



CHAPTER 7

Software Upgrades

You can use the Software Upgrades options to perform the following types of installations and upgrades:

- **Install/Upgrade**—Use this option to upgrade the application software, install Cisco Unified Communications Manager Locale Installers and dial plans, and upload and install device packs, phone firmware loads, and other COP files.
- **TFTP File Management**—Use this option to upload various device files for use by the phones to the TFTP server. The TFTP server files that you can upload include custom phone rings, callback tones, and phone backgrounds.

This chapter contains the following sections:

- [Pre-Upgrade Tasks, page 7-1](#)
- [Software Upgrade Considerations, page 7-3](#)
- [Software Upgrade Procedures, page 7-11](#)
- [Post-Upgrade Tasks, page 7-14](#)
- [Stalled Upgrades, page 7-15](#)
- [Reverting to a Previous Version, page 7-15](#)
- [Installing COP Files, Dial Plans, and Locales, page 7-17](#)
- [Managing TFTP Server Files, page 7-21](#)
- [Setting Up a Customized Log-on Message, page 7-22](#)

Pre-Upgrade Tasks

Before you begin the upgrade, perform the following tasks:

- Read the release notes for the new release and be sure that you understand the new features and how the upgrade interacts with the other products that are associated with your system, such as JTAPI, IPMA, RTMT, IPCC, firewalls, and so on.

For Cisco Unified Communications Manager, the release notes are located at

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

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

You must obtain a software feature license if you are upgrading from Cisco Unified Communications Manager 5.x. A software feature license activates features on your system for the specified license version. To use 5.0 device licenses with Cisco Unified Communications Manager 6.(x) or later, make sure that you obtain the software feature license for the Cisco Unified Communications Manager version that is running on your system.

For more information on obtaining and installing licenses, see the License File Upload chapter in the *Cisco Unified Communications Manager Administration Guide*.

- Before you begin the upgrade, back up your system.
- Disable the Cisco Extension Mobility service by navigating to **Cisco Unified Serviceability > Tools > Service Activation**. For more information, see the *Cisco Unified Serviceability Administration Guide*.



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

- Do not install Cisco Unified Communications Manager in a large Class A or Class B subnet that contains a large number of devices. When you install Cisco Unified Communications Manager in a large subnet with a large number of devices in that subnet, the Address Resolution Protocol (ARP) table can fill up quickly (maximum 1024 entries, by default). When the ARP table gets full, Cisco Unified Communications Manager can have difficulty talking to endpoints and cannot add more phones.



Caution

Failure to deactivate the Cisco Extension Mobility service could cause the upgrade to fail.

- Before you upgrade to a later release, refer to the documentation for your currently installed COP files to identify any special considerations related to upgrading Cisco Unified Communications Manager.



Note If you have the Nokia s60 COP file installed, you must install any newer version of it before you upgrade Cisco Unified Communications Manager.

- If you plan to use IPv6 with Cisco Unified Communications Manager Release 7.1(2), you can provision your DNS server for IPv6 prior to upgrading to Release 7.1(2). However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you upgrade to Release 7.1(2).



Caution

Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 7.1(2) causes the upgrade to fail.

- To preserve system stability during upgrades, the system throttles the upgrade process, which may take considerably longer to complete in Cisco Unified Communications Manager Release 7.0 and later than it did in earlier releases.



Caution

Although disabling throttling decreases the time it takes to perform the upgrade, it may degrade system performance. For more information about throttling and the causes of slow upgrades, see the [“Effects of I/O Throttling” section on page 7-9](#).

To disable throttling, use one of the following methods before you start the upgrade:

- In Cisco Unified Operating System Administration, choose **Software Upgrades > Install/Upgrade**, and check the **Disable I/O throttling** check box.
- In the CLI, use the following command:
utils iothrottle disable



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

- After you complete the pre-upgrade tasks, review with the [“Software Upgrade Considerations” section on page 7-3](#).

Software Upgrade Considerations

This section contains the following topics:

- [Overview of the Software Upgrade Process, page 7-3](#)
- [Making Configuration Changes During an Upgrade, page 7-4](#)
- [Upgrading a Cluster in Parallel, page 7-5](#)
- [Supported Upgrades, page 7-6](#)
- [Upgrading to Cisco Unified Communications Manager Release 6.0\(1\) or Higher from a Release Prior to Release 6.0\(1\), page 7-6](#)
- [Upgrading to Cisco Unified Communications Manager Release 7.0\(1\) or Higher from a Release Prior to Release 6.0\(1\), page 7-7](#)
- [Upgrading from Cisco Unified Communications Manager Release 5.1\(3e\) to 7.1.x Releases, page 7-7](#)
- [Partition Size Limitations When You Upgrade from a 5.x Release to a 7.x Release, page 7-7](#)
- [Obtaining the Upgrade File, page 7-8](#)
- [Supported SFTP Servers, page 7-8](#)
- [Effects of I/O Throttling, page 7-9](#)

Overview of the Software Upgrade Process

With this version of Cisco Unified Communications Manager, you can install upgrade software on your server while the system continues to operate. Two partitions exist on your system: an active, bootable partition and an inactive, bootable partition. The system boots up and operates entirely on the partition that is marked as the active partition.



Note

If you have users logging in and logging out of Cisco Extension Mobility, this could cause the upgrade to fail. Before starting the upgrade, you must disable the Cisco Extension Mobility service. For more information, see the [“Pre-Upgrade Tasks” section on page 7-1](#).

When you install upgrade software, you install the software on the inactive partition. The system continues to function normally while you are installing the software. When you are ready, you activate the inactive partition and reboot the system with the new upgrade software. The current active partition will then get identified as the inactive partition when the system restarts. The current software remains in the inactive partition until the next upgrade. Your configuration information migrates automatically to the upgraded version in the active partition.

When you upgrade a cluster, you start by upgrading the first node. You can begin upgrading subsequent nodes in parallel after the first node reaches a specified point in the upgrade, as described in the [“Upgrading a Cluster in Parallel” section on page 7-5](#).

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

If 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 get lost.

**Note**

You can only make changes to the database on the active partition. The database on the inactive partition does not get updated. If you make changes to the database after an upgrade, you must repeat those changes after switching the partition.

If the upgrade of a subsequent node fails after you upgrade the first node and switch it to the new version or fail to upgrade one of the subsequent nodes in your cluster during the upgrade cycle, you can do one of the following:

- Correct the errors that caused the upgrade failure on the subsequent node. You may want to check the network connectivity of the nodes in your cluster, reboot the subsequent node, ensure the server memory and CPU usage on the subsequent node is not too high. Upgrade the subsequent node again.
- Make sure that the active partition of the first node runs the newest version of software installed on the server. Perform a fresh installation on the subsequent node using the same software version as that running on the active partition of the first node. If you are reinstalling the subsequent node, you should delete the server from Cisco Unified Communications Manager Administration and add the server again as described in the Cisco Unified Communications Manager Administration Guide.
- Revert the first node and all subsequent nodes to the previous version as described in the [Reverting to a Previous Version, page 7-15](#), install a previous version on the subsequent nodes, upgrade the first node again to the new version (not revert), and upgrade the subsequent nodes to the new version. If you attempt to revert the first node to the new version rather than upgrade again to the new version, the databases will not synchronize and synchronization cannot be repaired.

You can install a patch or upgrade version from a DVD (local source) or from a network location (remote source) that the Cisco Unified Communications Manager server can access.

**Note**

Be sure to back up your system data before starting the software upgrade process. For more information, see the *Disaster Recovery System Administration Guide*.

Making Configuration Changes During an Upgrade

This section describes the restrictions that apply to the configuration and provisioning changes that you can make during an upgrade.

Administration Changes

The administrator must not make any configuration changes to Cisco Unified Communications Manager during an upgrade. Configuration changes include any changes that you make in Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, and the User Option windows.

Any configuration changes that you make during an upgrade could get lost after the upgrade completes, and some configuration changes can cause the upgrade to fail.

For Cisco Unified Communications Manager Release 7.1(2), this restriction applies to upgrades from 4.x, 5.x, and 6.x releases.

For upgrades from Cisco Unified Communications Manager Release 4.x, you must discontinue all configuration activity before you run the Data Migration Assistant (DMA).

For upgrades from Cisco Unified Communications Manager Release 5.x and 6.x, you must discontinue all configuration activity before you upgrade to the new release by using either Cisco Unified Communications Operating System Administration or the Command Line Interface.

User Provisioning

For upgrades from Cisco Unified Communications Manager Release 4.x and 5.x, any provisioning that the end user performs to user-facing features after the upgrade begins could get lost.

For upgrades from Cisco Unified Communications Manager Release 6.x, changes that are made to the following user-facing features get preserved after the upgrade completes:

- Call Forward All (CFA)
- Message Waiting Indication (MWI)
- Privacy Enable/Disable
- Do Not Disturb Enable/Disable (DND)
- Extension Mobility Login (EM)
- Hunt Group Logout
- Device Mobility
- CTI CAPF status for end users and application users
- Credential hacking and authentication
- Recording enabling
- Single Number Reach enabling

Upgrading a Cluster in Parallel

When you upgrade a cluster that is running a supported version of Cisco Unified Communications Manager 5.x or 6.x to Cisco Unified Communications Manager 7.1(2), begin upgrading the first node first. You can begin upgrading subsequent nodes in parallel after the first node reaches a specified point in the upgrade.

During the upgrade of the first node, view the installation log, `install_log_<date+time>.log`, by using the Software Installation/Upgrade window in Cisco Unified Communications Operating System Administration or the command line interface (CLI). You can begin the upgrade of the subsequent nodes after the following information displays in the log:

```
PRODUCT_TARGET is <product target id>
```

PRODUCT_NAME is <product name>

PRODUCT_VERSION is <product version to which you are upgrading, such as 7.1(2)>

You can also use the CLI to search for the relevant information in the install log by following this procedure:

Procedure

Step 1 List the install logs; for example:

```
file list install install_* date

install_log_2008-10-01.09.41.57.log      install_log_2008-10-08.12.59.29.log
install_log_2008-10-14.09.31.06.log
dir count = 0, file count = 3
```

Step 2 Search the most recent install log for the string PRODUCT_VERSION; for example:

```
file search install install_log_2008-10-14.09.31.06.log PRODUCT_VERSION

Searching path: /var/log/install/install_log_2008-10-14.09.31.06.log
Searching file: /var/log/install/install_log_2008-10-14.09.31.06.log
10/14/2008 09:52:14 upgrade_os.sh|PRODUCT_VERSION is 7.1.0.39000-97|<LVL::Info>

Search completed
```

Step 3 When the **file search** command finds the PRODUCT_VERSION string in the install log, you can start the upgrade of the subsequent nodes.



Caution

If you want to upgrade the subsequent nodes in parallel with the first node, do not choose the Reboot to upgraded partition on either first node or subsequent nodes while configuring the upgrade options. If selected, the first node may complete its upgrade and reboot while the subsequent nodes are upgrading, which causes the upgrade of the subsequent nodes to fail.

When you are ready to activate the new version, you must activate the new software on the first node before activating it on all other nodes.

Supported Upgrades

For information about supported upgrades, see the Release Notes for your product release and the Cisco Unified Communications Manager Compatibility Matrix at the following URL:

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

Upgrading to Cisco Unified Communications Manager Release 6.0(1) or Higher from a Release Prior to Release 6.0(1)

Starting with Cisco Unified Communications Manager Release 6.0(1), CAPF uses the Certificate Manager Infrastructure to manage its certificates and keys. Because of this, when you upgrade to Release 6.0(1) or higher from any release prior to 6.0(1), CAPF keys and certificates automatically get

regenerated. You must then rerun the CTL Client application to upgrade the CTL file. For information on using CAPF with Cisco Unified Communications Manager, refer to the *Cisco Unified Communications Manager Security Guide*.

Obtain licenses for your release of Cisco Unified Communications Manager before upgrading to the newer release. You must import your new licenses after you upgrade to enable the system. Refer to *Cisco Unified Communications Manager Administration Guide* for information about licensing and obtaining licenses.

Upgrading to Cisco Unified Communications Manager Release 7.0(1) or Higher from a Release Prior to Release 6.0(1)

If you upgrade from a Cisco Unified Communications Manager release prior to release 6.0(1) to release 7.0(1) or higher, the /spare partition does not get created on the server. If you upgrade from release 6.0(1) or higher to release 7.0(1) or higher, or perform a fresh installation of release 7.0(1) or higher, the /spare partition gets created.

The /spare partition increases the efficiency of CTI Monitor tracing on the server.

Upgrading from Cisco Unified Communications Manager Release 5.1(3e) to 7.1.x Releases

This information applies when you upgrade from any of the following releases to to any 7.1.x release:

- 5.1(3e) (5.1.3.6000-2)
- The following 5.1(3e) Engineering Special releases:
 - 5.1(3.6103-1)
 - 5.1(3.6102-1)
 - 5.1(3.6101-1)

Before you upgrade, you must install the COP file `ciscocm.513e_upgrade.cop.sgn` on the server. This COP file is available from the following URL:

<http://tools.cisco.com/support/downloads/go/ImageList.x?relVer=COP-Files&mdfid=280735907&sftType=Unified+Communications+Manager%2FCallManager+Utilities&optPlat=&nodecount=2&edesignator=null&modelName=Cisco+Unified+Communications+Manager+Version+5.1&treeMdfId>

For information about installing this COP file, follow the installation instructions included with the COP file.

Partition Size Limitations When You Upgrade from a 5.x Release to a 7.x Release

Cisco Unified Communications Manager 5.x releases create disk partitions of a fixed size. If you install a 5.x release on a server with more disk space than required by the fixed partitions, the partitions still get created at the fixed size.

When you upgrade such a server from a 5.x release to a 7.x release, the disk partitions remain at the fixed size. If you perform a fresh installation of a 7.x release, the disk partitions get created as percentages of the available disk space, so your server will use all the available disk space effectively.

Obtaining the Upgrade File

Before you begin the upgrade process, you must obtain the appropriate upgrade file from Cisco.com. If you are performing a major upgrade, that is an upgrade between release trains, such as an upgrade between 6.01(1) to 7.0(1), you must obtain a DVD by using the Product Upgrade Tool (PUT) or by purchasing the upgrade from Cisco Sales.

To use the PUT, go to <https://tools.cisco.com/gct/Upgrade/jsp/index.jsp>. You must enter your Cisco contract number (Smartnet, SASU or ESW) and request the DVD/DVD set. If you do not have a contract for Cisco Unified Communications Manager, you must purchase the upgrade from Cisco Sales.

If you are performing a minor upgrade, that is an upgrade within the release train, such as an upgrade from 7.0(1) to 7.1(2), you can also access the upgrade file on Cisco.com.

Upgrading From Supported Cisco Unified Communications Manager 5.1(x) Releases

If you are upgrading from Cisco Unified Communications Manager release 5.1(3), the upgrade requires a set of files called a patch set. These files exist on the a Cisco-provided DVD in directory named cisco-ipt-k9-patchX.X.X.X-X, where X.X.X.X-X represents the release and build number.

**Note**

Do not rename the directory or files within it before you install it, because the system will not recognize them as a valid files.

Upgrading From Cisco Unified Communications Manager 6.x and 7.x

If you are upgrading from Cisco Unified Communications Manager Release 6.x or 7.x, the upgrade file name uses the following format:

```
UCSInstall_UCOS_X.X.X.X.X.sgn.iso
```

Where X.X.X.X-X represents the release and build number.

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

Supported SFTP Servers

Cisco allows you to use any SFTP server product but recommends SFTP products that have been certified with Cisco through the Cisco Technology Developer Partner program (CTDP). CTDP partners, such as GlobalSCAPE, certify their products with specified versions of Cisco Unified Communications Manager. For information on which vendors have certified their products with your version of Cisco Unified Communications Manager, refer to the following URL:

<http://www.cisco.com/cgi-bin/ctdp/Search.pl>

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://sshtwindows.sourceforge.net/>)
- Cygwin (refer to <http://www.cygwin.com/>)

- Titan (refer to <http://www.titanftp.com/>)

**Note**

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

Effects of I/O Throttling

This section describes how throttling affects the upgrade process, identifies possible causes of slow or stalled upgrades, and provides actions you can take to speed up the upgrade.

This section contains the following information:

- [Overview, page 7-9](#)
- [Disabling Throttling, page 7-9](#)
- [Server Models, page 7-9](#)
- [Write-Cache, page 7-9](#)

Overview

Throttling prevents call processing degradation during the upgrade but may cause the upgrade to take longer. Throttling gets enabled by default and is necessary if you perform the upgrade during normal business hours. Be aware that the higher the call processing load on the system during the upgrade, the longer the upgrade takes.

Disabling Throttling

To disable throttling, use one of the following methods before you start the upgrade:

- In Cisco Unified Operating System Administration, choose **Software Upgrades > Install/Upgrade**, and check the **Disable I/O throttling** check box.
- In the CLI, use the following command:
utils iothrottle disable

**Note**

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

Server Models

The Server model you have also impacts the upgrade speed. Upgrades on servers that have SATA hard drives, such as MCS-7816, MCS-7825, MCS-7828, take longer than servers with SAS/SCSI hard drives, such as MCS-7835 and MCS-7845.

Write-Cache

A disabled write-cache on the server also causes the upgrade process to run more slowly. Multiple factors can cause the write-cache to get disabled, including dead batteries on older servers.

Before starting an upgrade, verify the status of the write-cache on the MCS-7828-H4 and MCS-7835/45 disk controllers. You do not need to verify the write-cache status on the MCS-7816, MCS-7825, or other MCS-7828 servers. To verify write-cache status, access the Cisco Unified Operating System Administration, and choose **Show > Hardware**.

If you determine that your write-cache is disabled because of a dead battery, you need to replace the hard disk controller cache battery. Follow your local support procedures to get this battery replaced.

See the following examples of output from the **Show > Hardware** menu for details on determining the battery and write-back cache status.

The following example shows write-cache enabled. The example indicates that 50 percent of the cache is reserved for write and 50 percent of the cache is reserved for read. If the write-cache was disabled, 100 percent of the cache would be reserved for read or the Cache Status would not equal "OK". Also, the battery count equals "1". If the controller battery was dead or missing, it would indicate "0".

Example 7-1 7835/45-H1, 7835/45-H2, 7828-H4 Servers with Write-Cache Enabled

```

-----
RAID Details      :

Smart Array 6i in Slot 0
  Bus Interface: PCI
  Slot: 0
  Cache Serial Number: P75B20C9SR642P
  RAID 6 (ADG) Status: Disabled
  Controller Status: OK
  Chassis Slot:
  Hardware Revision: Rev B
  Firmware Version: 2.80
  Rebuild Priority: Low
  Expand Priority: Low
  Surface Scan Delay: 15 sec
  Cache Board Present: True
  Cache Status: OK
  Accelerator Ratio: 50% Read / 50% Write
  Total Cache Size: 192 MB
  Battery Pack Count: 1
  Battery Status: OK
  SATA NCQ Supported: False

```

The following example indicates that the battery status is enabled and that the write-cache mode is enabled in (write-back) mode.

Example 7-2 7835/45-I2 Servers with Write-Cache Enabled

```

-----
RAID Details      :
Controllers found: 1

-----
Controller information
-----
Controller Status      : Okay
Channel description    : SAS/SATA
Controller Model       : IBM ServeRAID 8k
Controller Serial Number : 20ee0001
Physical Slot          : 0
Copyback               : Disabled
Data scrubbing         : Enabled

```

```

Defunct disk drive count          : 0
Logical drives/Offline/Critical  : 2/0/0
-----
Controller Version Information
-----
BIOS                             : 5.2-0 (15421)
Firmware                         : 5.2-0 (15421)
Driver                          : 1.1-5 (2412)
Boot Flash                       : 5.1-0 (15421)
-----
Controller Battery Information
-----
Status                        : Okay
Over temperature                 : No
Capacity remaining              : 100 percent
Time remaining (at current draw) : 4 days, 18 hours, 40 minutes
-----
Controller Vital Product Data
-----
VPD Assigned#                   : 25R8075
EC Version#                     : J85096
Controller FRU#                 : 25R8076
Battery FRU#                    : 25R8088
-----
Logical drive information
-----
Logical drive number 1
  Logical drive name             : Logical Drive 1
  RAID level                     : 1
  Status of logical drive       : Okay
  Size                           : 69900 MB
  Read-cache mode               : Enabled
  Write-cache mode              : Enabled (write-back)
  Write-cache setting           : Enabled (write-back) when protected by battery
  Number of chunks              : 2
  Drive(s) (Channel,Device)     : 0,0 0,1
Logical drive number 2
  Logical drive name             : Logical Drive 2
  RAID level                     : 1
  Status of logical drive       : Okay
  Size                           : 69900 MB
  Read-cache mode               : Enabled
  Write-cache mode              : Enabled (write-back)
  Write-cache setting           : Enabled (write-back) when protected by battery
  Number of chunks              : 2
  Drive(s) (Channel,Device)     : 0,2 0,3

```

Software Upgrade Procedures

This section provides procedures for upgrading from either a local or a remote source and contains the following topics:

- [Upgrading from a Local Source, page 7-12](#)
- [Upgrading from a Remote Source, page 7-13](#)

Upgrading from a Local Source

To upgrade the software from local DVD, follow this procedure:

Procedure

-
- Step 1** If you do not have a Cisco-provided upgrade disk, create an upgrade disk by burning the upgrade file that you downloaded onto a DVD as an ISO image.



Note Just copying the .iso file to the DVD will not work. Most commercial disk burning applications can create ISO image disks.

- Step 2** Insert the new DVD into the disc drive on the local server that is to be upgraded.

- Step 3** Log in to Cisco Unified Communications Operating System Administration.

- Step 4** Navigate to **Software Upgrades > Install/Upgrade**.

The Software Installation/Upgrade window displays.

- Step 5** From the **Source** list, choose **DVD**.

- Step 6** Enter a slash (/) in the Directory field.

- Step 7** To disable throttling, check the **Disable I/O throttling** check box.



Caution Although disabling throttling decreases the time it takes to perform the upgrade, it may degrade system performance. For more information about throttling and the causes of slow upgrades, see the [“Effects of I/O Throttling” section on page 7-9](#).

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

- Step 8** To continue the upgrade process, click **Next**.

- Step 9** Choose the upgrade version that you want to install and click **Next**.

- Step 10** In the next window, monitor the progress of the download.

- Step 11** If you want to install the upgrade and automatically reboot to the upgraded partition, choose **Reboot to upgraded partition**. The system restarts and is running the upgraded software.

- Step 12** If you want to install the upgrade and then manually reboot to the upgraded partition at a later time, do the following steps:

- a. Choose **Do not reboot after upgrade**.
- b. Click **Next**.

The Upgrade Status window displays the Upgrade log.

- c. When the installation completes, click **Finish**.
- d. To restart the system and activate the upgrade, choose **Settings > Version**; then, click **Switch Version**.

The system restarts running the upgraded software.


Upgrading from a Remote Source

To upgrade the software from a network location or remote server, use the following procedure.

**Note**

Do not use the browser controls, such as Refresh/Reload, while you are accessing Cisco Unified Operating System Administration. Instead, use the navigation controls that are provided by the interface.

Procedure

- Step 1** Put the upgrade file on an FTP or SFTP server that the server that you are upgrading can access.
- If you are upgrading from release a supported 5.1(x) release, the upgrade requires a set of files, called a patch set. Put the patch set files on the FTP or SFTP server by using one of these methods:
- If you have a Cisco-provided upgrade disk, copy the contents of the disk to the remote server.
 - If you downloaded the upgrade files, copy the files you downloaded to the remote server.
- Step 2** Log in to Cisco Unified Communications Operating System Administration.
- Step 3** Navigate to **Software Upgrades > Install/Upgrade**.
- The Software Installation/Upgrade window displays.
- Step 4** From the **Source** list, choose **Remote Filesystem**.
- Step 5** In the **Directory** field, enter the path to the directory that contains the patch file on the remote system.
- 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. 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, remember that you are connecting to an FTP or SFTP server, so use the appropriate syntax, including
- Begin the path with a forward slash (/) and use forward slashes throughout the path.
 - The path must start from the FTP or SFTP root directory on the server, so you cannot enter a Windows absolute path, which starts with a drive letter (for example, C:).
- Step 6** In the **Server** field, enter the server name or IP address.
- Step 7** In the **User Name** field, enter your user name on the remote server.
- Step 8** In the **User Password** field, enter your password on the remote server.
- Step 9** Select the transfer protocol from the **Transfer Protocol** field.
- Step 10** To disable throttling, check the **Disable I/O throttling** check box.
- 
- Caution** Although disabling throttling decreases the time it takes to perform the upgrade, it may degrade system performance. For more information about throttling and the causes of slow upgrades, see the [“Effects of I/O Throttling” section on page 7-9](#).
- If you want to reenble throttling after you start the upgrade, you must cancel the upgrade, reenble throttling, and then restart the upgrade.
- Step 11** To continue the upgrade process, click **Next**.
- Step 12** Choose the upgrade version that you want to install and click **Next**.

- If you are upgrading from Cisco Unified Communications Manager Release 5.1(x), the upgrade requires a set of files that are called a patch set. Choose the upgrade version to install from the list. The upgrade version name does not include any file extensions, because it represents a patch set.
- If you are upgrading from Cisco Unified Communications Manager Release 6.x or 7.x, the upgrade file has the extension `sgn.iso`.

Step 13 In the next window, monitor the progress of the download.



Note If you lose your connection with the server or close your browser during the upgrade process, you may see the following message when you try to access the Software Upgrades menu again:

Warning: Another session is installing software, click Assume Control to take over the installation.

If you are sure you want to take over the session, click **Assume Control**.

If Assume Control does not display, you can also monitor the upgrade with the Real Time Monitoring Tool.

Step 14 If you want to install the upgrade and automatically reboot to the upgraded partition, choose **Reboot to upgraded partition**. The system restarts and runs the upgraded software.

Step 15 If you want to install the upgrade and then manually reboot to the upgraded partition at a later time, do the following steps:

- Choose **Do not reboot after upgrade**.
- Click **Next**.
The Upgrade Status window displays the Upgrade log.
- When the installation completes, click **Finish**.
- To restart the system and activate the upgrade, choose **Settings > Version**; then, click **Switch Version**.

The system restarts and is running the upgraded software.

Post-Upgrade Tasks

After the upgrade, perform the following tasks:

- Enable the Cisco Extension Mobility service by navigating to **Cisco Unified Serviceability > Tools > Service Activation**. For more information, see the *Cisco Unified Serviceability Administration Guide*.



Note If you do not enable the Cisco Extension Mobility service, Cisco Extension Mobility users cannot log in and log out of phones that support Cisco Extension Mobility.

- 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
- If necessary, reinstall the Real Time Monitoring Tool.

Stalled Upgrades

During the installation of upgrade software, the upgrade may seem to stall. The upgrade log stops displaying new log messages. When the upgrade stalls, you must cancel the upgrade, disable I/O throttling, and restart the upgrade procedure. For more information, see the [“Effects of I/O Throttling” section on page 7-9](#).

Reverting to a Previous Version

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

This section contains the following topics:

- [Reverting a Cluster to a Previous Version, page 7-15](#)
- [Reverting the Publisher Node to a Previous Version, page 7-16](#)
- [Reverting a Subscriber Node to a Previous Version, page 7-17](#)
- [Resetting Database Replication When Reverting to an Older Product Release, page 7-17](#)

Reverting a Cluster to a Previous Version

To revert a cluster to a previous version, follow these major steps:

	Task	For Additional Information
Step 1	Revert the publisher node.	“Reverting the Publisher Node to a Previous Version” section on page 7-16.
Step 2	Revert all backup subscriber nodes.	“Reverting a Subscriber Node to a Previous Version” section on page 7-17
Step 3	Revert all primary subscriber nodes.	“Reverting a Subscriber Node to a Previous Version” section on page 7-17
Step 4	If you are reverting to an older product release, reset database replication within the cluster.	“Resetting Database Replication When Reverting to an Older Product Release” section on page 7-17

Reverting the Publisher Node to a Previous Version

Procedure

-
- Step 1** Open Cisco Unified Communications Operating System Administration directly by entering the following URL:
- https://server-name/cmplatform**
- where *server-name* specifies the host name or IP address of the Cisco Unified Communications Manager server.
- Step 2** Enter your Administrator user name and password.
- Step 3** Choose **Settings > Version**.
The Version Settings window displays.
- Step 4** 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 5** To verify that the version switch was successful, you can follow these steps:
- Log in to Open Cisco Unified Communications Operating System Administration again.
 - Choose **Settings > Version**.
The Version Settings window displays.
 - Verify that the correct product version is now running on the active partition.
 - Verify that all activated services are running.
 - Log in to Cisco Unified Communications Manager Administration by entering the following URL and entering your user name and password:
https://server-name/ccmadmin
 - Verify that you can log in and that your configuration data exists.
-

Reverting a Subscriber Node to a Previous Version

Procedure

- Step 1** Open Cisco Unified Communications Operating System Administration directly by entering the following URL:
- `https://server-name/cmplatform`**
- where *server-name* is the host name or IP address of the Cisco Unified Communications Manager server.
- Step 2** Enter your Administrator user name and password.
- Step 3** Choose **Settings > Version**.
- The Version Settings window displays.
- Step 4** 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 5** To verify that the version switch was successful, you can follow these steps:
- Log in to Open Cisco Unified Communications Operating System Administration again.
 - Choose **Settings > Version**.
 - The Version Settings window displays.
 - Verify that the correct product version is now running on the active partition.
 - Verify that all activated services are running.
-

Resetting Database Replication When Reverting to an Older Product Release

If you revert 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.

Installing COP Files, Dial Plans, and Locales

This section contains the following topics:

- [COP File Installation, page 7-18](#)
- [Dial Plan Installation, page 7-18](#)
- [Locale Installation, page 7-18](#)

COP File Installation

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

- Install the COP file on every server in a cluster.
- After you install a COP file, you must restart the server.

**Note**

You must restart Cisco Unified Communications Manager to ensure that configuration changes that are made during the COP file installation get written into the database. Cisco recommends that you perform this restart during an off-peak period.

Dial Plan Installation

You can install dial plan files from either a local or a remote source by using the same process that is described earlier in this chapter for installing software upgrades. See the [“Software Upgrade Procedures” section on page 7-11](#) for more information about this process.

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

Locale Installation

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

User Locales

User locale files provide translated text and voice prompts, if available, for phone displays, user applications, and user web pages in the locale that the user chooses. User-only locale installers exist on the web.

Network Locales

Network locale files provide country-specific phone tones and gateway tones, if available. Network-only locale installers exist on the web.

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

**Note**

The Cisco Media Convergence Server (MCS) or Cisco-approved, customer-provided server can support multiple locales. Installing multiple locale installers ensures that the user can choose from a multitude of locales.

Changes do not take effect until you reboot every server in the cluster. Cisco strongly recommends that you do not reboot the servers until you have installed all locales on all servers in the cluster. Minimize call-processing interruptions by rebooting the servers after regular business hours.

Installing Locales

You can install locale files from either a local or a remote source by using the same process that is described earlier in this chapter for installing software upgrades. See the “[Software Upgrade Procedures](#)” section on page 7-11 for more information about this process.



Note

To activate the newly installed locales, you must restart the server.

See the “[Cisco Unified Communications Manager Locale Files](#)” section on page 7-19 for information on the Cisco Unified Communications Manager locale files that you must install. You can install more than one locale before you restart the server.

Cisco Unified Communications Manager Locale Files

When you are installing Cisco Unified Communications Manager locales, you must install the following files:

- User Locale files—Contain language information for a specific language and country and use the following convention:

`cm-locale-language-country-version.cop`

- 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`

Error Messages

See [Table 7-1](#) for a description of the messages that can occur during Locale Installer activation. If an error occurs, you can view the messages in the installation log.

Table 7-1 *Locale Installer Error Messages and Descriptions*

Message	Description
[LOCALE] File not found: <language>_<country>_user_locale.csv, the user locale has not been added to the database.	This error occurs when the system cannot locate the CSV file, which contains user locale information to add to the database. This indicates an error with the build process.
[LOCALE] File not found: <country>_network_locale.csv, the network locale has not been added to the database.	This error occurs when the system cannot locate the CSV file, which contains network locale information to add to the database. This indicates an error with the build process.

Table 7-1 *Locale Installer Error Messages and Descriptions (continued)*

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

Supported Cisco Unified Communications Products

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

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

Managing 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 servers, 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:
- Click **Upload File**.
The Upload File dialog box opens.
 - To upload a file, click **Browse** and then choose the file that you want to upload.
 - To upload the file to a subdirectory of the `tftp` directory, enter the subdirectory in the **Directory** field.
 - To start the upload, click **Upload File**.
The Status area indicates when the file uploads successfully.
 - 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:
- 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.
 - 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 Solutions*.

Setting Up a Customized 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 Communications Manager Administration, and the command line interface.

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

Procedure

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

The Customized Logon Message window displays.

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

Step 3 Click **Upload File**.



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

The system displays the customized log-on message.

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

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