Phone 6941
- Cisco Unified IP Phone 6945
- Cisco Unified IP Phone 6961
- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified Wireless IP Phone 7925G
- Cisco Unified Wireless IP Phone 7925G-EX
- Cisco Unified Wireless IP Phone 7926G
- Cisco Unified IP Phone 7931
- Cisco Unified IP Conference Station 7936
- Cisco Unified IP Conference Station 7937
- Cisco Unified IP Phone 7940
- Cisco Unified IP Phone 7941
- Cisco Unified IP Phone 7960
- Cisco Unified IP Phone 7961
For Cisco Unified Communications Manager Firmware Release 12.5, no additional phones are deprecated. As of Cisco Unified Communications Manager Firmware Release 12.0, the following phones are not supported:

- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified Wireless IP Phone 7921G

As of Cisco Unified Communications Manager Firmware Release 11.5, the following phones are not supported:

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

The above deprecated phones continue to be supported on older releases of Unified Communications Manager. However, when you upgrade to a Unified Communications Manager release that doesn't support the deprecated phones, the phones won't work after the upgrade completes.


### Upgrades that Involve Deprecated Phones

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

1. Confirm whether the phones in your network will be supported in this release.
2. Identify any non-supported phones.
3. For any non-supported phones, power down the phone and disconnect the phone from the network.
4. Provision a supported phone for the phone user. You can use the Migration FX tool to migrate from older model to newer model phones. For details, go to: [https://www.unifiedfx.com/products/unifiedfx-migrationfx#endpoint_refresh_tool](https://www.unifiedfx.com/products/unifiedfx-migrationfx#endpoint_refresh_tool).
5. Once all the phones in your network are supported by this release, upgrade your system.
Deprecation phones can also be removed after the upgrade. When the administrator logs in to Unified Communications Manager after completing the upgrade, the system displays a warning message notifying the administrator of the deprecated phones.

**Licensing**

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

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

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

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

**Upgrades from 11.5(1)SU2 with Push Notifications Enabled**

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

After you upgrade your system, do the following:

**Procedure**

**Step 1**

Disable Push Notifications

Follow these steps:

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

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


**Step 3**
Enable Push Notifications for this release.


---

**Database Migration Required for Upgrades with Microsoft SQL Server**

If you have Microsoft SQL Server deployed as an external database with the IM and Presence Service and you are upgrading from 11.5(1), 11.5(1)SU1, or 11.5(1)SU2, you must create a new SQL Server database and migrate to the new database. This is required due to enhanced data type support in this release. If you don't migrate your database, schema verification failure will occur on the existing SQL Server database and services that rely on the external database, such as persistent chat, will not start.

After you upgrade your IM and Presence Service, use this procedure to create a new SQL Server database and migrate data to the new database.

**Note**
This migration is not required for Oracle or PostgreSQL external databases.

**Before You Begin**

The database migration is dependent on the `MSSQL_migrate_script.sql` script. Contact Cisco TAC to obtain a copy.

**Table 4:**

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Create a snapshot of your external Microsoft SQL Server database.</td>
</tr>
</tbody>
</table>
| Step 2 | Create a new (empty) SQL Server database. For details, see the following chapters in the *Database Setup Guide for the IM and Presence Service:*  
  1. "Microsoft SQL Installation and Setup"—Refer to this chapter for details on how to create your new SQL server database on your upgraded IM and Presence Service.  
  2. "IM and Presence Service External Database Setup"—After your new database is created, refer to this chapter to add the database as an external database in the IM and Presence Service. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
</table>
| Step 3 | Run the System Troubleshooter to confirm that there are no errors with the new database.  
1. From Cisco Unified CM IM and Presence Administration, choose **Diagnostics > System Troubleshooter**.  
2. Verify that no errors appear in the **External Database Troubleshooter** section. |
| Step 4 | Restart the Cisco XCP Router on all IM and Presence Service cluster nodes:  
1. From Cisco Unified IM and Presence Serviceability, choose **Tools > Control Center - Network Services**.  
2. From the **Server** menu, select an IM and Presence Service node and click **Go**.  
3. Under **IM and Presence Services**, select **Cisco XCP Router** and click **Restart**. |
| Step 5 | Turn off services that depend on the external database:  
1. From Cisco Unified IM and Presence Serviceability, choose **Tools > Control Center - Feature Services**.  
2. From the **Server** menu, select an IM and Presence node and click **Go**.  
3. Under **IM and Presence Services**, select the following services:.  
   - Cisco XCP Text Conference Manager  
   - Cisco XCP File Transfer Manager  
   - Cisco XCP Message Archiver  
4. Click **Stop**. |
| Step 6 | Run the following script to migrate data from the old database to the new database **MSSQL_migrate_script.sql**.  
**Note** Contact Cisco TAC to obtain a copy of this script |
| Step 7 | Run the System Troubleshooter to confirm that there are no errors with the new database.  
1. From Cisco Unified CM IM and Presence Administration, choose **Diagnostics > System Troubleshooter**.  
2. Verify that no errors appear in the **External Database Troubleshooter** section. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
</table>
| Step 8 | Start the services that you stopped previously.  
1. From Cisco Unified IM and Presence Serviceability, choose **Tools > Control Center - Feature Services**.  
2. From the **Server** menu, select an IM and Presence node and click **Go**.  
3. Under **IM and Presence Services**, select the following services:  
   - Cisco XCP Text Conference Manager  
   - Cisco XCP File Transfer Manager  
   - Cisco XCP Message Archiver  
4. Click **Start**. |
| Step 9 | Confirm that the external database is running and that all chat rooms are visible from a Cisco Jabber client. Delete the old database only after you're confident that the new database is working. |

### Migrations from 12.0(1) via Prime Collaboration Deployment

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

ciscocm-slm-migration.k3.cop.sgn


---

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

---

### FIPS Mode Not Supported in 12.x

Releases 12.0(1) and 12.5(1) of Cisco Unified Communications Manager and the IM and Presence Service do not support FIPS mode. If you are upgrading from an earlier release with FIPS mode, Enhanced Security Mode, or Common Criteria Mode enabled, you must disable them prior to the upgrade. TFTP and other services will not work in 12.0(1) or 12.5(1) with FIPS mode enabled.
Supported Upgrade and Migration Paths

- Supported Versions, on page 33
- Supported Upgrade and Migration Paths, on page 33

**Supported Versions**

The following software versions apply to Release 12.5(1):

- Unified Communications Manager 12.5.1.10000-22
- IM and Presence Service 12.5.1.10000-22

**Version Mismatches**

This release offers two main deployment options for this release of Unified Communications Manager and the IM and Presence Service:

- Standard Deployments—Both Unified Communications Manager and the IM and Presence Service must be running the above 12.5.1.10000-22 version for your deployment to be supported. A version mismatch is not supported.

- Centralized Deployments of IM and Presence Service—If you have the Centralized Deployment option configured on the IM and Presence Service, then within the IM and Presence central cluster, both the Unified Communications Manager instance and the IM and Presence Service must be running a 12.5.1.10000-22 version. However, the telephony cluster that the central cluster connects to does not have to be running a 12.5.1.10000-22 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
Cisco Unified CM OS Admin upgrades can be initiated through the OS Admin user interface or through the admin CLI command.

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*. 

### Applications Installed on Cisco Media Convergence Servers Hardware

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

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

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 5: 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>12.5(x)</td>
<td>PCD Migration</td>
</tr>
<tr>
<td>7.1(3) and 7.1(5)</td>
<td>12.5(x)</td>
<td>PCD Migration</td>
</tr>
<tr>
<td>8.x</td>
<td>12.5(x)</td>
<td>PCD Migration</td>
</tr>
<tr>
<td>9.x</td>
<td>12.5(x)</td>
<td>PCD Migration</td>
</tr>
</tbody>
</table>

#### Table 6: 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>12.5(x)</td>
<td>PCD Migration</td>
</tr>
<tr>
<td>CUP 8.6(3), 8.6(4), and 8.6(5)</td>
<td>12.5(x)</td>
<td>PCD Migration</td>
</tr>
<tr>
<td>IM and Presence 9.x</td>
<td>12.5(x)</td>
<td>PCD Migration</td>
</tr>
</tbody>
</table>
Applications Installed on Virtual Machines

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

**Table 7: Unified Communications Manager Releases Installed on Virtual Machines**

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Supported Methods</th>
<th>Version Switching (From Source To Destination and vice versa)</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.6(x)</td>
<td>12.5(x)</td>
<td>PCD Migration</td>
<td>Not supported</td>
</tr>
<tr>
<td>9.0(x)</td>
<td>12.5(x)</td>
<td>PCD Migration</td>
<td>Not supported</td>
</tr>
<tr>
<td>9.1(x)</td>
<td>12.5(x)</td>
<td>PCD Migration</td>
<td>Not supported</td>
</tr>
<tr>
<td>10.0(x)</td>
<td>12.5(x)</td>
<td>PCD Migration</td>
<td>Not supported</td>
</tr>
<tr>
<td>10.5(x)</td>
<td>12.5(x)</td>
<td>PCD Migration, PCD Upgrade (Direct Refresh), Cisco Unified OS Admin (Direct Refresh)</td>
<td>Supported</td>
</tr>
<tr>
<td>11.x</td>
<td>12.5(x)</td>
<td>PCD Migration, PCD Upgrade (Direct Refresh), Cisco Unified OS Admin (Direct Refresh)</td>
<td>Supported</td>
</tr>
<tr>
<td>12.0(x)</td>
<td>12.5(x)</td>
<td>PCD Migration, PCD Upgrade (Direct Refresh), Cisco Unified OS Admin (Direct Refresh)</td>
<td>Supported</td>
</tr>
<tr>
<td>12.5(x)</td>
<td>12.5(x)</td>
<td>Direct Standard (L2 upgrade)</td>
<td>Supported</td>
</tr>
</tbody>
</table>

**Table 8: Cisco Unified Presence and IM and Presence Releases Installed on Virtual Machines**

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Supported Methods</th>
<th>Version Switching (From Source To Destination and vice versa)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CUP 8.5(4)</td>
<td>12.5(x)</td>
<td>PCD Migration</td>
<td>Not supported</td>
</tr>
<tr>
<td>CUP 8.6(3), 8.6(4), and 8.6(5)</td>
<td>12.5(x)</td>
<td>PCD Migration</td>
<td>Not supported</td>
</tr>
<tr>
<td>CUP 8.6(x)</td>
<td>12.5(x)</td>
<td>PCD Migration</td>
<td>Not supported</td>
</tr>
<tr>
<td>From</td>
<td>To</td>
<td>Supported Methods</td>
<td>Version Switching (From Source To Destination and vice versa)</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------</td>
<td>-------------------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>IM and Presence 9.0(x)</td>
<td>12.5(x)</td>
<td>PCD Migration</td>
<td>Not supported</td>
</tr>
<tr>
<td>IM and Presence 9.1(x)</td>
<td>12.5(x)</td>
<td>PCD Migration</td>
<td>Not supported</td>
</tr>
<tr>
<td>IM and Presence 10.0(x)</td>
<td>12.5(x)</td>
<td>PCD Migration</td>
<td>Not supported</td>
</tr>
<tr>
<td>IM and Presence 10.5(x)</td>
<td>12.5(x)</td>
<td>PCD Migration</td>
<td>Not supported</td>
</tr>
<tr>
<td>IM and Presence 10.5(x)</td>
<td>12.5(x)</td>
<td>PCD Migration</td>
<td>Not supported</td>
</tr>
<tr>
<td>IM and Presence 11.0(1)</td>
<td>12.5(x)</td>
<td>PCD Migration</td>
<td>Supported</td>
</tr>
<tr>
<td>IM and Presence 11.5(x)</td>
<td>12.5(x)</td>
<td>PCD Migration</td>
<td>Supported</td>
</tr>
<tr>
<td>IM and Presence 12.0(x)</td>
<td>12.5(x)</td>
<td>PCD Migration</td>
<td>Supported</td>
</tr>
<tr>
<td>IM and Presence 12.5(x)</td>
<td>12.5(y)</td>
<td>Direct Standard (L2 upgrade)</td>
<td>Supported</td>
</tr>
</tbody>
</table>
Deployment Types and Recommendations

- Type of Deployment, on page 37

Type of Deployment

Use the information in this section after you have reviewed the tables in the Supported Upgrade and Migration Paths, on page 33 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 IM and Presence Service, such as Cisco Unity Connection and/or Cisco Unified Contact Center Express, you can use the PCD upgrade task to automate the process.

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

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

Consider performing a PCD migration when:
- you need old and new systems up in parallel.
- you want to change virtual machine configurations in Release 11.5(1) but the change forces a reinstall.

Consider performing a PCD upgrade when:
- you have large number of virtual machines and a complex upgrade sequence or a need to forward-schedule.
- you need to upgrade other applications, such as Cisco Unity Connection or Cisco Unified Contact Center Express.
CHAPTER 7

Sequencing Rules and Time Requirements

• Upgrade Sequence and Time Requirements, on page 39
• Upgrade time requirements, on page 45

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 39
• Recommended Sequence for the Least Impact, on page 41

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 44

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 IM 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 IM and Presence Service nodes, you must reboot all IM and Presence nodes after the Unified Communications Manager upgrade is complete.

**Refresh Upgrades**

Use the table below to plan a refresh upgrade when your priority is to perform the upgrade in the least amount of time. If you are unsure whether you need to perform a refresh upgrade or a standard upgrade, review the information in Direct Upgrades, on page 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 IM 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 IM 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 IM 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 IM and Presence Service 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" in the *System Configuration Guide for Unified Communications Manager* at [http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html](http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html).

**Refresh Upgrades**

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

**Table 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 IM 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>
</tbody>
</table>
8. Ensure that database replication is complete and functioning between the publisher node and all primary subscriber nodes.

9. Switch the software version on the database publisher node and reboot it. The new software is active.

10. Switch the software version on the subscriber nodes in parallel and reboot them. The new software is active.

11. Ensure that database replication is complete and functioning between the publisher node and all subscriber nodes.

**Standard Upgrades**

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

**Table 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 IM 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>
</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 IM and Presence Service nodes, you must reboot all IM and Presence nodes after the Unified Communications Manager upgrade is complete.

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

• If you are upgrading IM and Presence nodes to a Maintenance Release (MR) or an Engineering Special (ES) Release and you are not upgrading Unified Communications Manager nodes, the following additional sequencing rules apply:
  • For upgrades using the Unified CM OS Admin interface, you must upgrade the Unified Communications Manager publisher node and then upgrade the IM and Presence nodes to the Maintenance Release (MR) or an Engineering Special (ES) Release.
  • If you are using the Prime Collaboration Deployment migration task, you must select the Unified Communications Manager publisher node in addition to the IM and Presence nodes.
  • If you are using the Prime Collaboration Deployment upgrade task, you do not need to select the Unified Communications Manager publisher node as long as the first 3 digits of new version of IM and Presence 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.  
**Note** To avoid upgrade failures due to time sync issues with VM, disable the VM's NTP sync with the ESXi host using the workaround mentioned in the following link:  
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessibility of upgrade images</td>
<td>Save time by ensuring that ISO images are on DVD, or are already downloaded and staged on the same LAN as the Unified Communications Manager and IM and Presence Service virtual machines (VM).</td>
</tr>
<tr>
<td>System health</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>System health</td>
<td>Low memory or memory leaks will impact the upgrade.</td>
</tr>
<tr>
<td>System health</td>
<td>Round Trip Times (RTT) between nodes will extend the time required.</td>
</tr>
<tr>
<td>System health</td>
<td>Ensure that there are no OutOfSynch (OOS) tables in the database.</td>
</tr>
<tr>
<td>System health</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>System health</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>Physical and virtual hardware infrastructure</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>Physical and virtual hardware infrastructure</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>Physical and virtual hardware infrastructure</td>
<td>• Storage latencies meet the requirements specified at <a href="http://www.cisco.com/go/virtualized-collaboration">www.cisco.com/go/virtualized-collaboration</a>.</td>
</tr>
<tr>
<td>Physical and virtual hardware infrastructure</td>
<td>• The physical CPU cores and the virtualization design comply with virtualization requirements of Unified Communications Manager and IM and Presence Service. Do not oversubscribe CPUs by having VMs share the host resources; use logical cores or resource reservations</td>
</tr>
<tr>
<td>Physical and virtual hardware infrastructure</td>
<td>• Unified Communications Manager and IM and Presence Service virtual machines are on same hosts, or on hosts with 1GbE LAN between them with low contention from other traffic.</td>
</tr>
<tr>
<td>Physical and virtual hardware infrastructure</td>
<td>• If the cluster is over a WAN, ensure that you follow all bandwidth and latency rules listed in the Cisco Collaboration Systems Solution Reference Network Designs (SRND) for at <a href="http://www.cisco.com/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html">http://www.cisco.com/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html</a>.</td>
</tr>
</tbody>
</table>
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.

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

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

<table>
<thead>
<tr>
<th>Table 14: Minimum Time Required for Upgrade Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Task</strong></td>
</tr>
<tr>
<td>Upgrade the Unified Communications Manager publisher node to an inactive version</td>
</tr>
<tr>
<td>Upgrade the Unified Communications Manager subscriber nodes to an inactive version</td>
</tr>
<tr>
<td>Switch the Unified Communications Manager publisher node to the new software version and reboot</td>
</tr>
<tr>
<td>Task</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td>Switch the Unified Communications Manager subscriber nodes to the</td>
</tr>
<tr>
<td>new software version and reboot</td>
</tr>
<tr>
<td>Unified Communications Manager database replication</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Note</td>
</tr>
<tr>
<td>Upgrade the IM and Presence database publisher node to an inactive</td>
</tr>
<tr>
<td>version</td>
</tr>
<tr>
<td>Upgrade the IM and Presence subscriber nodes to an inactive version</td>
</tr>
<tr>
<td>Switch the IM and Presence publisher node to the new software version</td>
</tr>
<tr>
<td>and reboot</td>
</tr>
<tr>
<td>Switch the IM and Presence subscriber nodes to the new software</td>
</tr>
<tr>
<td>version and reboot</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 IM and Presence nodes
- 75,000 users
- a system that is healthy and that has been optimized for the upgrade, as described in Factors that Affect Upgrade Time Requirements, on page 45

#### 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>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>2-4 hours</td>
</tr>
<tr>
<td>2 In parallel:</td>
<td></td>
</tr>
<tr>
<td>• Upgrade the Unified Communications Manager subscriber nodes. The new software is inactive.</td>
<td>2-3 hours</td>
</tr>
<tr>
<td>• Upgrade the IM and Presence database publisher node.</td>
<td></td>
</tr>
<tr>
<td>3 Upgrade the IM and Presence subscriber nodes. The new software is inactive.</td>
<td>1-2 hours</td>
</tr>
<tr>
<td>4 Switch the software version on the Unified Communications Manager publisher node and reboot it.</td>
<td>30 minutes</td>
</tr>
</tbody>
</table>

---

### Service Impact

<table>
<thead>
<tr>
<th>IM and Presence database replication</th>
<th>Minimum Time</th>
<th>Service Impact</th>
</tr>
</thead>
<tbody>
<tr>
<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>
<td></td>
</tr>
</tbody>
</table>

**Note**

WAN latency of 80ms or more can significantly lengthen these times.
### 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 IM and Presence database publisher node to the new software version. The new software is inactive.</td>
</tr>
<tr>
<td>4</td>
<td>Upgrade the IM 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>
</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>
<tr>
<td>2</td>
<td>In parallel:</td>
</tr>
<tr>
<td></td>
<td>• Upgrade all of the Unified Communications Manager subscriber nodes. The new software is inactive.</td>
</tr>
<tr>
<td></td>
<td>• Upgrade the IM and Presence database publisher node.</td>
</tr>
<tr>
<td>3</td>
<td>Upgrade the IM and Presence subscriber nodes in parallel. The new software is inactive.</td>
</tr>
<tr>
<td>4</td>
<td>Switch the software version on the Unified Communications Manager publisher node and reboot it.</td>
</tr>
<tr>
<td>5</td>
<td>In parallel:</td>
</tr>
<tr>
<td></td>
<td>• Switch the software version on the Unified Communications Manager secondary subscriber nodes and reboot them.</td>
</tr>
<tr>
<td></td>
<td>• Switch the software version on the IM and Presence database publisher node and reboot it.</td>
</tr>
<tr>
<td>Task</td>
<td>Minimum Estimated Time</td>
</tr>
<tr>
<td>------</td>
<td>------------------------</td>
</tr>
<tr>
<td>6</td>
<td>2 hours In parallel:</td>
</tr>
<tr>
<td></td>
<td>• Wait for database replication on the Unified Communications Manager secondary subscriber nodes.</td>
</tr>
<tr>
<td></td>
<td>• Switch the software version on the IM and Presence subscriber nodes in parallel and reboot them.</td>
</tr>
<tr>
<td>7</td>
<td>2 hours In parallel:</td>
</tr>
<tr>
<td></td>
<td>• Wait for database replication on the IM and Presence subscriber nodes.</td>
</tr>
<tr>
<td></td>
<td>Switch the software version on the Unified Communications Manager primary subscriber nodes and reboot them.</td>
</tr>
<tr>
<td>8</td>
<td>2 hours Wait for database replication on the Unified Communications Manager primary subscriber nodes.</td>
</tr>
<tr>
<td>Total</td>
<td>12-15 hours</td>
</tr>
</tbody>
</table>

### 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>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
</tbody>
</table>
### 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>5</td>
<td>Switch the software version on the Unified Communications Manager secondary subscriber nodes and reboot them.</td>
</tr>
<tr>
<td>6</td>
<td>Wait for database replication on the Unified Communications Manager secondary subscriber nodes.</td>
</tr>
<tr>
<td>7</td>
<td>Switch the software version on the Unified Communications Manager primary subscriber nodes and reboot them.</td>
</tr>
<tr>
<td>8</td>
<td>Wait for database replication on the Unified Communications Manager primary subscriber nodes.</td>
</tr>
<tr>
<td>9</td>
<td>Switch the software version on the IM and Presence database publisher node and reboot it.</td>
</tr>
<tr>
<td>10</td>
<td>Switch the software version on the IM and Presence subscriber nodes in parallel and reboot them.</td>
</tr>
<tr>
<td>11</td>
<td>Wait for database replication on the IM and Presence subscriber nodes.</td>
</tr>
</tbody>
</table>

**Total** | 16-20 hours |
## 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><strong>Prepare the hardware platform</strong></td>
<td></td>
</tr>
<tr>
<td>Install new virtualized 3rd-party specs-based server or Cisco UCS specs-based server</td>
<td>See the documentation from the server vendor and from VMware. See application support information at <a href="http://www.cisco.com/go/virtualized-collaboration">www.cisco.com go virtualized-collaboration</a> Information about specs-based support is available by searching on the topic &quot;UC Virtualization Supported Hardware&quot; at <a href="http://www.cisco.com/go/virtualized-collaboration">www.cisco.com go virtualized-collaboration</a></td>
</tr>
</tbody>
</table>
### Task | See . . .
---|---
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

| Activity | See . . . |
---|---|


Edit the virtual machine configuration | Vendor documentation at [http://www.VMware.com](http://www.VMware.com)


---

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

| Activity | See . . . |
---|---|


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

Change the Virtualization Software

• Change the Virtualization Software, on page 61
# Change the Virtualization Software

- Virtual Machine Configuration Tasks, on page 61

## 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 [www.cisco.com go virtualized-collaboration](http://www.cisco.com) and following the links for the Unified Communications Manager and IM 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 62</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 IM and Presence on UC on UCS tested reference configuration hardware.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Upgrade vSphere ESXi, on page 63</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 IM and Presence Service; however, if your currently...</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Download and Install OVA Templates, on page 63</td>
<td></td>
</tr>
<tr>
<td></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 IM and Presence on a virtual machine, and your deployment size has not changed, you do not need to download and install a new OVA template. If you are changing the size of your system, download and install an OVA template for the new release that is sized for your deployment.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Change Virtual Machine Configuration Specifications, on page 64</td>
<td></td>
</tr>
<tr>
<td></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 IM and Presence Service. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Migrate From Single to Multi-vDisk Virtual Machine, on page 65</td>
<td></td>
</tr>
<tr>
<td></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 IM and Presence on UC on UCS tested reference configuration hardware. VMware vCenter is mandatory when you deploy on UC on UCS specs-based and third-party server specs-based hardware.

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

**Procedure**

**Step 1** Install VMware vCenter.
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.

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](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html).

This procedure is optional. If you are already running Unified Communications Manager or IM and Presence 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 IM and Presence Service.

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

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

Procedure

Step 1 Perform a Disaster Recovery System (DRS) backup.
Step 2 (Optional) For an upgrade from 9.x or earlier, if you need to increase the vDisk space to meet the space requirements of a refresh upgrade, install the following COP file:

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

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 64 to ensure that the specifications match the requirements of the release.

**Procedure**

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

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

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

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

**Step 5** Perform a DRS restore on the new VM.
PART IV

Upgrade the Applications

• Pre-upgrade Tasks, on page 69
• Upgrade Procedures, on page 95
• Post-upgrade Tasks, on page 119
Pre-upgrade Tasks

- Pre-Upgrade Task Flow, on page 69

Pre-Upgrade Task Flow

Complete the following tasks before you begin 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>Read the release notes for the new release: <a href="http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html">http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html</a></td>
<td>Ensure that you understand the new features and how the upgrade interacts with the other products that are associated with your system. Do this step for all upgrade and migration methods.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Run the pre-upgrade COP.</td>
<td>It runs a series of tests and detects issues that can cause upgrade failures. Install the pre-upgrade COP file to check the upgrade readiness from the current version to the version you are upgrading to, and if you find any issues in the report, fix them before upgrading. This reduces the chances of an upgrade failure.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Consider Smart Licensing Requirements</td>
<td>Release 12.0(1) introduces Smart Licensing as a replacement for Prime License Manager. You must set up a Customer Smart account. You may optionally create the Virtual account under the Smart account based on the organization structure. For more details on Cisco Smart Accounts, see <a href="https://www.cisco.com/c/en/us/buy/smart-accounts.html">https://www.cisco.com/c/en/us/buy/smart-accounts.html</a> and for details on Smart Software Licensing Overview, see <a href="https://www.cisco.com/c/en/us/buy/smart-accounts/software-licensing.html">https://www.cisco.com/c/en/us/buy/smart-accounts/software-licensing.html</a>.</td>
</tr>
<tr>
<td>Step 4</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 <em>Cisco Prime Collaboration Deployment Administration Guide</em> 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>
<td>Purpose: You cannot install or run Unified Communications Manager and the IM and Presence Service directly on server hardware; you must run these applications on virtual machines. Do this step for all upgrade and migration methods.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Familiarize yourself with the requirements and limitations of this release: <a href="#">Requirements and Limitations, on page 17</a>.</td>
<td>Ensure that your system meets all requirements, including network requirements, platform requirements, and software requirements. Do this step for all upgrade and migration methods.</td>
</tr>
</tbody>
</table>
| Step 6 | Check the health of your network:  
- Read [Factors that Affect Upgrade Time Requirements, on page 45](#) and ensure that your system meets the conditions described in that section.  
- Generate a Database Status Report, on page 75  
- Check Database Replication, on page 75  
- Check Performance Reports, on page 76  
- Run CLI Diagnostics, on page 77 | The health of your system affects the amount of time that an upgrade requires. You can reduce the amount of time needed for an upgrade by ensuring that your system meets the conditions described in these sections. Do this step for all upgrade and migration methods. |
| Step 7 | Ensure that there are no expired certificates on the partition, including any trust certificates in the certificate chain. If there are expired certificates, perform one or more of the following procedures:  
- Delete a Trust Certificate, on page 77  
- Regenerate a Certificate, on page 78 if an identity certificate is expired | 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. |
<p>| Step 8 | Take a Fresh Backup, on page 79 | 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. <strong>Caution</strong> You may lose data or you may be unable to restore your system if your backup is outdated. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 9</strong></td>
<td>Back Up Custom Ringtones and Background Images, on page 80 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 10</strong></td>
<td>Check Network Connectivity, on page 80 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 11</strong></td>
<td>Verify IPv6 Networking, on page 81 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 Manager subscriber nodes, load detection may take 20 minutes. Do this step for all upgrade and migration methods.</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>Check Connectivity between IM and Presence and Cisco Unified Communications Manager, on page 81 Verify that the IM and Presence Service node has connectivity with Unified Communications Manager. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.</td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>Collect Configuration and Login Information, on page 82 Record the current configuration and login information for your Unified Communications Manager nodes in case any issues are encountered during the upgrade process.</td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td>Record the Registered Device Count, on page 82 Use the Real Time Monitoring Tool (RTMT) to capture the device count so that you can verify your endpoints and resources after the upgrade is complete. You can also use this information to verify that you have not exceeded the capacity of the virtual machine (VM) that you are deploying. Do this step for all upgrade and migration methods.</td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td>Record the Number of Assigned Users, on page 83 Record the number of assigned users on IM and Presence Service nodes so that you can</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Verify this information after the upgrade is complete. Do this step for all upgrade and migration methods.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 16</strong> Record TFTP Parameters, on page 83</td>
<td>The upgrade process changes a TFTP parameter. Record the current setting so that you can reset the parameter after the upgrade is complete.</td>
</tr>
<tr>
<td><strong>Step 17</strong> Record Enterprise Parameters, on page 84</td>
<td>Record the settings for Enterprise Parameters on both Unified Communications Manager nodes and IM and Presence Service nodes. Some Enterprise Parameters exist on both types of nodes and the settings that are configured on Unified Communications Manager nodes may overwrite the settings configured on IM and Presence Service nodes during an upgrade. Record the settings so that you can restore them as needed after the upgrade is complete. Do this step for all upgrade and migration methods.</td>
</tr>
<tr>
<td><strong>Step 18</strong> Export User Records, on page 84</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 19</strong> Upgrade IP Phone Firmware, on page 85</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. 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> Verify Critical Services, on page 85</td>
<td>Verify that all critical services are activated.</td>
</tr>
<tr>
<td><strong>Step 21</strong> Deactivate Cisco Extension Mobility, on page 86</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...</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Deactivate TFTP services, on page 86</td>
<td>Stop TFTP services on Unified Communications Manager nodes before you begin an upgrade.</td>
</tr>
<tr>
<td>Stop the IM and Presence Sync Agent, on page 87</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 or the PCD Upgrade task to perform the upgrade.</td>
</tr>
<tr>
<td>Check the Available Common Partition Space, on page 87</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>
<tr>
<td>If you do not have enough common partition space, perform one or more of the following procedures:</td>
<td>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>• Adjust High and Low Watermarks, on page 87</td>
<td>Caution: Performing an upgrade without sufficient disk space can cause the upgrade to fail.</td>
</tr>
<tr>
<td>• Create Additional Partition Space, on page 88</td>
<td></td>
</tr>
<tr>
<td>Obtain Upgrade Files, on page 89</td>
<td>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</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>or the PCD Upgrade task to perform the upgrade.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 27</strong></td>
<td>Ensure that you have the necessary license files for the new release.</td>
</tr>
<tr>
<td><strong>Step 28</strong></td>
<td>Increase the Database Replication Timeout, on page 91</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 29</strong></td>
<td>Disable High Availability on Presence Redundancy Groups, on page 92</td>
</tr>
<tr>
<td>This procedure applies to IM and Presence Service nodes only. If you have configured</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Step 30</td>
<td>Add a Serial Port to the Virtual Machine, on page 92 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.</td>
</tr>
</tbody>
</table>

### Generate a Database Status Report

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

**Procedure**

#### Step 1
Log in to the reporting interface for the node:
- For Unified Communications Manager nodes, log in to the Cisco Unified Reporting interface.
- For IM and Presence Service nodes, log in to the Cisco Unified IM and Presence Reporting interface.

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

#### Step 3
Select the report for the node:
- To check database replication on a Unified Communications Manager node, select **Unified CM Database Status**.
- To check database replication on an IM and Presence Service node, select **IM and Presence Database Status**.

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

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

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

### Check Database Replication

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

Run CLI Diagnostics

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

Procedure

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

Step 2  Execute the `utils diagnose test` command.

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

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

Delete a Trust Certificate

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

Caution

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

Procedure

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

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

Step 3  Choose the filename of the certificate.

Step 4  Click Delete.

Step 5  Click OK.

Note

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

• If you import a certificate into the CAPF-trust, it is enabled only on that particular node and is not replicated across the cluster.
Regenerate a Certificate

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

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 Certificate Names and Descriptions, on page 78 for more information.

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 78

Certificate Names and Descriptions

The following table describes the system security certificates that you can regenerate and the related services that must be restarted. For information about regenerating the TFTP certificate, see the Cisco Unified
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>
<tr>
<td>CAPF</td>
<td>The system copies this root certificate to your node or to all nodes in the cluster after you complete the Cisco client configuration.</td>
<td>CallManager and CAPF</td>
</tr>
<tr>
<td>TVS</td>
<td>This is a self-signed root certificate.</td>
<td>TVS</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 IM and Presence Service cluster nodes must be running the same version of the IM and Presence Service application.

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

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

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

Procedure

Step 1 From the Disaster Recovery System, select **Backup > Manual Backup**.
Step 2 In the **Manual Backup** window, select a backup device from the **Backup Device Name** area.
Step 3 Choose a feature from the **Select Features** area.
Step 4 Click **Start Backup**.

**Back Up Custom Ringtones and Background Images**

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

Procedure

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

**Check Network Connectivity**

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

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

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

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

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

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

Step 6  Check that DNS name resolution is working correctly:
   a) Ping the FQDN of each Unified Communications Manager node to ensure that it resolves to the IP address.
   b) Ping the IP address of each Unified Communications Manager to ensure that it resolves to the FQDN.

Verify IPv6 Networking

This procedure applies to Unified Communications Manager nodes only.

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

Procedure

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

Step 2  Execute the following command:

```
utils network ipv6 ping destination [count]
```

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

Check Connectivity between IM and Presence and Cisco Unified Communications Manager

Verify that the IM and Presence Service 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**.
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>
<tr>
<td>XCODE</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 IM and Presence Service nodes. Some Enterprise Parameters exist on both Unified Communications Manager nodes and IM and Presence Service nodes. Where the same parameter exists, the settings that are configured on Unified Communications Manager nodes overwrite the settings configured on IM and Presence Service nodes during the upgrade process. Enterprise Parameters that are unique to IM and Presence Service nodes are retained during an upgrade.

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

Procedure

Step 1  From the Cisco Unified CM Administration interface, choose System > Enterprise Parameters.
Step 2  Take screen captures to record the settings that you have configured, and save the information so that you can restore the settings after the upgrade is complete.
Step 3  From the Cisco Unified CM IM and Presence Administration interface, choose System > Enterprise Parameters.
Step 4  Take screen captures to record the settings that you have configured, and save the information so that you can restore the settings after the upgrade is complete.

Export User Records

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

Procedure

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

Upgrade IP Phone Firmware

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

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

Before you begin

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

Procedure

Step 1 From Cisco Unified OS Administration, choose Software Upgrades > Install/Upgrade.
Step 2 Fill in the applicable values in the Software Location section and click Next.
Step 3 In the Available Software drop-down list, select the device package file and click Next.
Step 4 Verify that the MD5 value is correct, and then click Next.
Step 5 In the warning box, verify that you selected the correct firmware, and then click Install.
Step 6 Check that you received a success message.

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

Step 7 Stop and restart the TFTP server.
Step 8 Reset the affected devices to upgrade the devices to the new load.
Step 9 From Cisco Unified CM Administration, choose Device > Device Settings > Device Defaults and manually change the name of the "Load 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.
Deactivate Cisco Extension Mobility

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

Procedure

Step 1: From Cisco Unified Serviceability, choose Tools > Service Activation.
Step 2: From the Server list, choose the node on which you want to deactivate services and click Go.
Step 3: Deselect the Cisco Extension Mobility services.
Step 4: Click Stop.
Step 5: Repeat Steps 2 through 4 for each node that is running Cisco Extension Mobility services.
Step 6: Make a list of all the nodes on which you have disabled these services. You will need to restart the services after the upgrade is complete.

Deactivate TFTP services

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

Procedure

Step 1: From Cisco Unified Serviceability, choose Tools > Service Activation.
Step 2: From the Server list, choose the node on which you want to deactivate services and click Go.
Step 3: Deselect Cisco TFTP services.
Step 4: Click Stop.
Step 5: Repeat Steps 2 through 4 for each node that is running Cisco TFTP services.
Step 6

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

---

**Stop the IM and Presence Sync Agent**

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

**Procedure**

**Step 1**

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

**Step 2**

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

**Step 3**

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

---

**Check the Available Common Partition Space**

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

**Procedure**

**Step 1**

In the Real-Time Monitoring Tool, select Disk Usage from the list of System counters on the left navigation pane.

A page displays detailed information about disk usage.

**Step 2**

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

However, your deployment may require more space if you have numerous TFTP data (device firmware loads), music-on-hold (MOH) files, or if you have many locale files installed. In some cases, even if 25GB of free space is available, upgrade may fail with the error message as insufficient space. The workaround is to delete the unnecessary files and create more space in the common partition.

---

**Adjust High and Low Watermarks**

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

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

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

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

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

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

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

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

**Required COP Files**

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 Unified Communications Manager Release 12.0(1)**

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Upgrade Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.6(x)</td>
<td>12.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>12.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>12.x</td>
<td>Standard upgrade; no COP file required.</td>
</tr>
<tr>
<td>11.0(x)</td>
<td>12.x</td>
<td>Standard upgrade; no COP file required.</td>
</tr>
<tr>
<td>11.5(x)</td>
<td>12.x</td>
<td>Standard upgrade; COP file is updated to increase the disk space.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ciscocm.free_common_space_v&lt;latest_version&gt;.cop.sgn</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To download the COP files and the Readme files, go to <a href="https://software.cisco.com">https://software.cisco.com</a> &gt; click <strong>Software Download</strong> link under <strong>Download &amp; Upgrade</strong> section, and then, navigate to the **Unified Communications &gt; Call Control &gt; Cisco Unified Communications Manager (CallManager) &gt; &lt;Version&gt; &gt; Unified Communications Manager/CallManager/Cisco Unity Connection Utilities.</td>
</tr>
</tbody>
</table>
Upgrade TypeTo From
PCD Migrations require a COP file:
- ciscocm-slm-migration.k3.cop.sgn
  
  **Note** This requirement applies only for Prime Collaboration Deployment migrations from Release 12.0(1) of Unified Communications Manager (build 12.0.1.10000-10). If you are migrating from a higher release, such as Unified Communications Manager 12.0(1)SU1, you don't need to install the COP file.

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

<table>
<thead>
<tr>
<th>From IM and Presence Release</th>
<th>To IM and Presence Release</th>
<th>Upgrade Type</th>
</tr>
</thead>
</table>
| 9.1(x)                      | 12.x                      | Refresh upgrade. Requires the following COP file:  
  - ciscocm.version3-keys.cop.sgn |
| 10.5(x)                     | 12.x                      | Standard upgrade; no COP file required. |
| 11.0(x)                     | 12.x                      | Standard upgrade; no COP file required. |
| 11.5(x)                     | 12.x                      | Standard upgrade; no COP file required. |

**Increase the Database Replication Timeout**

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

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

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

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

Disable High Availability on Presence Redundancy Groups

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

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

Procedure

Step 1   From the Cisco Unified CM Administration user interface, choose System > Presence Redundancy Groups.
Step 2   Click Find and select the group.
Step 3   On the Presence Redundancy Group Configuration window, uncheck the Enable High Availability check box.
Step 4   Click Save.
Step 5   Repeat this procedure for each Presence Redundancy Group.
Step 6   When you are done, wait at least two minutes to sync the new HA settings across the cluster before you make any further changes

Add a Serial Port to the Virtual Machine

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

Procedure

Step 1   Power off the virtual machine.
Step 2  Edit the settings to add a serial port. For more information about making configuration changes using vSphere Client, refer to the user manual for the product.

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

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

What to do next

After you successfully upgrade the system, follow the procedure to Remove the Serial Port, on page 123. In the event of an upgrade failure, refer to Dump a Log File After an Upgrade Failure, on page 139.
Add a Serial Port to the Virtual Machine
Upgrade Procedures

- Upgrade Overview, on page 95
- Before You Begin, on page 98
- Upgrade Task Flow, on page 99
- Upgrade the Applications, on page 100
- Version Switching, on page 109
- Cluster-Wide Reboot, on page 110
- Switch to Previous Version, on page 111
- Verify that Database Replication is Functioning, on page 113
- Verify that Database Replication is Complete, on page 114
- Upgrade Individual Cluster Nodes through CLI, on page 114
- Upgrade Cluster Through CLI, on page 116

Upgrade Overview

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

Publisher Nodes and Subscriber Nodes

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

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

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

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

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

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

<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>Upgrade type</td>
<td>Switching type</td>
<td>When prompted, choose . . .</td>
<td>Result</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------</td>
<td>------------------------------</td>
<td>------------------------------------------------------------------------</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>Automatic</td>
<td>Switch to new version after upgrade</td>
<td>Choose this option to use the new software version immediately following the upgrade. When you use this upgrade method, you must switch your publisher node to the new software version before you upgrade your subscriber nodes.</td>
<td></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

⚠️ Caution
Stop all configuration tasks. Do not make any configuration changes during an upgrade. For example, do not change passwords, perform LDAP synchronizations, or run any automated jobs. Do not remove, re-add, or re-install any nodes in the cluster during the upgrade process. You can make configuration changes only when you have completed the upgrade on all nodes and performed the post-upgrade tasks. Any configuration changes that you make during an upgrade will be lost, and some configuration changes can cause the upgrade to fail.

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

- Review the pre-installation tasks and ensure that you have performed all the steps.
- Do not rename the upgrade file before you install it because the system will not recognize it as a valid file.
- Do not decompress the file. If you do, the system may not be able to read the upgrade file.
- For upgrades to the IM and Presence Service software, check that the contact list size for users has not reached the maximum value. The System Troubleshooter in Cisco Unified CM IM and Presence Administration indicates if there are users who have reached the contact list limit.
- Modify the network adapter to VMXNET3 before the upgrade process. See OVA readme files.
- If you are upgrading a node in FIPS mode, make sure that your security password has a minimum of 14 characters. For details on how to change security passwords, see the "Reset the Administrative or Security Password" chapter of the Administrative Guide for Cisco Unified Communications Manager and IM and Presence Service at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_0_1/admin/cucm_b_administration-guide-1201.html

⚠️ 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.
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

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Upgrade the application using one of the following procedures:</td>
<td>Use these procedures when you upgrade Unified Communications Manager or the IM and Presence Service using the Unified CM OS Administration interface.</td>
</tr>
<tr>
<td></td>
<td>• Upgrade from a Local Source, on page 101</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Upgrade from a Remote Source, on page 104</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Upgrade from Local Filesystem, on page 106</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Switch the Software Version, on page 109</td>
<td>Use this procedure to activate the new software.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Switch to Previous Version, on page 111</td>
<td>Use the procedures in this section if you need to revert to the software version that was running before the upgrade.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Verify that Database Replication is Functioning, on page 113</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Verify that Database Replication is Complete, on page 114</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>Upgrade Individual Cluster Nodes through CLI, on page 114</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>Upgrade Cluster Through CLI, on page 116</td>
<td></td>
</tr>
</tbody>
</table>
Upgrade the Applications

You can perform single node upgrades and cluster-wide upgrades. To upgrade the applications, you have the following options to access the upgrade files:

• Access the upgrade file using the **Use download credentials from Publisher** option. With this option, you can use the source configurations from the publisher. This option is applicable only for single cluster upgrade.

  ![Note](image)
  
  If the free common space COP file is used on the CUCM publisher, the subscriber nodes may experience errors during the listing of the valid upgrade files. In such a scenario, the following message is displayed:

  Connectivity issue to the first node. Verify that the first node is powered on, the network connection is up and the security password on this node and the first node are the same.
  
  You might also be seeing this message due to the installation of the free common space COP file on the publisher.

  If the intent was to set the "use publisher setting" to "yes/no" in order to facilitate a cluster wide upgrade, then you may ignore this message.

• Access the upgrade file during the installation process from either a local CD or DVD, or from a remote FTP or SFTP server, or from a local file. The directory names and filenames that you enter to access the upgrade file are case-sensitive.
• If a cluster upgrade is in progress, and another upgrade is initiated using User Interface, then, the following warning message is displayed:

A cluster upgrade is in progress. You can check the status of the cluster upgrade using the CLI or GUI of the CUCM Publisher.

• If a single-node upgrade is in progress, and a cluster upgrade is initiated using User Interface, then, the following message is displayed:

A stand-alone upgrade is in progress. You must cancel the upgrade to initiate a cluster upgrade.

• When a single-node upgrade is progress in Unified Communications Manager publisher using either CLI or User Interface, if a cluster upgrade is initiated using the User Interface, then the following message is displayed:

You must cancel the upgrade to initiate a cluster upgrade.

• When a cluster upgrade session is in progress in Unified Communications Manager publisher using either User Interface or CLI, and if another cluster session is initiated using the User Interface, then the following message is displayed:

A cluster upgrade is in progress. Click Assume Control to take over the installation.

• To use the credentials from the publisher, check the Use download credentials from Publisher check box under the Software Upgrades > Install/Upgrade. If you do not want to use this option, you can uncheck the Use download credentials from Publisher check box and proceed with any of the available options from the Source list.

By default, the Use download credentials from Publisher check box is checked. Later if you uncheck or check this Use download credentials from Publisher check box, the settings remain in the system.

If the publisher is set to CD or DVD, then the Use download credentials from Publisher option causes the subscriber to use its own local CD or DVD and not the publisher's local CD or DVD.

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

• During a cluster upgrade, if the publisher upgrade fails, then all the nodes in the cluster will not proceed with the upgrade. Cancel the cluster upgrade and retry after fixing the issues in the publisher node.

Upgrade from a Local Source

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

Before you begin

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

• UCSInstall_CUP_<XXXXXXXX>.sgn.iso
• 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:

Note You can also upgrade the Cisco Unified Communications Manager node through the admin CLI interface. For more information, see the "utils system upgrade" section at Command Line Interface Reference Guide for Cisco Unified Communications Solutions at the https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

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

Step 3
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
If you are performing a single node upgrade, select the Software Upgrades > Install/Upgrade, or If you are performing cluster-wide upgrade, select the Software Upgrades > Install/Upgrade Cluster.

Caution You can perform cluster-wide upgrade only for direct standard upgrade from 12.5(1) to a later release.

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
Check the Continue with upgrade after download check box to start the upgrade directly after the file download completes.

The Continue with upgrade after download check box is checked by default. If you check or uncheck Continue with upgrade after download check box, the settings remain in the system.

Step 9
Check the Switch-version server after upgrade (valid only for ISO) check box to automatically reboot the system after the upgrade completes.
The **Switch-version server after upgrade (valid only for ISO)** check box is unchecked by default. If you check or uncheck the **Switch-version server after upgrade (valid only for ISO)** check box, the settings remain in the system.

**Step 10**

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

If you perform single node upgrade, valid ISO upgrade file for the respective application type is displayed.

If you perform cluster-wide upgrade, valid ISO upgrade files for both Cisco Unified Communications Manager and IM and Presence files are displayed. If there are no valid Cisco Unified Communications Manager or IM and Presence ISO upgrade files, then **Do not upgrade UCM nodes** and **Do not upgrade IMP nodes** are displayed.

**Step 11**

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

**Step 12**

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

For cluster-wide upgrade, you can view the download status of all the nodes selected in the cluster for both Cisco Unified Communications Manager and IM and Presence upgrade filenames.

**Note** If you checked the **Continue with upgrade after download** check box, the upgrade starts directly after the file download. You do not need to validate the checksum details. Go to the **Step 15**.

**Step 13**

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

For cluster-wide upgrade, you can view the checksum details along with the version options (active and to be upgraded versions) and reboot options for both Cisco Unified Communications Manager and IM and Presence upgrade.

**Step 14**

Perform one of the following actions:

- Check the **Switch-version server after upgrade (valid only for ISO)** check box to automatically reboot the system when the upgrade completes.

- Uncheck the **Switch-version server after upgrade (valid only for ISO)** check box to perform a staged upgrade.

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

**Step 15**

Select **Next**.

For a single-node upgrade, the Installion status page displays Cisco Unified Communications Manager File Name, Installation Start Time, and Installation status and the Installation Log section displays Date, Time, and Description.

For cluster-wide upgrades, the Install Status page displays the following two sections:

- **Installation Status**: This section displays the Cisco Unified Communications Manager File Name, IM&Presence file name, Installation Start time, and Cluster Installation status.

- **Installation Log**: This section displays cluster details such as Node, Role, Step, Description, Historical time to complete, and Elapsed time. In case of an ISO upgrade, in the 'Installation Log' box, you will see a hyperlink with the node's name. If you click on the hyperlink, the 'Installation Status' page appears that displays the following details:
Upgrade from a Remote Source

Follow this procedure to upgrade to a new release of Cisco Unified Communications Manager or the IM and Presence Service 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:

Note
You can also upgrade the Cisco Unified Communications Manager node through the admin CLI interface. For more information, see the "utils system upgrade" section at Command Line Interface Reference Guide for Cisco Unified Communications Solutions at the https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

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

Step 3
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.

Select Finish when the installation completes.
Step 4  If you are performing a single node upgrade, select the Software Upgrades > Install/Upgrade, or If you are performing cluster-wide upgrade, select the Software Upgrades > Install/Upgrade Cluster.

Caution  You can perform cluster-wide upgrade only for direct standard upgrade from 12.5(1) to a later release.

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  Check the Continue with upgrade after download check box to start the upgrade directly after the file download completes.

The Continue with upgrade after download check box is checked by default. If you check or uncheck Continue with upgrade after download check box, the settings remain in the system.

Step 13  Check the Switch-version server after upgrade (valid only for ISO) check box to automatically reboot the system after the upgrade completes.

The Switch-version server after upgrade (valid only for ISO) check box is unchecked by default. If you check or uncheck the Switch-version server after upgrade (valid only for ISO) check box, the settings remain in the system.

Step 14  Select Next to continue the upgrade process.

If you perform a single node upgrade, valid ISO upgrade file for the respective application type is displayed.

If you perform cluster-wide upgrade, valid ISO upgrade files for both Cisco Unified Communications Manager and IM and Presence files are displayed. If there are no valid Cisco Unified Communications Manager or IM and Presence ISO upgrade files, then Do not upgrade UCM nodes and Do not upgrade IMP nodes are displayed.

Step 15  Select the upgrade version that you want to install and select Next.

Step 16  Monitor the progress of the download, which includes the filename and the number of megabytes that are being transferred.

For cluster-wide upgrade, you can view the download status of all the nodes selected in the cluster for both Cisco Unified Communications Manager and IM and Presence upgrade filenames.

Note  If you checked the Continue with upgrade after download check box, the upgrade starts directly after the file download. You do not need to validate the checksum details. Go to the Step 19.

Step 17  When the download completes, verify the checksum value against the checksum for the file that you downloaded from Cisco.com.
For cluster-wide upgrade, you can view the checksum details along with the version options (active and to be upgraded versions) and reboot options for both Cisco Unified Communications Manager and IM and Presence upgrade.

**Step 18**
Perform one of the following actions:

- Check the **Switch-version server after upgrade (valid only for ISO)** check box to automatically reboot the system when the upgrade completes.
- Uncheck the **Switch-version server after upgrade (valid only for ISO)** check box to perform a staged upgrade.

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

**Step 19**
Select **Next**.

For a single-node upgrade, the Installion status page displays Cisco Unified Communications Manager File Name, Installation Start Time, and Installation status and the Installation Log section displays Date, Time, and Description.

For cluster-wide upgrades, the Install Status page displays the following two sections:

- **Installation Status**: This section displays the Cisco Unified Communications Manager File Name, IM&Presence file name, Installation Start time, and Cluster Installation status.
- **Installation Log**: This section displays cluster details such as Node, Role, Step, Description, Historical time to complete, and Elapsed time. In case of an ISO upgrade, in the 'Installation Log' box, you will see a hyper link with the node's name. If you click on the hyper link, the 'Installation Status' page appears that displays the following details:
  - Step
  - Description
  - Historical Time to complete
  - Percentage of total time spent in this step
  - Elapsed time

**Step 20**
Select **Finish** when the installation completes.

---

### Upgrade from Local Filesystem

Follow this procedure to upgrade to a new release of Cisco Unified Communications Manager or the IM and Presence Service using software using previously downloaded ISO or COP file.

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

**Note** You can also upgrade the Cisco Unified Communications Manager node through the admin CLI interface. For more information, see the "utils system upgrade" section at [Command Line Interface Reference Guide for Cisco Unified Communications Solutions](https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html).

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

**Step 2**
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 3**
If you are performing a single node upgrade, select the **Software Upgrades > Install/Upgrade**, or If you are performing cluster-wide upgrade, select the **Software Upgrades > Install/Upgrade Cluster**.

You can view the existing ISO file as **Local Storage Images: UCSInstall_UCOS_<XXXXXXXX>.sgn.iso**.

**Caution** You can perform cluster-wide upgrade only for direct standard upgrade from 12.5(1) to a later release.

**Step 4**
Select **Local Filesystem** from the **Source** list to use the existing ISO or COP file for upgrade.

**Note** You can use this Local Filesystem option, if you want to resume the upgrade after a cancel operation.

**Step 5**
Enter your email address and IP address in the **Email Notification** and **SMTP Server** fields. This enables you to receive an email notification upon successful completion of the upgrade.

**Note** These fields are only visible for refresh upgrades.

**Step 6**
Check the **Continue with upgrade after download** check box to start the upgrade directly after the file download completes.

The **Continue with upgrade after download** is checked by default. If you check or uncheck the **Continue with upgrade after download** check box, the settings remain in the system.

**Step 7**
Check the **Switch-version server after upgrade (valid only for ISO)** check box to automatically reboot the system after the upgrade completes.
The **Switch-version server after upgrade (valid only for ISO)** check box is unchecked by default. If you check or uncheck the **Switch-version server after upgrade (valid only for ISO)** check box, the settings remain in the system.

**Step 8**

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

If you perform a single node upgrade, valid ISO upgrade file for the respective application type is displayed.

If you perform cluster-wide upgrade, valid ISO upgrade files for both Cisco Unified Communications Manager and IM and Presence files are displayed. If there are no valid Cisco Unified Communications Manager or IM and Presence ISO upgrade files, then **Do not upgrade UCM nodes** and **Do not upgrade IMP nodes** are displayed.

**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.

If subscriber is selected to use download credentials from Publisher, and the file is not present in any of the nodes. Then, the download fails during validation.

**Note** If you checked the **Continue with upgrade after download** check box, the upgrade starts directly after the file download. You do not need to validate the checksum details. Go to the **Step 13**.

**Step 11**

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

For cluster-wide upgrade, you can view the checksum details along with the version options (active and to be upgraded versions) and reboot options for both Cisco Unified Communications Manager and IM and Presence upgrade.

**Step 12**

Perform one of the following actions:

- Check the **Switch-version server after upgrade (valid only for ISO)** check box to automatically reboot the system when the upgrade completes.
- Uncheck the **Switch-version server after upgrade (valid only for ISO)** check box to perform a staged upgrade.

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

**Step 13**

Select **Next**.

For a single-node upgrade, the Installion status page displays Cisco Unified Communications Manager File Name, Installation Start Time, and Installation status and the Installation Log section displays Date, Time, and Description.

For cluster-wide upgrades, the Install Status page displays the following two sections:

- Installation Status: This section displays the Cisco Unified Communications Manager File Name, IM&Presence file name, Installation Start time, and Cluster Installation status.
- Installation Log: This section displays cluster details such as Node, Role, Step, Description, Historical time to complete, and Elapsed time. In case of an ISO upgrade, in the 'Installation Log' box, you will see a hyper link with the node's name. If you click on the hyper link, the 'Installation Status' page appears that displays the following details:
• Step
• Description
• Historical Time to complete
• Percentage of total time spent in this step
• Elapsed time

**Step 14**

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.

For information on the supported version switching, see the Applications Installed on Virtual Machines, on page 35 the section of this document.

---

**Switch the Software Version**

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

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

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

---

**Caution**

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

---

**Before you begin**

The software versions on Unified Communications Manager and IM and Presence nodes must match according to the manual switching rules. Therefore, you must switch Unified Communications Manager before you switch IM and Presence.
Review the information in Understanding Version Switching, on page 96

**Procedure**

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

**Step 2** Log in to the management software for the node that you are upgrading:
- If you are upgrading an IM and Presence node, log in to Cisco Unified IM and Presence Operating System Administration.
- If you are upgrading a Unified Communications Manager node, log in to Cisco Unified Communications Operating System Administration.

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

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

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

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

**Cluster-Wide Reboot**

You can perform the cluster-wide restart or switch version operation by placing cluster nodes in different batches in sequential order using sliders.

**Before you begin**

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

**Note**

From 12.5(1) release onwards, you can upgrade Unified Communication and IM&P cluster through Direct Standard (L2) and Refresh Upgrade (RU). To return to the previous version, switch to the older version of the software using the CLI command (**utils system switch-version**) or OS Admin (Settings->Version->Switch Version). This is a new feature introduced from release 12.5(1) onwards. You cannot switch version to previous version other than the current 12.5 release using Reboot cluster switch version.

**Procedure**

**Step 1** Log in to the management software for the cluster that you are upgrading:
- For upgrading a Unified Communications Manager cluster or IM and Presence cluster, log in to Cisco Unified Communications Operating System Administration interface of the Publisher.

**Step 2** Select **Software Upgrades > Reboot Cluster**.
Unified Communications Manager and IM and Presence have default supported sequence of nodes. You can change the sequence if required by moving the sliders of respective nodes in batches in sequential order to initiate the restart and switch version operations.

**Note** The slider of Cisco Unified Communications Manger publisher is placed in Batch1 by default. You cannot change the sequence of Cisco Unified Communications Manger publisher.

**Step 3** Click **Reset** to reset to the Cisco-defined default best practices configuration.

**Step 4** To skip any of the nodes from restart and switch version operation, check the **Skip** check box of the respective nodes.

**Step 5** Click **Save** to save the sequence.

Unified Communications Manager validates the node sequence and generates the error message if you entered an unsupported sequence.

**Step 6** Click **Switch Version** to switch to a previous version or to a newly upgraded version.

**Step 7** Click **Restart** to restart the system.

---

### Switch to Previous Version

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

### Switch Cluster to Previous Version

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

**Procedure**

**Step 1** Switch back the publisher node.

**Step 2** Switch back all backup subscriber nodes.

**Step 3** Switch back all primary subscriber nodes.

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

### Switch Node to Previous Version

**Procedure**

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

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

Step 2  Choose Settings > Version.
The Version Settings window displays.

Step 3  Click the Switch Versions button.
After you verify that you want to restart the system, the system restarts, which might take up to 15 minutes.

Step 4  To verify that the version switch was successful, follow these steps:
a) Log in again to the management software for the node that you are upgrading.
b) Choose Settings > Version.
The Version Settings window displays.
c) Verify that the correct product version is now running on the active partition.
d) Verify that all activated services are running.
e) For the publisher node, log in to Cisco Unified CM Administration.
f) Verify that you can log in and that your configuration data exists.

Reset Database Replication

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

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

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

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

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

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

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

Before you begin
Switch versions on Unified Communications Manager.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>Download the following COP file from Cisco.com:</strong> ciscocm.cup.pe_db_install.cop.</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>Sign into Cisco Unified IM and Presence Operating System Administration.</strong></td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>Select Settings &gt; Version.</strong></td>
</tr>
</tbody>
</table>
| 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 multimode environment, you must install the COP file on every node in the cluster. |
| Step 7  | **After you have installed the COP file, manually restart the system. To do this, select Settings > Version and select Restart.** |
| Step 8  | **Run the following CLI command (on the publisher or subscriber node) to check if the database replication is active on the node:** \texttt{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:** \texttt{utils dbreplication reset all}  

---

**Verify that Database Replication is Functioning**

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

**Before you begin**

Ensure that the Cisco Tomcat service is running.

**Procedure**

| Step 1  | **Log in to the reporting interface for the node:**  
  • For Unified Communications Manager nodes, log in to the Cisco Unified Reporting interface. |
• For IM and Presence Service nodes, log in to the Cisco Unified IM and Presence Reporting interface.

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

**Step 3** Select the report for the node:
- To check database replication on a Unified Communications Manager node, select **Unified CM Database Status**.
- To check database replication on an IM and Presence Service node, select **IM and Presence Database Status**.

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

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

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

---

## Verify that Database Replication is Complete

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

**Procedure**

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

**Step 2** Execute the **utils dbreplication runtimestate** command to monitor whether the database replication is active on the node and to view the progress of the database setup.

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

If database replication is not complete (a value other than 2 is returned), core services will not start on the subscriber nodes until replication is complete.

---

## Upgrade Individual Cluster Nodes through CLI

Use this procedure to use the Command Line Interface to upgrade an individual Cisco Unified Communications Manager or IM and Presence Service cluster node. If you use this option, you must upgrade the Cisco Unified Communications Manager publisher node before upgrading any subscriber nodes or IM and Presence nodes.
Before you begin
Complete the Pre-upgrade Tasks.

Procedure

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

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

Step 3 When prompted, enter whether you want to use the publisher node credentials for the upgrade (the default value is yes). Later if you change the value to yes or no, the settings remain in the system.

If the publisher is set to CD or DVD, then the Use download credentials from Publisher option causes the subscriber to use its own local CD or DVD and not the publisher's local CD or DVD.

If subscriber is selected to use download credentials from Publisher, and the file is not present in any of the nodes. Then, the download fails during validation.

Note The Use download credentials from Publisher prompt does not appear if you are upgrading the Cisco Unified Communications Manager publisher node.

Step 4 When you enter the value as no, enter the Remote Filesystem, Local DVD/CD, or Local Image source details where the upgrade image is saved.

With the Local Image source option, you can use the previously downloaded ISO or COP file for the upgrade.

If there is no downloaded ISO or COP file, the source displays the Local Image<none>. If there is an ISO or COP file, then it displays the Local Image option with the .iso or .cop downloaded file.

Step 5 When prompted, enter yes or no to indicate whether to proceed with the upgrade automatically once the upgrade file downloads.

- Yes—the upgrade proceeds automatically once the file is downloaded.
- No—the file downloads, but the upgrade stops. You can reinitialize the upgrade later.

Note If a cluster upgrade is in progress, and another upgrade is initiated using the User Interface, then the following message is displayed:

A cluster upgrade is in progress. You can check the status of the cluster upgrade using the CLI or GUI of the CUCM Publisher.

Step 6 When prompted, enter yes or no to indicate whether to switch to the new version automatically after the upgrade completes. The default value is no. If you enter yes, the system reboots immediately following the upgrade.

- Yes—once the upgrade completes, the system switches over to the new version immediately and an automatic system reboot occurs.
- No—the upgrade commences, but remains at the old version when the upgrade completes. You can switch versions later. This is the default option.

Step 7 If you are prompted to start the installation, enter yes.

Upgrade Cluster Through CLI

Use this procedure to upgrade your system through the Command Line Interface. You can use a local source, remote upgrade file system, or local image to upgrade your system.

Before you begin
Complete the Pre-upgrade Tasks.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Log into the Command Line Interface from the Unified Communications Manager publisher node.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Run the <code>utils system upgrade cluster</code> CLI command and follow the prompts.</td>
</tr>
<tr>
<td>Step 3</td>
<td>When prompted, enter the Remote File system, Local DVD/CD, or Local Image source details where the upgrade image is saved. With the Local Image option, you can use the previously downloaded ISO or COP file for the upgrade. If there is no downloaded ISO or COP file, the source displays the Local Image&lt;none&gt;. If there is an ISO or COP file, then it displays the Local Image option with the .iso or .cop downloaded file.</td>
</tr>
</tbody>
</table>
| Step 4 | When prompted, enter yes or no to indicate whether to proceed with the upgrade automatically once the upgrade file downloads.  

  • Yes—the upgrade proceeds automatically once the file is downloaded.  
  • No—the file downloads, but the upgrade stops. You can reinitialize the upgrade later. |
| Step 5 | When prompted, enter yes or no to indicate whether to switch to the new version automatically after the upgrade completes. The default value is no. If you enter yes, the system reboots immediately following the upgrade.  

  • Yes—once the upgrade completes, the system switches over to the new version immediately and an automatic system reboot occurs.  
  • No—the upgrade commences, but remains at the old version when the upgrade completes. You can switch versions later. This is the default option. |

Note
If a single node upgrade is in progress, and a cluster upgrade is initiated using the CLI, then, the following message is displayed:

A stand-alone upgrade is in progress. You must cancel the upgrade to initiate a cluster upgrade.

If a cluster upgrade is in progress in Cisco Unified Communication Manager publisher either using CLI or User Interface, if a single node upgrade is initiated using CLI, then the following message is displayed:

A cluster upgrade is in progress. You can check the status of the cluster upgrade by running "utils system upgrade cluster initiate" on the CUCM Publisher

If a cluster upgrade session is in progress in Cisco Unified Communication Manager publisher either from User Interface or CLI, if another cluster session is initiated using another CLI, then the following message is displayed:

Another user session is currently configuring a cluster upgrade. Assume control (yes/no): yes
Step 6 If you are prompted to start the installation, enter yes.

Upgrade Cluster Through CLI
Post-upgrade Tasks

- Post-upgrade Task Flow, on page 119

Post-upgrade Task Flow

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

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Switch the Software Version, on page 122</td>
<td>If you did not switch versions immediately after completing the upgrade, do so now. You must switch versions so that the upgrade is complete and all nodes in the cluster are updated. Do not perform a backup until you have switched to the new software version. Perform this procedure for all nodes.</td>
</tr>
</tbody>
</table>

| Step 2 | Remove the Serial Port, on page 123 | During the pre-upgrade tasks, you added a serial port to the virtual machine to capture the upgrade logs. After you have successfully upgraded the system, you must remove the serial port so that it does not impact the performance of the virtual machine. Perform this procedure for all nodes. |

<p>| Step 3 | Restart Extension Mobility, on page 123 | 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 after the upgrade is complete. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> Restart TFTP Services, on page 124</td>
<td>Use this procedure to restart TFTP services on Unified Communications Manager nodes after you complete an upgrade.</td>
</tr>
<tr>
<td><strong>Step 5</strong> Run the post upgrade COP.</td>
<td>It runs a series of tests to verify that the system is stable. It also compares various parameters before the upgrade with the current version to identify any differences. After you complete all the steps in this table, run the post-upgrade COP file again and verify the COP report.</td>
</tr>
<tr>
<td><strong>Step 6</strong> Reset TFTP Parameters, on page 124</td>
<td>Reset TFTP parameters that are changed during the upgrade process.</td>
</tr>
<tr>
<td><strong>Step 7</strong> Restore Enterprise Parameters, on page 124</td>
<td>Use this procedure to restore Enterprise Parameters on IM and Presence Service nodes that may have been overwritten during the upgrade process.</td>
</tr>
<tr>
<td><strong>Step 8</strong> Reset High and Low Watermarks, on page 125</td>
<td>Use this procedure to restore the high and low watermarks to their original values in order to avoid premature purging of traces. Do this step for only for direct upgrades, which use either the Unified CMOS Admin interface or the PCD Upgrade task to perform the upgrade.</td>
</tr>
<tr>
<td><strong>Step 9</strong> Updating VMware Tools, on page 125</td>
<td>You must update the VMWare Tools after you complete the upgrade. Perform this procedure for all nodes.</td>
</tr>
<tr>
<td><strong>Step 10</strong> Install Locales, on page 126</td>
<td>Use this procedure to install locales. After an upgrade, you must reinstall any locales that you are using, with the exception of US-English, which is installed by default. Perform this procedure for all nodes.</td>
</tr>
<tr>
<td><strong>Step 11</strong> Restore the Database Replication Timeout, on page 128</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 12</strong> Verify the Registered Device Count, on page 128</td>
<td>Use this procedure to verify your endpoints and resources on Unified Communications Manager nodes after the upgrade is complete.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 13</th>
<th>Verify Assigned Users, on page 129</th>
<th>Purpose: Use this procedure to verify the number of assigned users on IM and Presence Service nodes after the upgrade is complete.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 14</td>
<td>Test Functionality, on page 129</td>
<td>Purpose: Verify phone functions and features are working correctly after the upgrade.</td>
</tr>
<tr>
<td>Step 15</td>
<td>Upgrade RTMT, on page 130</td>
<td>Purpose: If you use Cisco Unified Real Time Monitoring Tool (RTMT), upgrade to the new software version.</td>
</tr>
<tr>
<td>Step 16</td>
<td>Manage TFTP Server Files, on page 131</td>
<td>Optional. Use this procedure to upload phone rings, callback tones, and backgrounds to a TFTP server so that they are available to Unified Communications Manager nodes.</td>
</tr>
<tr>
<td>Step 17</td>
<td>Set Up a Custom Log-On Message, on page 132</td>
<td>Optional. Upload a text file that contains a customized log-on message that appears in Cisco Unified Communications Operating System Administration, Cisco Unified CM Administration, Cisco Unified Serviceability, Disaster Recovery System Administration, Cisco Prime License Manager, and the command line interface. Perform this procedure on Unified Communications Manager nodes only.</td>
</tr>
<tr>
<td>Step 18</td>
<td>Configure IPSec Policies, on page 132</td>
<td>Purpose: 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.</td>
</tr>
<tr>
<td>Step 19</td>
<td>Assign New Manager Assistant Roles, on page 133</td>
<td>Purpose: 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 and are removed during the upgrade process. You must assign new roles for those users. Perform this procedure on Unified Communications Manager nodes only.</td>
</tr>
</tbody>
</table>
| Step 20 | Verify IM and Presence Service Data Migration, on page 133 | Purpose: Use this procedure only if you performed an upgrade or migration from Cisco Unified Communications Manager and the IM and Presence Service, Release 12.5(1)
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 21</td>
<td>Enable High Availability on Presence Redundancy Groups, on page 134</td>
</tr>
<tr>
<td></td>
<td>Presence Release 8.x to an IM and Presence Service release.</td>
</tr>
<tr>
<td></td>
<td>This procedure applies to IM and Presence Service nodes only. If you</td>
</tr>
<tr>
<td></td>
<td>disabled high availability on presence redundancy groups before</td>
</tr>
<tr>
<td></td>
<td>beginning the upgrade process, use this procedure to enable it now.</td>
</tr>
<tr>
<td>Step 22</td>
<td>Restart the IM and Presence Sync Agent, on page 135</td>
</tr>
<tr>
<td></td>
<td>If you stopped the IM and Presence Sync Agent service before you began</td>
</tr>
<tr>
<td></td>
<td>the upgrade process, restart it now.</td>
</tr>
<tr>
<td>Step 23</td>
<td>Restart CER Service</td>
</tr>
<tr>
<td></td>
<td>For AXL Connection to be established after Unified Communications</td>
</tr>
<tr>
<td></td>
<td>Manager upgrades, you need to restart the CER service.</td>
</tr>
<tr>
<td></td>
<td>You need to restart the AXL Change notification toggle on Unified</td>
</tr>
<tr>
<td></td>
<td>Communications Manager publisher as well.</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 IM and Presence nodes must match according to the manual switching rules. Therefore, you must switch Unified Communications Manager before you switch IM and Presence.

Review the information in Understanding Version Switching, on page 96

**Procedure**

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

**Step 2**  Log in to the management software for the node that you are upgrading:
If you are upgrading an IM and Presence node, log in to Cisco Unified IM and Presence Operating System Administration.

If you are upgrading a Unified Communications Manager node, log in to Cisco Unified Communications Operating System Administration.

Step 3 Select Settings > Version.
Step 4 Verify the version of the active software and the inactive software.
Step 5 Select Switch Versions to switch versions and restart the system.

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

**Remove the Serial Port**

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

**Procedure**

Step 1 Power off the virtual machine.
Step 2 Edit the settings to remove the serial port. For information about how to edit the settings, see the VMWare documentation.
Step 3 Power on the virtual machine and proceed with the post-upgrade tasks.

**Restart Extension Mobility**

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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>From Cisco Unified Serviceability, choose Tools &gt; Service Activation.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>From the Server list, choose the node on which you want to deactivate services and click Go.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Select the Cisco Extension Mobility services.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Click Restart.</td>
</tr>
</tbody>
</table>
Restart TFTP Services

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

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>From Cisco Unified Serviceability, choose <em>Tools &gt; Service Activation</em>.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>From the <em>Server</em> list, choose the node on which you want to deactivate services and click <em>Go</em>.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Select the <em>Cisco TFTP</em> services.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Click <em>Restart</em>.</td>
</tr>
</tbody>
</table>

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**

1. From the Cisco Unified CM Administration interface, choose *System > Service Parameters*.
2. From the *Server* drop-down list, select the node that is running the TFTP service.
3. From the *Service* drop-down list, select *Cisco TFTP service*.
4. Click *Advanced*.
5. Click *Save*.
6. Set the *Maximum Serving Count* to the same value that you used prior to the upgrade, or to the value that is recommended for your configuration.

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

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

Restore Enterprise Parameters

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

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

**Before you begin**

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

**Procedure**

**Step 1**

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

**Step 2**

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

**Step 3**

Click **Save**.

**Step 4**

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

---

**Reset High and Low Watermarks**

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

**Procedure**

**Step 1**

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

**Step 2**

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

**Step 3**

Select **Next**.

**Step 4**

Adjust the slider value to 80.

**Step 5**

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

**Step 6**

Select **Next**.

**Step 7**

Adjust the slider value to 85.

---

**Updating VMware Tools**

VMware Tools are a set of utilities for management and performance optimization. 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](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 IM and Presence Service node.

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

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

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

#### Step 1
Find the locale installer for your release on cisco.com:
- For Cisco Unified Communications Manager, go to [https://software.cisco.com/download/navigator.html?mdfid=268439621&i=rm](https://software.cisco.com/download/navigator.html?mdfid=268439621&i=rm)

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

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

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

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

#### Step 6
Click Next.

#### Step 7
Download and install the locale on the server.

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

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

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

### Verify Assigned Users

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

**Procedure**

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

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

### Test Functionality

After the upgrade, perform the following tasks:

- Run the post-upgrade COP.

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

- Verify phone functions by making the following types of calls:
  - Voice mail
  - Interoffice
  - Mobile phone
  - Local
  - National
  - International
  - Shared line

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

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

Upgrade RTMT

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

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

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

Procedure

Step 1  From Unified Communications Manager Administration, choose Application > Plugins.
Step 2  Click Find.
Step 3  Perform one of the following actions:
  • To install the tool on a computer that is running the Microsoft Windows operating system, click the Download link for the Cisco Unified Real-Time Monitoring Tool - Windows.
  • To install the tool on a computer that is running the Linux operating system, click the Download link for the Cisco Unified Real-Time Monitoring Tool - Linux.
Step 4  Download the installation file to your preferred location.
Step 5  Locate and run the installation file.
The extraction process begins.

Step 6  In the RTMT welcome window, click Next.

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

Step 8  In the Maintenance Complete window, click Finish.

Manage TFTP Server Files

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

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

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

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

**Procedure**

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

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

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

a)  Click Upload File.

   The Upload File dialog box opens.

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

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

d)  To start the upload, click Upload File.

   The Status area indicates when the file uploads successfully.

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

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

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

**Step 3**
To delete files, follow this procedure:

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

b) Click Delete Selected.

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

---

### Set Up a Custom Log-On Message

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

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

**Procedure**

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

The Customized Logon Message window displays.

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

**Step 3** Click Upload File.

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

The system displays the customized log-on message.

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

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

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

---

### Configure IPSec Policies

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

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

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

**Procedure**

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

**Step 2**
Click **Add New**.

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

**Step 4**
Click **Save**.

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

---

**Assign New Manager Assistant Roles**

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

**Procedure**

**Step 1**

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

---

**Verify IM and Presence Service Data Migration**

When you upgrade from Cisco Unified Presence Release 8.x to an IM and Presence Service release, user profiles are migrated to 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: UServiceProfile_Migration_x (where x is a number starting at 1)

Description: Migrated Service Profile Number x

To ensure that users can successfully log into Cisco Jabber after an upgrade from Cisco Unified Presence Release 8.x, you must verify that the user profile data migration was successful.
Profiles that are created but that are not assigned to users are not migrated to Unified Communications Manager.

Procedure

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

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

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

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

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

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

---

**What to do next**

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

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

---

**Enable High Availability on Presence Redundancy Groups**

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

**Before you begin**

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

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

**Procedure**

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

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

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

**Step 4**
Click **Save**.

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

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

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>From the Cisco Unified Serviceability interface, select <strong>Tools &gt; Control Center - Network Services</strong>.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Select an IM and Presence Service node from the <strong>Server</strong> drop-down list and click <strong>Go</strong>.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>In the <strong>IM and Presence Services</strong> section, select the <strong>Cisco Sync Agent</strong> and click <strong>Restart</strong>.</td>
</tr>
</tbody>
</table>

Example

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

Note

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

Restart CER Service

Procedure

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>From the Cisco Emergency Responder serviceability interface, select <strong>Tools &gt; Control Center</strong>.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Select <strong>Cisco Emergency Responder</strong> and click <strong>Restart</strong>.</td>
</tr>
</tbody>
</table>
Restart CER Service
PART V

Troubleshooting

• Troubleshooting, on page 139
Troubleshooting

This section contains the following information:

- Dump a Log File After an Upgrade Failure, on page 139
- Troubleshooting Unified Communications Manager Upgrades, on page 140
- Troubleshooting IM and Presence Upgrades, on page 144

Dump a Log File After an Upgrade Failure

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

Before you begin

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

Procedure

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

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

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

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

Step 4 Select the datastore where you created the file.

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

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

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

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

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

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

---

## Troubleshooting Unified Communications Manager Upgrades

This section provides information about troubleshooting Unified Communications Manager upgrades.

### Upgrade Failure

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

**Solution** Do one of the following:

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

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

### Retrying a Cluster or Single-node Upgrade

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

### Troubleshooting Simplified Upgrade Issues

**Download Failure in Some Nodes of the Cluster**

**Problem:** Download failed in some nodes of the cluster while performing simplified upgrade.
Solution: Verify the Software location configuration for the nodes that failed to download. Invalid location or wrong credentials may cause the failure. If you are using the 'Use download credentials from publisher' option, then, ensure that the configuration of the failed node is correct.

To verify, perform one of the following:

• User Interface: Open the Install/Upgrade page of the node and see if the check box is checked. If it is checked, it indicates that the configuration is correct. If the check box is not checked, check it and click Next to save the configuration and then click Cancel to exit from the Install/Upgrade page.

• CLI: Use the `utils system upgrade initiate` command, and ensure that 'Use download credentials from Publisher (yes/no)' is set to 'yes'. If it is set to 'yes', it indicates that the configuration is correct. If not, set it to 'yes' and come out by selecting 'q' and execute the `utils system upgrade cancel` command for a clean exit.

Download or Installation Failure in Some Nodes of the cluster

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

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

Note

When simplified upgrade fails in Download or Install phase:

• User Interface: Install/Upgrade Cluster page displays the status of each node to identify the failed nodes until cancel is clicked.

• CLI: `utils system upgrade cluster initiate` or `utils system upgrade cluster status` displays the status of each node to identify the failed nodes until the `utils system upgrade cluster cancel` command is executed.

Switch Version or Reboot Failure in Some Nodes of the Cluster

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

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

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

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

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

**Problem:** High CPU alerts were received during Cluster upgrade

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

Retrying a Cluster Upgrade after a Failed Cluster Upgrade

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

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

Download Failure due to SSL Error

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

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

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

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

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

Changes to 'Skip' Checkbox are not Saved

**Problem:** Skip check box selections are not saved.

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

Unable to Retry Cluster Upgrade or Single-node Upgrade

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

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

Upgrade Fails with Insufficient Disk Space

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

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

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

- Use the Disk Expansion COP file (ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn) to expand the vDisk size if your virtual environment has additional available disk space. Ensure that you review the Readme file that supports this COP file before you proceed.
- Use the Free Common Space COP file (ciscocm.free_common_space_v<latest_version>.cop.sgn). This COP file removes the inactive side in the common partition to increase available disk space without requiring a system rebuild. Ensure that you review the Readme file that supports this COP file before you proceed.
- Manually remove outdated or unused firmware files from the TFTP directory. You can remove these files using the TFTP File Management page in the OS Administration interface, or you can use the `file list tftp` and `file delete tftp` commands from the command line interface.

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

### Resuming a Failed Upgrade

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

**Note**

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

**Procedure**

**Step 1**

Cancel the upgrade.

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

**Step 2**

Fix your system issue. Refer to the sections in this Troubleshooting Guide to address your system issues.

**Step 3**

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

**Step 4**

Complete your system upgrade.

### Reduced Permissions for Access Control Groups

**Problem**

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

**Solution**

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

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

**Loss of Phone Settings**

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

**Post-Upgrade Failure of Unified Communications Manager Publisher Node**

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

**Solution** Do one of the following:

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

**Post-Upgrade Failure of Unified Communications Manager Subscriber Nodes**

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

**Solution** Do one of the following:

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

**Troubleshooting IM and Presence Upgrades**

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

**Upgrade Failure of IM and Presence Database Publisher Node**

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

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

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

Upgrade Failure of IM and Presence Subscriber Node

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

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

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

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

Upgrade From Pre Release 8.6(4) Fails

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

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

1. Log into Cisco Unified Presence Administration interface and choose System > CUCM Publisher.
2. If the CUCM Publisher Hostname value does not match the hostname, modify it and click Save.
3. Restart the Cluster Manager service with the following CLI command: \texttt{utils service restart Cluster Manager}
4. Open the `platformConfig.xml` file at the following location: `/usr/local/platform/conf/`

5. Verify that the values for `IPSecMasterHost` and `NTPServerHost` match exactly the Cisco Unified Communications Manager hostname.

6. If necessary, modify the value for `IPSecMasterHost` and `NTPServerHost`, save the `platformConfig.xml` file and restart the Cluster Manager service again.

---

**IM and Presence user phone presence problems**

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

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

---

**Presence User Experiences Issues Obtaining Availability**

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

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

---

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

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

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

---

**Cannot find upgrade file on remote server**

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

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

---

**Upgrade file checksum values do not match**

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

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

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

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

Cisco UP Presence Engine database does not restart

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

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

Version Errors

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

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

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

**Version Does Not Match the Active or Inactive Version**

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

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

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

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

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

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

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

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

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

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

Failed refresh upgrade

Problem A refresh upgrade failed.

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

Cancelled or failed upgrade

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

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

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

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

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

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

**Solution** Download and apply the COP file `ciscoim.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 153
• Upgrading from Legacy Releases, on page 157
• Additional Upgrade Resources, on page 159
Frequently Asked Questions

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

Verify the requirements for the new release using the information below. After you have verified the requirements for the new release, see Change the Virtualization Software, on page 59 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 IM and Presence applications. The correct VM configuration to use from the OVA file is based on the size of the deployment. For more information about the OVA files, search 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 of 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 IM and Presence on Business Edition 6000/7000 appliances, or on UC on UCS tested reference configuration hardware. VMware vCenter is mandatory when you deploy on UC on UCS specs-based and third-party server specs-based hardware.

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

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

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

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

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

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

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

To obtain an OVA file, see Download and Install OVA Templates, on page 63.

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

See the Cisco Unified Communications Compatibility Tool at http://tools.cisco.com/ITDIT/vtgsc/VTGServlet for software compatibility information.
I have applications that use an administrative XML (AXL) interface to access and modify Unified Communications Manager information. Will my application continue to work after I upgrade to Unified Communications Manager?

For information about upgrading your AXL applications, see https://developer.cisco.com/site/axl/learn/how-to/upgrade-to-a-new-axl-schema.gsp. To see a list of the AXL operations supported for your release, refer to https://developer.cisco.com/site/axl/documents/operations-by-release/.
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 to Release 12.0(1) from 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>Unified Communications Manager Releases</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.x</td>
<td>Migrate to 6.1(5), 7.1(3), or 7.1(5) using 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 12.0(1)</td>
</tr>
</tbody>
</table>
### Installed Version

<table>
<thead>
<tr>
<th>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 12.0(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), 8.0(x), 8.5(1), or 8.6(2)</td>
<td>PCD Migration to 12.0(1)</td>
</tr>
<tr>
<td>7.1(2)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Cisco Unified Presence Releases

<table>
<thead>
<tr>
<th>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 12.0(1)</td>
</tr>
</tbody>
</table>

### Unified Communications Manager Business Edition Releases

<table>
<thead>
<tr>
<th>Edition</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 to Unified Communications Manager Release 12.0(1) are not supported for these deployments. We recommend that you perform a fresh installation for upgrades from these products to the current Unified Communications Manager release.</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 159

Additional Upgrade Resources


