



# 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, install Cisco Unity Connection locales, 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 7-2](#)
- [Software Upgrade Procedures, page 7-9](#)
- [Post-Upgrade Tasks, page 7-13](#)
- [Stalled Upgrades, page 7-14](#)
- [Reverting to a Previous Version, page 7-14](#)
- [Installing COP Files, Dial Plans, and Locales, page 7-15](#)
- [Managing TFTP Server Files, page 7-17](#)
- [Setting Up a Customized Log-on Message, page 7-18](#)

## 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 Business Edition 5000, the release notes are located at [http://cisco.com/en/US/products/ps7273/prod\\_release\\_notes\\_list.html](http://cisco.com/en/US/products/ps7273/prod_release_notes_list.html)

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

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 8.0(2) or later, you can provision your DNS server for IPv6 prior to upgrading to Release 8.0(2) or later. However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you perform the upgrade.



**Caution**

Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 8.0(2) or later causes the upgrade to fail.

- Before you upgrade a cluster, execute the **utils network ipv6 ping** CLI command to verify IPv6 networking on the first node (publisher server) and subsequent nodes (subscriber servers). If IPv6 is configured incorrectly on the subsequent nodes, load detection may take 20 minutes.
- Before you perform the Cisco Unified Communications Manager upgrade, 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.
- After you complete the pre-upgrade tasks, review with the [“Software Upgrade Considerations” section on page 7-2](#).

## 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 7-3](#)
- [Obtaining the Upgrade File, page 7-5](#)
- [Supported SFTP Servers, page 7-6](#)
- [Effects of I/O Throttling, page 7-6](#)

## Overview of the Software Upgrade Process

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.

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.

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 Business Edition 5000 server can access.

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

**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 8.5(1), this restriction applies to upgrades from 6.x releases.

For upgrades from Cisco Unified Communications Manager Release 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.

If you are upgrading your system, you must complete the upgrade tasks in this section before you perform any configuration tasks.

**Caution**

---

If you fail to follow these recommendations, unexpected behavior may occur; for example, ports may not initialize as expected.

---

## Upgrade Tasks

To successfully complete the upgrade, perform the upgrade tasks in the following order before you begin making configuration changes.

**Note**

---

Cisco strongly recommends that you do not perform configuration tasks until the upgrade completes on all servers in the cluster, until you have switched the servers over to the upgraded partition, and until you have verified that database replication is functioning.

---

### Procedure

- 
- Step 1** Stop all configuration tasks; that is, do not perform configuration tasks in the various Cisco Unified Communications Manager-related GUIs or the CLI (with the exception of performing the upgrade in the Cisco Unified Communications Operating System GUI).
  - Step 2** Upgrade the first node in the cluster (the publisher node).
  - Step 3** Upgrade the subsequent nodes in the cluster (the subscriber nodes).
  - Step 4** Switch over the first node to the upgraded partition.
  - Step 5** Switch over subsequent nodes to the upgraded partition.

**Note**

---

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

---

- Step 6** Ensure that database replication is functioning between the first node and the subsequent nodes. You can check database replication status by using one of the following methods:

- In Cisco Unified Reporting, access the Unified CM Database Status report. Before you proceed, ensure the report indicates that you have a good database replication status with no errors. For more information about using Cisco Unified Reporting, see the *Cisco Unified Reporting Administration Guide*.
- In the Cisco Real Time Monitoring Tool, access the Database Summary service under the CallManager tab to monitor database replication status. The following list indicates the database replication status progress:
  - 0—Initializing.
  - 1—Replication setup script fired from this node.
  - 2—Good replication.
  - 3—Bad replication.
  - 4—Replication setup did not succeed.

Before you proceed, ensure that you have a good database replication status. For more information about using the Real Time Monitoring Tool, see the *Cisco Unified Cisco Unified Real Time Monitoring Tool Administration Guide*.

**Step 7** When all other upgrade tasks are complete, you can perform any needed configuration tasks as required.

---

## User Provisioning

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

## Obtaining the Upgrade File

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

For more information, see the “Installation and Upgrade Information” section of the applicable Cisco Unified Communications Manager Business Edition 5000 release notes at [http://www.cisco.com/en/US/products/ps7273/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps7273/prod_release_notes_list.html).

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). CTDTP 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/pcgi-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/>)

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

**Note**

---

For issues with third-party products that have not been certified through the CTDTP 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 7-6](#)
- [Server Models, page 7-7](#)
- [Write-Cache, page 7-7](#)

### 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.

## Server Models

The server model you have 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 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 Communications 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 Software or Installing Locales from a Local Source, page 7-9](#)
- [Upgrading Software or Installing Locales from a Remote Source, page 7-10](#)
- [Bridge Upgrade, page 7-12](#)

## Upgrading Software or Installing Locales from a Local Source

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

### Procedure

- 
- Step 1** If you are upgrading Cisco Unified Communications Manager Business Edition 5000, skip to [Step 2](#). If you are adding a Cisco Unity Connection locale, stop the Connection Conversation Manager and Connection Mixer services:
- a. Start Cisco Unity Connection Serviceability.
  - b. Navigate to **Tools > Control Center - Feature Services**.
  - c. Under Critical Services, in the Connection Conversation Manager row, click **Stop**.
  - d. Wait for the service to stop.
  - e. Also under Critical Services, in the Connection Mixer row, click **Stop**.
  - f. Wait for the service to stop.
- 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 continue the upgrade process, click **Next**.
- Step 8** Choose the upgrade version that you want to install and click **Next**.
- Step 9** In the next window, monitor the progress of the download.
- Step 10** If you are upgrading Cisco Unified Communications Manager Business Edition 5000, skip to [Step 11](#). If you are installing Cisco Unity Connection locales and want to install another locale, click **Install Another**, and return to [Step 4](#).  
If you do not want to install another locale, restart the Connection Conversation Manager and Connection Mixer services:
- a. Start Cisco Unity Connection Serviceability.
  - b. Navigate to **Tools > Control Center - Feature Services**.
  - c. Under Critical Services, in the Connection Conversation Manager row, click **Start**.

- d. Wait for the service to start.
  - e. Also under Critical Services, in the Connection Mixer row, click **Start**.
  - f. Wait for the service to start.
  - g. Skip the rest of the procedure.
- 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 Software or Installing Locales 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 Communications 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.
- Step 2** If you are upgrading Cisco Unified Communications Manager Business Edition 5000, skip to [Step 3](#).  
If you are adding a Cisco Unity Connection locale, stop the Connection Conversation Manager and Connection Mixer services:
- a. Start Cisco Unity Connection Serviceability.
  - b. Navigate to **Tools > Control Center - Feature Services**.
  - c. Under Critical Services, in the Connection Conversation Manager row, click **Stop**.
  - d. Wait for the service to stop.
  - e. Also under Critical Services, in the Connection Mixer row, click **Stop**.
  - f. Wait for the service to stop.
- 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 **Remote Filesystem**.
- Step 6** 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 7** In the **Server** field, enter the server name or IP address.
- Step 8** In the **User Name** field, enter your user name on the remote server.
- Step 9** In the **User Password** field, enter your password on the remote server.
- Step 10** Select the transfer protocol from the **Transfer Protocol** field.
- Step 11** To continue the upgrade process, click **Next**.
- Step 12** Choose the upgrade version that you want to install and click **Next**.
- 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 are installing upgrade software, skip to [Step 15](#).  
If you are installing Cisco Unity Connection locales and want to install another locale, click **Install Another**, and return to [Step 4](#).  
If you do not want to install another locale, restart the Connection Conversation Manager and Connection Mixer services:
- a. Start Cisco Unity Connection Serviceability.
  - b. Navigate to **Tools > Control Center - Feature Services**.
  - c. Under Critical Services, in the Connection Conversation Manager row, click **Start**.
  - d. Wait for the service to start.
  - e. Also under Critical Services, in the Connection Mixer row, click **Start**.
  - f. Wait for the service to start.
  - g. Skip the rest of the procedure.
- Step 15** 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 16** 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 and is running the upgraded software.

---

## Bridge Upgrade

The bridge upgrade provides a migration path for customers who want to migrate from discontinued Cisco Unified Communications Manager server to a server that supports the newest release of Cisco Unified Communications Manager.

Servers that are no longer supported, but are permitted to function as bridge upgrade servers, can upgrade and boot but will not allow Cisco Unified Communications Manager to function.

When you attempt to upgrade your Cisco Unified Communications Manager version on a discontinued server model, Cisco Unified Communications Manager inserts a message into the upgrade log. The upgrade log is displayed on the web browser when the upgrade is initiated through the Cisco Unified Communications Operating System Administration window, or you can view it through CLI if you used CLI to perform the upgrade. This message notes that you can only use the new version to obtain a DRS backup. The warning message in the log is followed by a delay that allows you to cancel the upgrade if you do not want to do a bridge upgrade.

When the system boots the new Cisco Unified Communications Manager version, a warning appears on the console that tells you that the only thing you can do with the new Cisco Unified Communications Manager version is to perform a DRS backup (“This hardware has limited functionality. Backup and Restore is the only supported functionality.”). Because of the restricted visibility of the console, the warning displays during both CLI and GUI sessions.

Use the following procedure to perform a bridge upgrade:

### Procedure

---

**Step 1** Perform an upgrade to the new Cisco Unified Communications Manager version on your discontinued first node (publisher) server. Refer to the preceding sections in this chapter that describe the kind of upgrade you want to do. Observe the warning on the console that tells you that the only thing you can do with the new Cisco Unified Communications Manager version is to perform a DRS backup (“This hardware has limited functionality. Backup and Restore is the only supported functionality.”).

**Step 2** Perform an upgrade to the new Cisco Unified Communications Manager version on your subsequent node (subscriber) servers. Refer to the preceding sections in this chapter that describe the kind of upgrade you want to do.

**Step 3** Verify database synchronization between all nodes. You can use the CLI commands `utils dbreplication runtimestate` and `utils dbreplication status`. For more information, refer to the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

- Step 4** Using the new Cisco Unified Communications Manager version on your discontinued first node server, perform a DRS backup. The DRS backups are encrypted using the cluster security password provided at install time. You must remember this security password as the “old” password, because you may be prompted to enter this “old” password at the time of restore. Refer to the *Disaster Recovery System Administration Guide*.
- Step 5** Disconnect your discontinued server from the network.
- Step 6** Install the new Cisco Unified Communications Manager version on your new supported first node server. You must obtain and install a new license on this server. Refer to the guide *Installing Cisco Unified Communications Manager*. You will be prompted to enter a “new” security password, a password that is different from the “old” password you noted in [Step 4](#). The guide *Installing Cisco Unified Communications Manager* describes the requirements of a “new” security password that Cisco Unified Communications Manager will accept. You must remember this “new” security password.
- Step 7** Using the new Cisco Unified Communications Manager version on your new supported first node server, perform the *Disaster Recovery System Administration Guide* procedure “Restoring the First Node only (Rebuilding the Publisher Alone)”. First, select only select the first node for restore. You can only select the subsequent nodes for restore after the completion of first node restore. Use the discontinued server’s backup file that you created in [Step 4](#). You will be prompted for the “old” security password that you noted in [Step 4](#). For further details, refer to the *Disaster Recovery System Administration Guide*.
- Step 8** On your new supported first node server, reactivate all services that used to be active on your discontinued first node server before the bridge upgrade. Refer to the *Administration Guide for Cisco Unity Connection Serviceability*.
- Step 9** Verify database synchronization between all nodes. You can use the CLI commands `utils dbreplication runtimestate` and `utils dbreplication status`. For more information, refer to the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.
- 

## 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 7-6](#).

## 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.

### 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 Business Edition 5000 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:
- a. Log in to Open Cisco Unified Communications Operating System Administration again.

- 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. Log in to Cisco Unified Communications Manager Administration by entering the following URL and entering your user name and password:  
**`https://server-name/ccmadmin`**
  - f. Verify that you can log in and that your configuration data exists.
- 

## Installing COP Files, Dial Plans, and Locales

This section contains the following topics:

- [COP File Installation, page 7-15](#)
- [Dial Plan Installation, page 7-15](#)
- [Locale Installation, page 7-16](#)

### 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 7-9 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](http://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.

### Cisco Unity Connection Locales

Cisco Unity Connection locales (languages) provide country-specific system prompts, graphical user interface, and text-to-speech functionality. For information on downloading Cisco Unity Connection locales, see the “Installation and Upgrade Information” section of the applicable Cisco Unified Communications Manager Business Edition 5000 release notes at [http://www.cisco.com/en/US/products/ps7273/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps7273/prod_release_notes_list.html).



#### Caution

---

Do not install more than five Cisco Unity Connection locales.

---

## 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 7-9](#) 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 7-16](#) 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

## 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:

- 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*.

## 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, Cisco Unified Serviceability, Disaster Recovery System Administration, Cisco Unity Connection Administration, Cisco Unity Connection Serviceability Administration, Cisco Personal Communications Assistant (CPCA) 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.