Upgrading to Cisco Unified Communications Manager Release 7.1(2) from 4.x Releases

Published: May 13, 2009

Revised: July 23, 2009

This document describes how to upgrade to Cisco Unified Communications Manager 7.1(2) from a 4.x release.

For information about upgrading your Cisco Unified Communications Manager software after you have upgraded to release 5.0(1) or later, refer to*Cisco Unified Communications Operating System Administration Guide*.

For information about performing a fresh installation of Cisco Unified Communications Manager (rather then upgrading from an earlier release) or configuring Cisco Unified Communications Manager when it is preinstalled on your server, refer to *Installing Cisco Unified Communications Manager*.

The 7.1(2) release of Cisco Unified Communications Manager uses a different installation framework than releases of Cisco Unified Communications Manager prior to 5.0. Before upgrading to Cisco Unified Communications Manager 7.1(2), review all upgrade instructions carefully.

Contents

This document contains the following topics:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Installation Overview

Cisco Unified Communications Manager uses a different installation framework than previous releases. The installation process allows you to perform a basic installation, upgrade from Cisco Unified CallManager 4.x or Cisco Unified Communications Manager 4.x to Cisco Unified Communications Manager 7.1(2), and upgrade to a newer service release during the installation.

For a more detailed description of the different installation types, see Table 1.

Table 1 Installation Options

Installation Types	Description
Basic Install	This option represents the basic Cisco Unified Communications Manager 7.1(2) installation. It installs the software from the installation disc, does not use any imported data, and does not import any data.
Applying a Patch (upgrade during install)	This option allows you to upgrade the software version that the installation disc contains with the latest service release. You can also choose to apply a patch and then do a Windows upgrade, performing both during the installation process. You can choose to apply a patch and import Windows data during the installation. You need to apply the patch first and then import the Windows data.
Import Windows Data (Windows upgrade)	This option allows you to import database information from a 4.x system by using a file that the Data Migration Assistant (DMA) tool produces.

Note The document describes the procedure for performing a Windows Upgrade. For basic installation instructions, see *Installing Cisco Unified Communications Manager*.

Related Documentation

For further information about related Cisco IP telephony applications and products, refer to the *Cisco Unified Communications Manager Documentation Guide* at the following URL:

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

Table 2 lists URLs for software and additional documentation.

Table 2 Quick Reference for URLs

Related Information and Software	URL
Cisco MCS data sheets	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/index.html
Software-only servers (IBM, HP, Compaq, Aquarius)	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html
Cisco Unified Communications Manager service releases	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml

Important Considerations

Before you proceed with the Cisco Unified Communications Manager upgrade, consider the following requirements and recommendations:

- Ensure that you connect each Cisco Unified Communications Manager node to an uninterruptible power supply (UPS) to provide backup power and protect your system.

Caution Failure to connect the Cisco Unified Communication Manager nodes to a UPS may result in damage to physical media and require a new installation of Cisco Unified Communications Manager.

- Be aware that when you install Cisco Unified Communications Manager 7.1(2) on an existing server, the hard drive gets formatted, and all existing data on the drive gets overwritten.
- Be aware that all secure phones will remain down during the upgrade process.
- Install the Cisco Unified Communications Manager software on the first node, or publisher, server first and then on the subsequent nodes.

  Before you can install subsequent, or subscriber, nodes, you must first configure them on the first, or publisher, node.
- Enter the same security password on all servers in the cluster.
- 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.
- Install the Cisco Unified Communications Manager software during off-peak hours or a maintenance window to avoid impact from call-processing interruptions.
- Configure the server by using static IP addressing to ensure that the server obtains a fixed IP address and that the Cisco Unified IP Phones can register with the application when you plug the phones into the network.
- 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 devices in that subnet, the Address Resolution Protocol (ARP) table can fill up quickly (maximum 1024 entries, by default). When the ARP table is full, Cisco Unified Communications Manager can have difficulty talking to endpoints and cannot add more phones.
- You must have access to an SFTP server to back up Cisco Unified Communications Manager over a network.
- 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 version 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://sshwindows.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

- Do not attempt to perform any configuration tasks or make any other changes during the upgrade.
- Do not install any Cisco-verified applications until you complete installing Cisco Unified Communications Manager on every server in the cluster.
- Be aware that customer background images, custom TFTP files, custom MoH files, and customer ring tones do not get migrated during the upgrade process. You must reinstall these files after the upgrade completes. See the "Post-Upgrade Tasks" section on page 39 for more information.
- Be aware that end-user settings such as ring tones and background images do not get migrated during the upgrade process. The end user must reconfigure these items after the upgrade completes.
- Be aware that the demo license feature is not available when you upgrade from a previous product version.
- Be aware that directory names and filenames that you enter while running the installation program are case-sensitive.
- Disk mirroring on server model 7825 I3 with 160 GB SATA disk drives takes approximately 3 hours.
- Disk mirroring on server model 7828 I3 with 250 GB SATA disk drives takes approximately 4 hours.
- Administrators can connect third-party voice-messaging systems to Cisco Unified Communications Manager. Ensure the voice-messaging system has a simplified message desk interface (SMDI) that is accessible with a null-modem EIA/TIA-232 cable (and an available serial port). To connect the EIA/TIA-232 cable to Cisco Unified Communications Manager Release 5.0 or later, use a Cisco certified serial-to-USB adapter with the part number USB-SERIAL-CA=.
- Be aware that all users get added to the Standard CCM End Users Group after an upgrade from a 4.x release to Release 7.1(2). You must manually remove any users that you do not want in this group.
- Restrictions apply to the configuration and provisioning changes that you can make during an upgrade.

  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 CallManager Administration, Cisco Unified CallManager 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.

  You must discontinue all configuration activity before you run DMA.
- Cisco Unified Communications Manager has a system history log. The system history log provides a central location for getting a quick overview of the initial system install, system upgrades, Cisco option installations, DRS backups and DRS restores, as well as switch version and reboot history. See the "Troubleshooting Tools" section of the *Troubleshooting Guide* for more information.
- Carefully read the instructions that follow before you proceed with the installation.

Preparing To Upgrade

This section describes how to prepare to upgrade from Cisco Unified CallManager 4.x or Cisco Unified Communications Manager 4.x to Release 7.1(2).

Frequently Asked Questions About the Cisco Unified Communications Manager Installation

The following section contains information about commonly asked questions and responses. Review this section carefully before you complete the Cisco Unified Communications Manager installation.

From What Version Can I Upgrade to Cisco Unified Communications Manager 7.1(2)?

For information on supported upgrades, refer to the *Cisco Unified Communications Manager Software Compatibility Matrix* at the following URL:

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

What User Names and Passwords Do I Need to Specify?

Note The system checks your passwords for strength. For guidelines on creating a strong passwords, see the "What is a Strong Password?" section on page 6.

During the Cisco Unified Communications Manager upgrade, you must specify the following user names and passwords:

- Administrator user name and password
- Application user name and password
- Security password
- End user password and PIN

Administrator User Name and Password

You use the Administrator user name and password to log in to the following areas:

- Cisco Unified Communications Operating System Administration
- Disaster Recovery System
- Command Line Interface

To specify the Administrator user name and password, follow these guidelines:

- Administrator Account user name—The Administrator Account user name must start with an alphabetic character and can contain alphanumeric characters, hyphens, and underscores.
- Administrator Account password—The Administrator Account password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

You can change the Administrator Account password or add a new Administrator account by using the command line interface. For more information, see Table 5 in the "Gathering Information for an Installation" section on page 18 or the *Cisco Unified Communications Operating System Administration Guide*.

Application User Name and Password

You use the Application user name and password to access applications that are installed on the system, including the following areas:

- Cisco Unified Communications Manager Administration
- Cisco Unified Serviceability
- Cisco Cisco Unified Real-Time Monitoring Tool
- Cisco Unified Reporting

To specify the Application user name and password, follow these guidelines:

- Application User name—The Application User name must start with an alphabetic character and can contain alphanumeric characters, hyphens and underscores.
- Application User password—The Application User password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

You can change the Application User name and password by using the command line interface. For more information, see Table 5 in the "Gathering Information for an Installation" section on page 18 or the *Cisco Unified Communications Operating System Administration Guide*.

Security Password

The system uses this password to authorize communications between nodes, and you must ensure that this password is identical on all nodes in the cluster.

The Security password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

End User Password and PIN

The system uses this password and PIN to reset the password and PIN for all end users that were configured on the Windows-based Cisco Unified Communications Manager.

Note After you upgrade the system, you must inform all end users about this new default password and PIN, which they can then change to a password and PIN of their choosing.

What is a Strong Password?

The installation wizard checks to ensure that you enter a strong password. To create a strong password, follow these recommendations:

- Mix uppercase and lowercase letters.
- Mix letters and numbers.
- Include hyphens and underscores.
- Remember that longer passwords are stronger and more secure than shorter ones.

Avoid the following types of passwords:

- Do not use recognizable words, such as proper names and dictionary words, even when combined with numbers.
- Do not invert recognizable words.
- Do not use word or number patterns, like aaabbb, qwerty, zyxwvuts, 123321, and so on.
- Do not use recognizable words from other languages.
- Do not use personal information of any kind, including birthdays, postal codes, names of children or pets, and so on.

Which servers does Cisco support for this installation?

To find which servers support Cisco Unified Communications Manager 7.1(2), refer to the Cisco Unified Communications Manager Server Support Matrix at

http://www.cisco.com/en/US/partner/products/hw/voiceapp/ps378/prod_brochure_list.html

May I install other software besides Cisco Unified Communications Manager on the server?

You must do all software installations and upgrades by using Cisco Unified Communications Operating System Administration. The system can upload and process only software that Cisco Systems approved. You cannot install or use third-party or Windows-based software applications that you may have been using with a previous version of Cisco Unified Communications Manager with Cisco Unified Communications Manager 7.1(2).

Browser Requirements

You can access Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, Cisco Unified Reporting, Cisco Unified Communications Operating System Administration, and Disaster Recovery System by using the following browsers:

- Microsoft Internet Explorer version 6.x or version 7.x
- Netscape Navigator version 7.1 or later

Note Cisco does not support or test other browsers, such as Mozilla Firefox.

Configuring the Hardware

As a part of software installation, the system installer configures the system BIOS and RAID settings for the new operating system and Cisco Unified Communications Manager application. Usually you should not need to do more configuration to perform an upgrade, unless you encounter problems with the upgrade. See Table 3 for the BIOS settings and Table 4 for the RAID settings that are set up during installation.

Note If the hardware configuration process fails during installation, you can use boot-time utilities on both the IBM and HP servers to manually configure the RAID and BIOS settings, as shown in Table 3 and Table 4.

Table 3 BIOS Configuration Settings for HP and IBM Servers

HP Servers	IBM Servers
OS Selection: Linux (not applicable on newer models)	OS Selection: Not applicable
Boot order: CD, Disk (HDD), USB	Boot order: CD, Disk (HDD), USB
Post F1 prompt: Delayed	Post F1 prompt: Delayed
Hyperthreading: Enabled	Hyperthreading: Enabled

Table 4 RAID Settings

MCS 7825 Servers (HP and IBM)	MCS 7828 Servers (HP and IBM)	MCS 7835 Servers (HP and IBM)	MCS 7845 Servers (HP and IBM)
Logical drives: 1		Logical drives: 1	Logical drives: 2
Software RAID: HP 7825-H1, 7825-H2, 7825-H3, IBM 7825-I1, and 7825-I2 are configured with RAID type 1(1+0) Hardware RAID: HP 7825-H4, IBM 7825-I3, and 7825-I4 are RAID type 1(1+0)		RAID type: 1(1+0)	RAID type: 1(1+0)

Performing Pre-Upgrade Tasks

Before you perform the following tasks, use Data Migration Assistant to back up your existing system's data. Refer to the *Data Migration Assistant User Guide*.

Note Allow as much time as possible—preferably several weeks—between the completion of your Data Migration Assistant backup and the beginning of your upgrade to Cisco Unified Communications Manager Release 7.1(2).

Perform the following tasks before you begin the upgrade:

	Pre-Upgrade Task	Important Notes
Step 1	Verify that your servers meet the system requirements for upgrading Cisco Unified Communications Manager nodes in the cluster.	Refer to the following documentation for information about the capacity of server models: • Release notes for your product release • http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html Make sure to account for any growth that has occurred since initial system configuration.
Step 2	Ensure that you connect each Cisco Unified CallManager node to an uninterruptible power supply (UPS) to provide backup power and protect your system.	**Caution** Failure to connect the Cisco Unified CallManager nodes to a UPS may result in damage to physical media and require a new installation of Cisco Unified Communications Manager.
Step 3	Verify the integrity of any new server hardware (such as hard drives and memory) by running any manufacturer-provided utilities.	
Step 4	Make sure that you have a copy of all custom ring files, phone backgrounds, and music on hold sources.	Consider this as precautionary because the restore is designed to restore these items.
Step 5	Obtain and store files for any locales that are installed on the server.	You might need to reinstall locales after doing the upgrade.
Step 6	Do not add more nodes to the cluster or make any other configuration changes during the upgrade.	The upgrade may be unsuccessful if you try to add more nodes to the cluster or make any other configuration changes while the upgrade is in progress.
Step 7	Verify the integrity of your software downloads and DVDs.	Perform the following tasks: • Check the MD5 checksum of downloaded software against the published value to verify that it downloaded properly. • Verify that the DVD is readable by a DVD drive.
Step 8	Perform any system tests that you intend to perform after the replacement before the replacement also, to verify that the tests pass before you do the replacement.	Document these tests, so you can perform them identically after doing the replacement.

	Pre-Upgrade Task	Important Notes
Step 9	If you use DNS, verify that all servers to be replaced are configured in DNS properly. All nodes in the cluster must either use DNS or not use it.	See the "Verifying DNS Registration" section on page 13.
Step 10	If you are getting the system time from an NTP server, verify that the first node can synchronize with the NTP server before you install a subsequent node. To verify the NTP status of the first node, log into the Command Line Interface on the first node and enter the following command: **utils ntp status** **Note** To avoid potential compatibility, accuracy, and network jitter problems, the external NTP servers that you specify for the primary node should be NTP v4 (version 4). If you are usingIPv6 addressing, external NTP servers must be NTP v4.	For more information, see the *Cisco Unified Communications Operating System Administration Guide*. ⚠ **Caution** If the first node fails to synchronize with an NTP server, installation of a subsequent node can also fail.
Step 11	Do not run Network Address Translation (NAT) or Port Address Translation (PAT) between Cisco Unified CallManager nodes.	The upgrade may be unsuccessful if you run NAT or PAT between the nodes.
Step 12	Record all the registration information by using the Cisco Unified CallManager Cisco Unified Real-Time Monitoring Tool (RTMT).	See the "Determining Registration Counts by Using RTMT" section on page 13.
Step 13	Record all the critical services and their activation status by using the Cisco Unified CallManager Real-Time Monitoring Tool (RTMT).	See the "Recording Critical Service Status" section on page 14.
Step 14	Using the Syslog viewer in the Cisco Unified CallManager Cisco Unified Real-Time Monitoring Tool (RTMT), locate any events that have a severity of Error or higher.	Perform this task to ensure that no system-affecting errors exist on your system. See the "Locating System Errors by Using Syslog Viewer" section on page 14.
Step 15	Record the details of all Trace and Log Central jobs.	See the "Recording Trace and Log Central Job Details" section on page 15.
Step 16	Record CDR Management configuration and destinations, if applicable.	See the "Accessing CDR Management Configuration" section on page 15.
Step 17	From Cisco Unified CallManager Administration, determine the number of specific items that are configured on the server.	See the "Determining System Configuration Counts" section on page 16.
Step 18	From Cisco Unified CallManager, record all the phone loads and device types that display on the Firmware Load Information window.	See the "Firmware Information" section on page 17. If you have custom device types that do not ship with Cisco Unified CallManager, make sure that you have the appropriate files. You might need to reinstall the devices types after performing the replacement.
Step 19	If your cluster is running in secure mode, make sure that you have USB eToken devices and CTL Client plug-in utility installed on a computer that is running the Windows operating system.	For information about performing these tasks and about Cisco Unified Communications Manager security, refer to the "Installing the CTL Client" procedures in the *Cisco Unified Communications Manager Security Guide*.
Step 20	Run Cisco Unified CallManager Upgrade Utility on the server to verify that the system is ready for upgrade.	Refer to *Using Cisco Unified CallManager Upgrade Utility*.

	Pre-Upgrade Task	Important Notes
Step 21	Perform the recommended backup procedures on the publisher server. Back up every database that is associated with your Cisco Unified CallManager server. Store copies of the resulting backup files on a separate reliable high-performance computer that runs FTP or SFTP. Store copies of your DMA backup files on this computer also.	Refer to *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide*.
Step 22	If you are using a third-party application to access Call Detail Records (CDR), perform a backup of the CDR data as recommended in the third-party vendor documentation.	**Caution** Data Migration Assistant does not migrate CDR data except records that are in the CAR database. For more information on CAR, refer to the *CDR Analysis and Reporting Administration Guide* for the version of Cisco Unified CallManager running on your system.
Step 23	If you use Cisco Unified Call Manager CDR Analysis and Reporting, make sure that the latest CDRs exist in the CAR database by setting the CDR load schedule to run before you execute the Data Migration Assistant. DMA will not migrate any CDRs that are generated after you have run the loader.	For information on configuring the CAR load schedule before you upgrade, see the *CDR Analysis and Reporting Administration Guide* for the version of Cisco CallManager running on your system.
Step 24	If you do not need to carry over your CAR data to Cisco Unified Communications Manager 7.1(2), Cisco recommends that you purge the CAR data before you run DMA. For best system performance, you should purge any CAR records that are older than 180 days. As an alternative, you can choose not to include CAR data in your Data Migration Assistant backup. Refer to the *Data Migration Assistant User Guide*.	For more information about migrating CAR data, see the "Migrating CAR Data" section on page 18. For information on purging CAR data manually and configuring automatic database purging after you upgrade, refer to the *CDR Analysis and Reporting Administration Guide*. If you want to export the CAR database, you must choose to do so within the Data Migration Assistant. If you export CAR data, Data Migration Assistant allows you to specify the amount of time that you want to allot for CAR migration. For more information on exporting the CAR database, or other functions of the Data Migration Assistant, see the *Data Migration Assistant User Guide*.

	Pre-Upgrade Task	Important Notes
Step 25	Export the data on the current Cisco Unified Communications Manager publisher server by running the Data Migration Assistant (DMA). Ensure the configuration files and exported data files are located in one of the following locations: • Hard drive (for DMABackupInfo.inf only) • Floppy drive (for DMABackupInfo.inf only) • Tape drive • Remote drive	DMA generates three files—and an optional fourth file: • A tape archive (TAR) file that contains the database and directory information. The format of the filename follows: DMABackup<M>-<D>-<Y>#<H>-<mm>.tar where M specifies the month, D specifies the day, Y specifies the year, H specifies the hour in a 24-hour format, and mm specifies the minutes. • A configuration file, platformConfig.xml, to facilitate the installation of Cisco Unified Communications Manager first nodes. Users generate this file by entering site-specific data at DMA's Answer File Generator window • A backup information file that contains Cisco Unified Communications Manager configuration data, named DMABackupInfo.inf. The system saves it in the D:\DMA folder as part of the TAR file. **Note** Do not change the configuration data filename. The upgrade fails if it does not find a file with the exact filename and format. • (Optional) A license file, licupgrade.lic, that you can import into the publisher server after the upgrade. This option expedites your upgrade by making the license file available immediately, rather than requiring you to generate a license file by using the License Registration web tool that e-mails you the license file. For more information on data migration, refer to *Data Migration Assistant User Guide*. You will be choosing an installation option based on the location of the DMA output configuration file and TAR file.
Step 26	Before the upgrade, obtain the necessary information for configuring the platform and Cisco Unified CallManager on the first and subsequent nodes.	See the "Gathering Information for an Installation" section on page 18.
Step 27	Record the Host Name/IP Address value that is configured on the Server Configuration Settings window of the Cisco Unified Communications Manager 4.x server.	To access the Host Name/IP Address field on the 4.x server, navigate to **System > Server**. For more information, see the "Assigning the Host Name/IP Address (Servername) to the 7.1(2) Server" section on page 24
Step 28	Familiarize yourself with the navigation options within the installation wizards.	See "Navigating Within the Installation Wizard" section on page 26.

	Pre-Upgrade Task	Important Notes
Step 29	Make sure that you have the 7.1(2) installation DVD. Also if you plan to install a patch during the upgrade, ensure you have the patch file available on a DVD or SFTP or FTP server that the Cisco Unified Communications Manager nodes can access.	See the "Applying a Patch" section on page 30 for more information.
Step 30	Disable the Cisco Extension Mobility service.	Navigate to **Cisco Unified Serviceability > Tools > Service Activation**. For more information, see the *Cisco Unified CallManager Serviceability Administration Guide*. **Note** Be aware that when you deactivate the Cisco Extension Mobility service, Cisco Extension Mobility users will not be able to log in and log out of phones that support Cisco Extension Mobility. For users to be able to control their phones through Cisco Extension Mobility they must log out before the upgrade, then log in again after the upgrade.

Verifying DNS Registration

If you use DNS, verify that all servers to be upgraded are registered in DNS properly.

Procedure

Step 1 Open a command prompt.

Step 2 To ping each server by its DNS name, enter **ping <***DNS name***>**.

Step 3 To look up each server by IP address, enter **nslookup <***IP address***>**.

Related Topics

Performing Pre-Upgrade Tasks, page 9

Determining Registration Counts by Using RTMT

Record the number of registered devices, including the numbers of registered phones and gateways, by using the Cisco Unified Communications Manager Cisco Unified Real-Time Monitoring Tool (RTMT).

Procedure

Step 1 Download and install the Cisco Unified Communications Manager Cisco Unified Real-Time Monitoring Tool (RTMT) by choosing **Application > Plugins** from Cisco Unified Communications Manager Administration, clicking **Find**, and clicking the **Download** link next to the appropriate RTMT installer.

If you are planning to install the RTMT tool on a computer that is running the Microsoft Windows operating system, click the **Download** link for the Cisco Unified Communications Manager Cisco Unified Real-Time Monitoring Tool-Windows. If you are planning to install the RTMT tool on a computer that is running the Linux operating system, click the **Download** link for the Cisco Unified Communications Manager Cisco Unified Real-Time Monitoring Tool-Linux.

Step 2 Open RTMT.

Step 3 Perform one of the following tasks:

- In the Quick Launch Channel, click the **View** tab, click the **Device** category, and click the **Device** icon.
- Choose **Monitor > Device Summary**.

Step 4 For each node, record the number for each device type that is displayed, including the numbers of registered phones, FXS, FXO, T1Cas, PRI, MOH, MTP, CFB, XCODE, and H323 gateways.

Related Topics

- Performing Pre-Upgrade Tasks, page 9
- Post-Upgrade Tasks, page 39
- *Cisco Unified Serviceability Administration Guide*

Recording Critical Service Status

Record all the critical services and their status by using the Cisco Unified Communications Manager Cisco Unified Real-Time Monitoring Tool (RTMT).

Procedure

Step 1 Perform one of the following tasks:

- In the Quick Launch Channel, click the **View** tab, click the **Server** category, and click the **Critical Services** icon.
- Choose **Monitor > Server > Critical Services**.

Step 2 Record the status of all critical services for each node in the cluster.

Related Topics

- Performing Pre-Upgrade Tasks, page 9
- Post-Upgrade Tasks, page 39
- *Cisco Unified Serviceability Administration Guide*

Locating System Errors by Using Syslog Viewer

Using the Syslog viewer in the Cisco Unified Communications Manager Cisco Unified Real-Time Monitoring Tool (RTMT), locate any events that have a severity of Error or higher.

Procedure

Step 1 Open RTMT and perform one of the following tasks:

- In the Quick Launch Channel, click the **Tools** tab; then, click **SysLog Viewer** and the **SysLog Viewer** icon.

- Choose **Tools > SysLog Viewer > Open SysLog Viewer**.

Step 2 From the Select a Node drop-down list box, choose the server where the logs that you want to view are stored.

Step 3 Double-click the Application Logs folder.

Step 4 Locate events with a severity of Error or higher.

Step 5 Review each log to locate system-affecting errors.

Related Topics

- Performing Pre-Upgrade Tasks, page 9
- Post-Upgrade Tasks, page 39
- *Cisco Unified Serviceability Administration Guide*

Recording Trace and Log Central Job Details

Record the details of all Trace and Log Central jobs.

Procedure

Step 1 Open RTMT and perform one of the following tasks:

- In the Quick Launch Channel, click the **Tools** tab; then, click **Trace** and the **Job Status** icon.
- Choose **Tools > Trace > Job Status**.

Step 2 Double click each scheduled job and record the details that display for each job in the Show Detail dialog box.

Related Topics

- Performing Pre-Upgrade Tasks, page 9
- *Cisco Unified Serviceability Administration Guide*

Accessing CDR Management Configuration

Record CDR Management configuration and destinations, if applicable.

You use the CDR Management Configuration window to set the amount of disk space to allocate to call detail record (CDR) and call management record (CMR) files, configure the number of days to preserve files before deletion, and configure up to three billing application server destinations for CDRs. The CDR repository manager service repeatedly attempts to deliver CDR and CMR files to the billing servers that you configure on the CDR Management Configuration window until it delivers the files successfully, until you change or delete the billing application server on the CDR Management Configuration window, or until the files fall outside the preservation window and are deleted.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools > CDR Management**.

The CDR Management Configuration window displays.

Step 2 Record the General Parameters and the Billing Application Server Parameters.

Related Topics

- Performing Pre-Upgrade Tasks, page 9
- *Cisco Unified Serviceability Administration Guide*

Determining System Configuration Counts

From Cisco Unified CallManager Administration, obtain counts of each of the items that are configured on the system that you want to verify after the replacement. Some examples of items to count follow:

- Phones
- Gateways
- Trunks
- Users
- Route Patterns
- CTI ports
- CTI route points

Procedure

Step 1 In Cisco Unified CallManager Administration, access the windows for each item that you want to count and click **Find** without entering any search parameters. Some examples follow:

- Find and List Phones (**Device > Phone**)
- Find and List Gateway (**Device > Gateway**)
- Find and List Trunks (**Device > Trunk**)
- Find and List Route Patterns (**Call Routing > Route/Hunt > Route Pattern**)
- Find and List Users (**User Management > End Users**)

Note Before the upgrade, locate users by choosing **User > Global Directory**.

- Find and List Application Users (**User Management > Application Users**)

Note Before the upgrade, locate users by choosing **User > Global Directory**.

Step 2 Record the number of each of the items (devices, route patterns, and users).

Related Topics

- Performing Pre-Upgrade Tasks, page 9
- Post-Upgrade Tasks, page 39

- *Cisco Unified Communications Manager Administration Guide*

Firmware Information

Record all of the phone loads and device types that display on the Firmware Load Information window.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Firmware Load Information**.

The Firmware Load Information window displays.

Step 2 Record all the phone loads and device types that display.

Note If you have custom device types that do not ship with Cisco Unified Communications Manager, make sure that you have the appropriate files, so you can reinsert them, if needed.

Related Topics

- Performing Pre-Upgrade Tasks, page 9
- Post-Upgrade Tasks, page 39
- *Cisco Unified Communications Manager Administration Guide*

Obtaining System Version Information

Compare the system version on each node in your cluster by using Cisco Unified Communications Operating System Administration.

Verify that you have DVDs with that version. If you have a service release, you need media for base image and the service release.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Help > About**.

Step 2 Make a note of the system version.

Note After the upgrade, you can also view the system version by choosing **Show > System** from Cisco Unified Communications Operating System Administration. Make a note of the value that displays in the Product Version field on the System Status window.

Related Topics

- Performing Pre-Upgrade Tasks, page 9
- Post-Upgrade Tasks, page 39

- *Cisco Unified Communications Operating System Administration Guide*

Migrating CAR Data

If you do not need to carry over your CAR data to Cisco Unified Communications Manager 7.1(2), Cisco recommends that you purge the CAR data before you run DMA. Purging the CDR data speeds up the migration process and decreases the size of the DMA TAR file.

Cisco recommends that you purge any CAR records older than 180 days. The *CDR Analysis and Reporting Administration Guide* describes how to purge CAR records manually. As an alternative, you can choose not to include CAR data in your Data Migration Assistant backup. Refer to the second "Caution" below.

Caution The version of CAR that runs on Cisco Unified Communications Manager 6.1(2) and higher does not retain CDRs older than the Administrative Reporting Tool (ART) Database Age that is configured in the 4.x ART database. ART database age gets configured on the "Configure Automatic Database Purge" window of ART. The default ART database age is 180 days. If the ART database age is greater than 180, the CAR database on the 6.x/7.x server will retain only 180 days (maximum) of data. However, if the ART database age is less than 180, only data within the age limit that is specified gets retained in the CAR database on the 6.x/7.x server after migration. If you migrate records older than 180 days, the system deletes them immediately after you upgrade.

Caution Before you perform the upgrade, Data Migration Assistant allows you to choose whether to export CAR data. If you choose to export CAR data, Data Migration Assistant allows you to specify the amount of time that you want to allot for CAR migration. The default is 60 minutes. You can choose amounts of time between 30 minutes and 8 hours. For detailed instructions about exporting CAR data, refer to the *Data Migration Assistant User Guide*.

Gathering Information for an Installation

Use Table 5 to record the information about your Cisco Unified Communications Manager server. Gather this information for each Cisco Unified Communications Manager server that you are installing in the cluster. You may not need to obtain all the information; gather only the information that is pertinent to your system and network configuration. You can make copies of this table and record your entries for each server in a separate table, even if you are planning to use the DMABackupInfo.inf file to configure your system.

Tip After you gather the following information, you can enter much of it at Data Migration Assistant's convenient interface, the Answer File Generator window. This window collects data for the Data Migration Assistant platformConfig.xml file. Refer to the *Data Migration Assistant User Guide*.

Note Because some of the fields are optional, they may not apply to your configuration. For example, you choose not to set up an SMTP host.

Caution You cannot change some of the fields after installation without reinstalling the software, so be sure to enter the values that you want.

The last column in the table shows whether a field can be changed after installation and, if so, whether you can change it through Cisco Unified Communications Operating System Administration or through the Command Line Interface (CLI).

Table 5 Node Configuration Data

Parameter	Description	Can Entry Be Changed After Installation?
Administrator ID Your entry:	This field specifies the administrator account user ID that you use for secure shell access to the CLI, for logging into Cisco Unified Communications Operating System Administration and for logging into the Disaster Recovery System.	No, you cannot change the entry after installation. **Note** After installation, you can create additional administrator accounts, but you cannot change the original administrator account user ID.
Administrator Password Your entry:	This field specifies the password for the Administrator account, which you use for secure shell access to the CLI, for logging into Cisco Unified Communications Operating System Administration, and for logging into the Disaster Recovery System. Ensure the password is at least six characters long; it can contain alphanumeric characters, hyphens, and underscore.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set password admin**
Application User Name Your entry:	You use the Application User name as the default password for applications that are installed on the system, including Cisco Unified Communications Manager and Cisco Unified Serviceability.	Yes, you can change the entry after installation by using the following CLI command: CLI > **utils reset_ui_administrator_name**
Application User Password Your entry:	You use the Application User password as the default password for applications that are installed on the system, including Cisco Unified Communications Manager and Cisco Unified CallManager Serviceability.	Yes, you can change the entry after installation by using the following CLI command: CLI > **utils reset_ui_administrator_password**
Country Your entry:	Choose the appropriate country for your installation. The system uses this information to generate certificate signing requests (CSRs), which are used to obtain third-party certificates.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set web-security**

Table 5 Node Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
DHCP Your entry:	If you want to use DHCP to automatically configure the network settings on your server, choose **Yes**. If you choose **Yes**, you do not get prompted for DNS or static configuration settings. If you choose **No**, you must enter a hostname, IP address, IP mask, and gateway.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network dhcp**
DNS Enable Your entry:	A DNS server resolves a hostname into an IP address or an IP address into a hostname. If you do not have a DNS server, enter **No**. If you have a DNS server, Cisco recommends that you enter **Yes** to enable DNS. **Note** When DNS is not enabled, you should only enter IP addresses (not host names) for all network devices in your Cisco Unified Communications Manager network.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network dns**
DNS Primary Your entry:	Enter the IP address of the DNS server that you want to specify as the primary DNS server. Enter the IP address in dotted decimal format as ddd.ddd.ddd.ddd. Consider this field mandatory if DNS is set to **yes**.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network dns**
DNS Secondary (optional) Your entry:	Enter the IP address of the DNS server that you want to specify as the optional secondary DNS server.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network dns**
Domain Your entry:	This field represents the name of the domain in which this machine is located. Consider this field mandatory if DNS is set to **yes**.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network domain**
End User Password Your entry:	The system uses this password to reset the password for all end users that were configured on the Windows-based Cisco Unified Communications Manager.	Yes, after you upgrade the system, you must inform all end users about this new password, which they can then change to a password of their choice.
End User PIN Your entry:	The system uses this PIN to reset the PIN for all end users that were configured on the Windows-based Cisco Unified Communications Manager.	Yes, after you upgrade the system, you must inform all end users about this new PIN, which they can then change to a PIN of their choice.

Table 5 Node Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
Gateway Address Your entry:	Enter the IP address of the network gateway. If you do not have a gateway, you must still set this field to 255.255.255.255. Not having a gateway may limit you to only being able to communicate with devices on your subnet. If DHCP is set to **No**, consider this field mandatory.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network gateway**
Hostname Your entry:	Enter a host name that is unique to your server. The host name can comprise up to 64 characters and can contain alphanumeric characters and hyphens. If DHCP is set to **No**, consider this field mandatory.	Yes, you can change the hostname after installation. For more information on changing hostnames, refer to the *Changing the IP Address and Host Name for Cisco Unified Communications Manager Release 7.1(2)* document at the following URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.
IP Address Your entry:	Enter the IP address of your server. If DHCP is set to **No**, consider this field mandatory.	Yes, you can change the entry after installation. For more information on changing IP addresses, refer to the *Changing the IP Address and Host Name for Cisco Unified Communications Manager Release 7.1(2)* document at the following URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.
IP Mask Your entry:	Enter the IP subnet mask of this machine. If DHCP is set to **No**, consider this field mandatory.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network ip eth0**
Location Your entry:	Enter the location of the server. The system uses this information to generate certificate signing requests (CSRs), which are used to obtain third-party certificates. You can enter any location that is meaningful within your organization. Examples include the state or the city where the server is located.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set web-security**

Table 5 Node Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
MTU Size Your entry:	The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host will transmit on the network. Enter the MTU size in bytes for your network. If you are unsure of the MTU setting for your network, use the default value. Default: 1500 bytes **Note** The MTU size on the first node must match the MTU size on the subsequent nodes. If these values do not match, the Cisco Unified Communications Manager upgrade will fail.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network mtu**
NIC Duplex Your entry:	Choose the duplex mode for the network interface card (NIC), either Full or Half. **Note** This parameter only displays when you choose not to use Automatic Negotiation.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network nic**
NIC Speed Your entry:	Choose the speed for the NIC, either 10 megabits per second or 100 megabits per second. **Note** This parameter only displays when you choose not to use Automatic Negotiation.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network nic**
NTP Server Your entry:	Enter the hostname or IP address of one or more network time protocol (NTP) servers with which you want to synchronize. You can enter up to five NTP servers. **Note** To avoid potential compatibility, accuracy, and network jitter problems, the external NTP servers that you specify for the primary node should be NTP v4 (version 4). If you are usingIPv6 addressing, external NTP servers must be NTP v4.	Yes, you can change the entry after installation by using the Cisco Unified Communications Operating System: **Settings > NTP Servers**

Table 5 Node Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
Organization Your entry:	Enter the name of your organization. **Tip** You can use this field to enter multiple organizational units. To enter more than one organizational unit name, separate the entries with a comma. For entries that already contain a comma, enter a backslash before the comma that is included as part of the entry. The system uses this information to generate certificate signing requests (CSRs), which are used to obtain third-party certificates.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set web-security**
Security Password Your entry:	Servers in the cluster use the security password to communicate with one another. The password must contain at least six alphanumeric characters. It can contain hyphens and underscores, but it must start with an alphanumeric character. **Note** Save this password. You will be asked to enter the same security password for each subsequent node in the cluster.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set password security** ⚠ **Caution** To avoid losing communications between nodes, you must change the security password on all nodes in a cluster and reboot all the nodes. For more information, refer to the description of this command in the *Cisco Unified Communications Operating System Administration Guide*
SMTP Location Your entry:	Enter the hostname or IP address for the SMTP server that is used for outbound e-mail. The hostname can contain alphanumeric characters, hyphens, or periods, but it must start with an alphanumeric character. **Note** You must fill in this field if you plan to use electronic notification.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set smtp**
State Your entry:	Enter the state where the server is located. **Note** You can enter a full name or abbreviation. The value that you enter gets used to generate a Certificate Signing Request (CSR).	Yes, you can change the entry after installation by using the following CLI command: CLI > **set web-security**
Time Zone Your entry:	This field specifies the local time zone and offset from Greenwich Mean Time (GMT). Choose the time zone that most closely matches the location of your machine.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set timezone**

Table 5 Node Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
Unit Your entry:	Enter your unit. **Note** The value that you enter gets used to generate a Certificate Signing Request (CSR).	Yes, you can change the entry after installation by using the following CLI command: CLI > **set web-security**

Handling Network Errors During Upgrade

During the upgrade process, the installation program verifies that the server can successfully connect to the network by using the network configuration that you enter. If it cannot, a message displays, and you are prompted to select one of the following options:

- **RETRY** —The installation program tries to validate networking again. If validation fails again, the error dialog box displays again.
- **REVIEW (Review Configuration)**—Allows you to review and modify the networking configuration. The installation program returns to the network configuration windows.

  Because networking is validated after you complete each networking window, the message might display multiple times. If the message displays while you are reviewing the network configuration windows, choose **IGNORE** to move to the next window. If you choose **REVIEW**, the first network configuration window displays again.
- **HALT**— The installation halts. You can copy the installation log files to a USB disk to aid troubleshooting of your network configuration.
- **IGNORE** —The installation continues. The networking error gets logged. In some cases, the installation program validates networking multiple times, so this error dialog box might display multiple times.

Assigning the Host Name/IP Address (Servername) to the 7.1(2) Server

In 4.x releases, the Host Name/IP Address field (also known as Servername) on the publisher server Server Configuration Settings window contains one of the following types of values:

- If DNS is enabled, it identifies the host name.
- If DNS is not enabled, it contains the IP address of the server.

To access Server Configuration Settings, navigate to **System > Server**.

The Data Migration Assistant (DMA) file that is used to migrate data from 4.x to 7.1(2) releases includes the Host Name/IP Address value. When you migrate data by using DMA, the Host Name/IP Address (Servername) for the publisher server gets imported into the 7.1(2) database as follows:

- If the Host Name/IP Address (Servername) was a host name, the installation program compares this Servername to the provisioned hostname for the 7.1(2) server (either through static provisioning or DNS/DHCP). If a mismatch exists, the installation program does the following actions:
  - Uses the provisioned hostname as the Host Name/IP address for the 7.x server, which overrides the servername in the DMA file.
  - Notifies you about the mismatch and its resolution.
  - Prompts you to proceed or cancel the installation.

- If the Host Name/IP Address (Servername) was an IP address, the installation program compares this Servername to the provisioned IP Address for the 7.x server (either through static provisioning or DNS/DHCP). If a mismatch exists, the installation program does the following actions:
  - Uses the provisioned IP address as the servername for the 7.x server, overriding the servername in the DMA file.
  - Notifies you about the mismatch and its resolution.
  - Prompts you to proceed or cancel the installation.

This feature allows you to import your 4.x data to a 7.1(2) server without having to preserve the IP address or host name. The IP address and/or host name of the 7.1(2) server can differ from the 4.x servername.

Caution Do not assign a hostname or IP address to the upgraded server that is already assigned to another node in the cluster. Doing so causes the cluster upgrade to fail.

Note If you change the Servername during the upgrade, the original Servername—rather than the changed Servername—appears in the Call Manager Administration window.

If you wish to change the Servername as it appears in the Call Manager Administration window so that it matches the name you assigned during the upgrade, you can do so after the upgrade. However, this is not required. For more information on how to do so, refer to the next note.

Note You can change the hostname or IP address of the Cisco Unified Communications Manager server after you upgrade. For more information, refer to the *Changing the IP Address and Host Name for Cisco Unified Communications Manager Release 7.1(2)* document at the following URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Upgrading a Cluster from Release 4.x to Cisco Unified Communications Manager Release 7.1(2) in Parallel

You can begin the installation of the first node and subsequent nodes at the same time. When the installation program prompts you to designate the first node as the first node, you must stop installing Cisco Unified Communications Manager on the subsequent nodes until the installation completes on the first node and you configure the subsequent nodes on the first node. After you have configured the subsequent nodes on the first node, you can continue the installation on the subsequent nodes. For optimal performance, you should choose the **Skip** option rather than the **Proceed** option in the installation program.

Upgrading Cisco Unified Communications Manager

This section describes how to upgrade Cisco Unified Communications Manager from a Windows-based version (4.x) to version 7.1(2). You upgrade the operating system and application by running one installation program.

Caution Before beginning this procedure, ensure that you have backed up the data on your current Windows-based version of Cisco Unified Communications Manager. For more information, see the documentation for your version of Backup and Restore Utility.

Navigating Within the Installation Wizard

For instructions on how to navigate within the installation wizard, see Table 6.

Table 6 Installation Wizard Navigation

To Do This	Press This
Move to the next field	**Tab**
Move to the previous field	**Alt-Tab**
Choose an option	**Spacebar**
Scroll up or down in a list	Up or down arrow
Go to the previous window	Space bar to choose **Back** (when available)
Get help information on a window	Space bar to choose **Help** (when available)

Using the Data Migration Assistant Generated Configuration File

The Data Migration Assistant generates a configuration file (platformConfig.xml) to facilitate the installation of Cisco Unified Communications Manager first nodes (publishers) and subsequent nodes (subscribers). The configuration file populates several fields during the upgrade, including domain name, IP address, primary DNS, secondary DNS, and NTP server.

The Data Migration Assistant generates the configuration file during the DMA export process. You use Data Migration Assistant's Answer File Generator window to specify where to save your platformConfig.xml file. Refer to the *Data Migration Assistant User Guide*.

To use the configuration file, copy the platformConfig.xml file to a USB key, and place the USB key into the Cisco Unified Communications Manager first node before you boot the server with the Cisco Unified Communications Manager DVD.

Note Cisco requires that you use USB keys that are compatible with Linux 2.4. Cisco recommends that you use USB keys that are formatted to be compatible with Linux 2.4 for the configuration file. These keys will have a W95 FAT32 format.

For more information on running Data Migration Assistant, refer to the *Data Migration Assistant User Guide* at the following URL:

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

Starting the Installation

You use this procedure to install the operating system on first and subsequent nodes.

Before you begin to upgrade the first node, make sure that you have reviewed and completed the tasks that are described in the "Performing Pre-Upgrade Tasks" section on page 9

Note Before you begin to upgrade the first node, make sure that you have copies of the backup files on a separate reliable high-performance computer that runs FTP or SFTP. Store copies of your DMA backup files on this computer also.

To upgrade a subsequent node in the cluster, you must first install the new operating system and the new Cisco Unified Communications Manager application on the first node and then configure the subsequent node on the first node by using Cisco Unified Communications Manager Administration.

To upgrade a subsequent node in the cluster from Cisco Unified CallManager 4.x to Cisco Unified Communications Manager Release 7.1(2), perform the following steps:

1. Upgrade the first node, the Cisco Unified CallManager 4.x publisher server, to Cisco Unified Communications Manager 7.1(2).
2. Using Cisco Unified Communications Manager Administration on the first node, configure the subsequent nodes. Refer to the *Cisco Unified Communications Manager Administration Guide* for more information about configuring subsequent nodes on the first node.
3. Ensure that the subsequent nodes have network connectivity to the first node.
4. Install the new operating system and Cisco Unified Communications Manager application from a DVD.
5. If required, upgrade the software to a later service release.
6. Configure the Cisco Unified Communications Operating System and Cisco Unified Communications Manager.

Note You must complete a successful migration of data on the first node prior to upgrading the subsequent nodes in the cluster.

Caution Before beginning this procedure for a subsequent node, ensure you have already upgraded the Cisco Unified CallManager 4.x publisher server, configured the subsequent node on the Cisco Unified Communications Manager 7.1(2) first node, and have network connectivity to the first node. Failure to meet these conditions can cause the installation to fail.

Caution If you configured Network Time Protocol on the first node, ensure that the first node is synchronized with an NTP server before you upgrade a subsequent node. From the Command Line Interface on the first node, enter utils ntp status. Ensure that the printout indicates that the node is synchronized with an NTP server.

If the first node is not synchronized with an NTP server, installation of the subsequent node will fail.

Step 1 Insert the installation DVD into the tray. If you are using the DMA-generated configuration file (platformConfig.xml), you must also insert the USB key into the USB port.

Step 2 Restart the server, so it boots from the DVD. After the server completes the boot sequence, the DVD Found window displays.

Step 3 If you are prompted to choose to perform the media check, choose **Yes**; or to skip the media check, choose **No**.

The media check checks the integrity of the DVD. If your DVD has passed the media check previously, you might choose to skip the media check.

Note If you have a new server with Cisco Unified Communications Manager preinstalled, you do not need to install from a DVD.

If you choose **No** and are not using the DMA-generated platformConfig.xml answer file, continue with Step 6.

If you choose **No** and are using the DMA-generated platformConfig.xml answer file, continue with Step 7.

Step 4 If you choose **Yes** to perform the media check, the system installer performs the media check and displays the Media Check Result window. Perform these tasks:

a. If the Media Check Result displays Pass, choose **OK** to continue the installation.

b. If the media fails the Media Check, either download another copy from Cisco.com or obtain another disc directly from Cisco Systems.

Step 5 The system installer performs the following hardware checks to ensure that your system is correctly configured. If the installer makes any changes to your hardware configuration settings, you will get prompted to restart your system. Leave the DVD in the drive during the reboot:

- First, the installation process checks for the correct drivers, and you may see the following message:

  ```
  No hard drives have been found. You probably need to manually choose device drivers
  for install to succeed. Would you like to select drivers now?
  ```

  To continue the installation, choose **Yes**.

- The installation next checks to see whether you have a supported hardware platform. If your server does not meet the exact hardware requirements, the installation process fails with a critical error. If you think this is not correct, capture the error and report it Cisco support.
- The installation process next verifies RAID configuration and BIOS settings.

Note If this step repeats, choose **Yes** again.

- If the installation program must install a BIOS update, a notification displays that tells you that the system must reboot. Press any key to continue with the installation.

After the hardware checks complete, the Product Deployment Selection window displays.

Step 6 In the Product Deployment Selection window, if you are prompted, choose Cisco Unified Communications Manager; then, choose **OK**.

Note The window indicates which products are supported and not supported by your hardware. If only one product is supported, you do not choose which product to install.

Note The system supports migrating data from a Windows-based release only if you choose to install Cisco Unified Communications Manager.

Step 7 If software is currently installed on the server, the Overwrite Hard Drive window opens and displays the current software version on your hard drive and the version on the DVD. Choose **Yes** to continue with the installation or **No** to cancel.

Caution If you choose **Yes** on the Overwrite Hard Drive window, all existing data on your hard drive gets overwritten and destroyed.

The Platform Installation Wizard window displays.

If you are using the DMA-generated configuration file for the installation of the first node, continue with Step 2 in the "Upgrading the First Node" section on page 33.

Step 8 Choose one of the following options:

- To cancel the installation, choose **Cancel**.
- To enter software configuration information manually, then have the installation program install the configured software on the server, choose **Proceed** and continue with Step 9 of this procedure.
- To do either of the following tasks, choose **Skip**:
  - Manually configure software that is preinstalled on your server: In this case, you do not need to install the software, but you must configure the preinstalled software.
  - Install the software before manually configuring it: In this case, the installation program installs the software, then prompts you to configure it manually. This method might cause you to spend more time performing the installation than the other methods.

Note You can choose **Skip** if you want to install the application on all your servers first and then enter the configuration information at a later time.

After the system restarts, the Preexisting Installation Configuration window displays. Choose **Continue** to continue the installation.

The Platform Installation Wizard window displays. To continue with the Platform Installation Wizard, choose **Proceed**.

Step 9 Choose the type of installation to perform by doing the following steps. See Table 1 for more information on installation options:

Note Do not attempt to upgrade by importing Windows data after you upgrade by applying a patch.

a. In the Apply Patch window, choose one of the options:

- To upgrade to a later Service Release of the software during installation, choose **Yes**. Continue with the "Applying a Patch" section on page 30.
- To skip this step, choose **No**.
- To return to the previous window, choose **Back**.

b. If you are upgrading the first node in a cluster, in the Import Windows Data window, choose **Yes**. Continue with the "Upgrading the First Node" section on page 33.

c. If you are upgrading a subsequent node in a cluster, in the Import Windows Data window, choose **No**.

Step 10 In the Basic Install window, choose **Continue**. Continue with the "Upgrading Subsequent Nodes in the Cluster" section on page 37.

Note To perform a basic installation, that is, to install the application without importing Windows data, see *Installing Cisco Unified Communications Manager*.

Applying a Patch

If you choose **Yes** in the Apply Patch window, the installation wizard installs the software version on the DVD first and then restarts the system. You must obtain the appropriate upgrade file from Cisco.com before you can upgrade during installation.

Note You can upgrade to any supported higher release, as long as you have a full patch, not an ES or an SR. If you have an ES or an SR, you can only upgrade to a later service release within the same maintenance release.

You can access the upgrade file during the installation process from either a local disk (CD or DVD) or from a remote FTP or TFTP server.

Procedure

Step 1 After the system restarts, the Platform Installation Wizard window displays. To continue the installation, choose **Proceed**.

The Apply Patch window displays.

Note If the installer pops up a window that states that it detected new hardware, press any key and then choose **Install** from the next window.

Step 2 Choose **Yes**.

The Install Upgrade Retrieval Mechanism Configuration window displays.

Step 3 Choose the upgrade retrieval mechanism to use to retrieve the upgrade file:

- **SFTP**—Retrieves the upgrade file from a remote server by using the Secure File Transfer Protocol (SFTP). Skip to the "Upgrading From a Remote Server" section on page 31.
- **FTP**—Retrieves the upgrade file from a remote server by using File Transfer Protocol (FTP). Skip to the "Upgrading From a Remote Server" section on page 31.
- **LOCAL**—Retrieves the upgrade file from a local CD or DVD. Continue with the "Upgrading from a Local Disk" section on page 31.

Upgrading from a Local Disk

Before you can upgrade from a local disk, you must download the appropriate patch file from Cisco.com and use it to create an upgrade DVD. You must create an ISO image on the DVD from the upgrade file. Just copying the ISO file to a DVD will not work.

Step 1 When the Local Patch Configuration window displays, enter the patch directory and patch name, if required, and choose **OK**.

The Install Upgrade Patch Selection Validation window displays.

Step 2 The window displays the patch file that is available on the DVD. To update the system with this patch, choose **Continue**.

Step 3 Choose the upgrade patch to install. The system installs the patch, then restarts the system by running the upgraded software version.

After the system restarts, the Preexisting Configuration Information window displays.

Step 4 To continue the installation, choose **Proceed**.

The Platform Installation Wizard window displays.

Step 5 To continue the installation, choose **Proceed** or choose **Cancel** to stop the installation.

If you choose **Proceed**, the Apply Patch window displays. Continue with Step 11.

If you choose **Cancel**, the system halts, and you can safely power down the server.

Step 6 When the Apply Patch window displays, choose **No**.

Step 7 The Windows Upgrade window displays.

Step 8 Continue with the upgrade procedure for the type of node that you are installing.

- "Upgrading the First Node" section on page 33
- "Upgrading Subsequent Nodes in the Cluster" section on page 37

Upgrading From a Remote Server

Before you can upgrade from a remote server, you must download the appropriate patch file from Cisco.com and copy the file to an FTP or SFTP server that the server can access.

If you are upgrading from release 5.1(3), you must download the appropriate patch file from Cisco.com, create an ISO image DVD from the patch file, then copy the contents of the DVD to the remote FTP or SFTP server that the server can access.

If you chose to upgrade through an FTP or SFTP connection to a remote server, you must first configure network settings so the server can connect to the network.

Step 1 The Auto Negotiation Configuration window displays.

Step 2 The installation process allows you to automatically set the speed and duplex settings of the Ethernet network interface card (NIC) by using automatic negotiation. You can change this setting after installation.

Note To use this option, your hub or Ethernet switch must support automatic negotiation.

- To enable automatic negotiation, choose **Yes**.

  The MTU Configuration window displays. Continue with Step 4.

- To disable automatic negotiation, choose **No**. The NIC Speed and Duplex Configuration window displays. Continue with Step 3.

Step 3 If you chose to disable automatic negotiation, manually choose the appropriate NIC speed and duplex settings now and choose **OK** to continue.

The MTU Configuration window displays.

Step 4 In the MTU Configuration window, you can change the MTU size from the operating system default.

The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host will transmit on the network. If you are unsure of the MTU setting for your network, use the default value.

Caution If you configure the MTU size incorrectly, be aware that your network performance can be affected.

- To accept the default value (1500 bytes), choose **No**.
- To change the MTU size from the operating system default, choose **Yes**, enter the new MTU size, and choose **OK**.

The DHCP Configuration window displays.

Step 5 For network configuration, you can choose to either set up static network IP addresses for the node and gateway or to use Dynamic Host Configuration Protocol (DHCP).

- If you have a DHCP server that is configured in your network and want to use DHCP, choose **Yes**. The system restarts and checks for network connectivity. Skip to Step 8.
- If you want to configure static IP addresses for the node, choose **No**. The Static Network Configuration window displays.

Step 6 If you chose not to use DHCP, enter your static network configuration values and choose **OK**. See Table 5 for field descriptions.

The DNS Client Configuration window displays.

Step 7 To enable DNS, choose **Yes**, enter your DNS client information, and choose **OK**. See Table 5 for field descriptions.

After the system configures the network and checks for connectivity, the Remote Patch Configuration window displays.

Step 8 Enter the location and login information for the remote file server. See Table 5 for field descriptions. After the network restarts, the system connects to the remote server and retrieves a list of available upgrade patches.

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. The following examples describe the syntax:

- Begin the pathname with a forward slash (/) and use forward slashes throughout the pathname.
- The pathname must start from the FTP or SFTP root directory on the server, so you cannot enter a Windows absolute pathname, which starts with a drive letter (for example, C:).

If you encounter problems, check with your system administrator for the correct directory path.

The Install Upgrade Patch Selection window displays.

Step 9 Choose the upgrade patch to install. The system downloads, unpacks, and installs the patch and then restarts the system by running the upgraded software version.

After the system restarts, the Preexisting Configuration Information window displays.

Step 10 To continue the installation, choose **Proceed**.

The Platform Installation Wizard window displays.

Step 11 To continue the installation, choose **Proceed** or choose **Cancel** to stop the installation.

If you choose **Proceed**, the Apply Patch window displays. Continue with Step 12.

If you choose **Cancel**, the system halts, and you can safely power down the server.

Step 12 When the Apply Patch window displays, choose **No**.

Step 13 The Windows Upgrade window displays.

Step 14 Continue with the procedure for the type of node that you are installing.

- "Upgrading the First Node" section on page 33
- "Upgrading Subsequent Nodes in the Cluster" section on page 37

Upgrading the First Node

When you choose Windows Upgrade, the installation wizard prompts you for the location of the preexisting Windows configuration information that the Data Migration Assistant (DMA) tool created. See the *Data Migration Assistant User Guide* for more information on the DMA tool.

Step 1 In the Windows Upgrade window, import data from a Windows version of Cisco Unified Communications Manager by choosing **Yes**.

The Timezone Configuration window displays.

Step 2 Choose the appropriate time zone for the server and then choose **OK**.

The Auto Negotiation Configuration window displays.

Step 3 The installation process allows you to automatically set the speed and duplex settings of the Ethernet network interface card (NIC) by using automatic negotiation. You can change this setting after installation.

- To enable automatic negotiation, choose **Yes**. The MTU Configuration window displays. Continue with Step 5.

  Note To use this option, your hub or Ethernet switch must support automatic negotiation.

- To disable automatic negotiation, choose **No**. The NIC Speed and Duplex Configuration window displays.

Step 4 If you chose to disable automatic negotiation, manually choose the appropriate NIC speed and duplex settings now and choose **OK** to continue.

The MTU Configuration window displays.

Step 5 In the MTU configuration window, you can change the MTU size from the operating system default.

The maximum transmission unity (MTU) represents the largest packet, in bytes, that this host will transmit on the network. If you are unsure of the MTU setting for your network, use the default value, which is 1500 bytes.

Caution If you configure the MTU size incorrectly, be aware that your network performance can be affected.

- To accept the default value (1500 bytes), choose **No**.
- To change the MTU size from the operating system default, choose **Yes**, enter the new MTU size, and choose **OK**.

The DHCP Configuration window displays.

Step 6 For network configuration, you can choose to either set up static network IP addresses for the node and gateway or to use Dynamic Host Configuration Protocol (DHCP).

- If you have a DHCP server that is configured in your network and want to use DHCP, choose **Yes**. The Administrator Login Configuration window displays. Continue with Step 9.
- If you want to configure static IP addresses for the node, choose **No**. The Static Network Configuration window displays.

Step 7 If you chose not to use DHCP, enter your static network configuration values and choose **OK**. See Table 5 for field descriptions.

If you are using the DMA-generated configuration file, the system populates these fields. If necessary, you can change them.

The DNS Client Configuration window displays.

Step 8 To enable DNS, choose **Yes**, enter your DNS client information, and choose **OK**. See Table 5 for field descriptions.

If you are using the DMA-generated configuration file, the system populates these fields. If necessary, you can change them.

The Administrator Login Configuration window displays.

Step 9 Enter your administrator login and password from Table 5.

Note The Administrator login must start with an alphabetic character, be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores. You will need the Administrator login to log in to Cisco Unified Communications Operating System Administration, the command line interface, and the Disaster Recovery System.

The Certificate Signing Request Information window displays.

Step 10 Enter your certificate signing request information from Table 5 and choose **OK**.

The First Node Configuration window displays.

Step 11 You must configure this node as the first node in the cluster. To continue, choose **Yes**.

The Network Time Protocol Client Configuration window displays.

Step 12 Choose whether you want to configure an external NTP server or manually configure the system time.

Note Cisco recommends that you use an external NTP server to ensure accurate system time on the first node. Ensure that the external NTP server is stratum 9 or higher (meaning strata 1-9). Subsequent nodes in the cluster will get their time from the first node.

- To set up an external NTP server, choose **Yes** and enter the IP address, NTP server name, or NTP server pool name for at least one NTP server. You can configure up to five NTP servers, and Cisco recommends that you use at least three. To continue with the installation, choose **Proceed**.

  The system contacts an NTP server and automatically sets the time on the hardware clock.

  Note If have already entered the network configuration information and the system has rebooted (a Skip installation), the Test button displays. You can choose **Test** to check whether the NTP servers are accessible.

- To manually configure the system time, choose **No** and enter the appropriate date and time to set the hardware clock. Choose **OK** to continue with the installation.

The Database Access Security Configuration window displays.

Step 13 Enter the Database Access Security password from Table 5.

Note The Database Access Security password must start with an alphanumeric character, be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores. Be sure that you save the Database Access security password. You must enter the same password on all nodes in the cluster.

The SMTP Host Configuration window displays.

Step 14 If you want to configure an SMTP server, choose **Yes** and enter the SMTP server name.

Note You must configure an SMTP server to use certain operating system features; however, you can also configure an SMTP server later by using the operating system GUI or the command line interface.

Step 15 Choose **OK**.

The DMA Retrieval Mechanism Configuration window displays.

Step 16 Choose the mechanism that will be used to retrieve the DMA file:

- **SFTP**—Retrieves the DMA file from a remote server by using Secure File Transfer Protocol (SFTP). The SFTP server must support the following commands: `cd`, `ls`, `get`.
- **FTP**—Retrieves the DMA file from a remote server by using File Transfer Protocol (FTP). The FTP server must support the following commands: `cd`, `bin`, `dir` and `get`.
- **TAPE**—Retrieves the DMA file from a locally attached tape drive.

Note To support retrieval of the DMA file, an FTP server should support the `cd`, `bin`, `dir` and `get` commands, and an SFTP server should support `cd`, `ls` and `get` commands.

To continue with the installation wizard, choose **OK**.

Note If you choose SFTP or FTP, the DMA Backup Configuration window displays, and you must enter the location of the DMA file and the login information for the remote server. If you choose TAPE, the system reads the DMA file from the locally attached tape.

Note The system does not verify filename, path, or credentials until after the installation begins. If the system detects that you provided incorrect data, a prompt displays that allows you to reenter the information. This prompt may display up to 45 minutes after installation begins.

Step 17 If you chose SFTP or FTP, enter the DMA Backup Configuration information and choose **OK**.

If the DMA 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. The following examples describe the syntax:

- Begin the pathname with a forward slash (/) and use forward slashes throughout the pathname.
- The pathname must start from the FTP or SFTP root directory on the server, so you cannot enter a Windows absolute pathname, which starts with a drive letter (for example, C:).

If you encounter problems, check with your system administrator for the correct directory path.

The installation program validates the DMA data. If no problems are detected, The Platform Configuration Confirmation window displays.

Step 18 If a problem with the DMA data is detected, the following types of notification windows can display:

- A failure window indicates that the DMA data failed validation and cannot be imported. Choose one of the following options:
  - Choose **Back** to back up and enter a different DMA data file.
  - Choose **Halt** to halt and exit the installation program.
- A warning window indicates that problems with the DMA data were detected that might prevent the data from importing correctly. Choose one of the following options:
  - Choose **Yes** to continue attempting to import the DMA data.
  - Choose **No** to back up and enter a different DMA file.

  Cisco Systems, Inc., recommends that you do not continue with DMA data that has warnings.
- An invalid version error screen indicates that the DMA file was generated for a different target software version than the version that you are installing. Choose **OK** to back up and enter a different DMA file.

Step 19 To continue with the installation, choose **OK** or choose **Back** to modify the platform configuration.

When you choose **OK**, the Application User Password Configuration window displays.

Step 20 Enter the Application User Name and Application User Password from Table 5 and confirm the password by entering it again.

Step 21 Choose **OK**.

The End User Password/PIN Configuration window displays.

Step 22 Enter and confirm the End User Password and PIN and choose **OK**.

The end user password must comprise five or more alphanumeric or special characters. The end user PIN must comprise five or more numeric characters.

The system installs the software, restarts the network, and reads the DMA file that you specified.

The DMA Retrieval Mechanism Configuration window displays.

Step 23 To continue, choose **OK**, or to choose a different DMA file, choose **Back**.

Step 24 The installation begins.

The installation program assigns a Host Name/ IP Address (Servername) to the 7.1(2) server by comparing the value in the DMA file to the value that is configured on the 7.1(2) system. For more information, refer to the "Assigning the Host Name/IP Address (Servername) to the 7.1(2) Server" section on page 24.

Step 25 After the installation has proceeded for approximately 30 minutes, the system compares host name/IP address (Servername) in the DMA file to the value that is configured on the 7.1(2) system.

If a mismatch exists between these values, you are prompted to Proceed or Cancel. Choose **Proceed** to proceed with the installation by using the Host Name/ IP Address (Servername) that the installation program assigned, or choose **Cancel** to cancel the installation.

Step 26 If no mismatch exists, or you choose **Proceed**, the Product Licensing window displays with information regarding how to obtain a license.

The installation continues automatically.

The DVD drive ejects, and the server reboots. Do not reinsert the DVD.

Step 27 When the installation process completes, you get prompted to log in by using the Administrator account and password.

Step 28 Complete the post-upgrade tasks that are listed in the "Post-Upgrade Tasks" section on page 39.

Upgrading Subsequent Nodes in the Cluster

Use this procedure to continue installing Cisco Unified Communications Manager on a subsequent node in your cluster. Before you complete this section, you must have installed the operating system, as described in the "Starting the Installation" section on page 26.

Step 1 In the Windows Upgrade window, choose **No**.

The Timezone Configuration displays.

Step 2 Choose the appropriate time zone for the server and then choose **OK**.

The Auto Negotiation Configuration window displays.

Step 3 The installation process allows you to automatically set the speed and duplex settings of the Ethernet network interface card (NIC) by using automatic negotiation. You can change this setting after installation.

- To enable automatic negotiation, choose **Yes**. The DHCP Configuration window displays.

Note To use this option, your hub or Ethernet switch must support automatic negotiation.

- To disable automatic negotiation, choose **No**. The NIC Speed and Duplex Configuration window displays.

Step 4 If you chose to disable automatic negotiation, manually choose the appropriate NIC Speed and Duplex settings now and choose **OK** to continue.

The DHCP Configuration window displays.

Step 5 For network configuration, you can choose to either set up static network IP address for the node or to use Dynamic Host Configuration Protocol (DHCP).

- If you have a DHCP server that is configured in your network and want to use DHCP, choose **Yes**. The network restarts, and the Administrator Login Configuration window displays.
- If you want to configure static IP address for the node, choose **No**. The Static Network Configuration window displays.

Step 6 If you chose not to use DHCP, enter your static network configuration values and choose **OK**. See Table 5 for field descriptions.

The DNS Client Configuration window displays.

Step 7 To enable DNS, choose **Yes**, enter your DNS client information, and choose **OK**. See Table 5 for field descriptions.

The network restarts by using the new configuration information, and the Administrator Login Configuration window displays.

Step 8 Enter your Administrator login and password from Table 5.

Note The Administrator login must start with an alphabetic character, be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores. You will need the Administrator login to log in to Cisco Unified Communications Operating System Administration, the command line interface, and the Disaster Recovery System.

The Certificate Signing Request Information window displays.

Step 9 Enter your certificate signing request information from Table 5 and choose **OK**.

The First Node Configuration window displays.

Step 10 To configure this server as a subsequent node in the cluster, choose **No**.

The First Node Access Configuration window displays.

Step 11 Enter the First Node Access Configuration information from Table 5.

The SMTP Host Configuration window displays.

Step 12 If you want to configure an SMTP server, choose **Yes** and enter the SMTP server name.

Note You must configure an SMTP server to use certain platform features; however, you can also configure an SMTP server later by using the platform GUI or the command line interface.

The Platform Configuration Confirmation window displays.

Step 13 To start installing the software, choose **OK**, or if you want to change the configuration, choose **Back**.

When the installation process completes, you get prompted to log in by using the administrator account and password.

Step 14 To log in, enter the administrator account name and password that you entered during installation.

Step 15 Complete the post-upgrade tasks that are listed in the "Post-Upgrade Tasks" section on page 39.

Post-Upgrade Tasks

When you complete your upgrade of Cisco Unified Communications Manager, you must perform all appropriate tasks as described in the following table:

Table 7 Post-Upgrade Tasks

Post-Upgrade Tasks	Important Notes
Obtain and install the software feature license and upgrade your product licenses.	See the "Uploading Licenses" section on page 45.
Delete intermediate license file.	After you upgrade your product license, use the following CLI command to remove the intermediate license file licupgrade_7.1.lic: **file delete license** *licupgrade_7.1.lic* If you do not remove this intermediate license file, the system generates the following message after you reboot: `%CCM_LICENSEMANAGER-JAVAAPPLICATIONS-3-CiscoLicenseFileError: License File Error Reason:Invalid or tampered License File App ID:Cisco License Manager` If you see the preceding message after you reboot, use the preceding described CLI command to remove the intermediate license file.
Verify that all appropriate Cisco Unified Communications Manager services started. Verify that you can make internal calls. Verify that you can place and receive a call across gateways.	Refer to the *Cisco Unified Serviceability Administration Guide* See the "Verifying Cisco Unified Communications Manager Services" section on page 48.

Table 7 Post-Upgrade Tasks (continued)

Post-Upgrade Tasks	Important Notes
If security is enabled on the cluster, you must configure CTL.	To configure CTL on the upgraded cluster, 1. Uninstall the existing CTL client. 2. Install the new CTL client. 3. Run the CTL client by using at least one of the previously used USB keys. 4. Update the new CTL file on all nodes. 5. Restart all nodes. 6. The secure phones register. You can now test internal calls among secure and non-secure phones. For information about performing these tasks and about Cisco Unified Communications Manager security, refer to the *Cisco Unified Communications Manager Security Guide*.
Using the Cisco Unified Communications Manager Cisco Unified Real-Time Monitoring Tool (RTMT), make sure that all the registration information values match the values that you recorded before the server replacement.	See the "Determining Registration Counts by Using RTMT" section on page 13.
Using the Cisco Unified Communications Manager Cisco Unified Real-Time Monitoring Tool (RTMT), make sure that all the critical services and their status match those that you recorded before the server upgrade.	See the "Recording Critical Service Status" section on page 14.
Using the Syslog viewer in the Cisco Unified Communications Manager Cisco Unified Real-Time Monitoring Tool (RTMT), locate any events that have a severity of Error or higher.	Perform this task to ensure that no system-affecting errors exist on your system. See the "Locating System Errors by Using Syslog Viewer" section on page 14.

Table 7 Post-Upgrade Tasks (continued)

Post-Upgrade Tasks	Important Notes
Using the Syslog viewer in the Cisco Unified Communications Manager Cisco Unified Real-Time Monitoring Tool (RTMT), check the Replicate_State counter for the Number of Replicates Created and State of Replication object on all nodes. The value on each node should equal 2. This counter represents the state of replication, which includes the following possible values: This counter represents the state of replication. The following list provides possible values: • 0—Initializing. The counter equals 0 when the server is not defined or when the server is defined but the realize template has not completed. • 1—The system created replicates of some tables but not all tables. Cisco recommends that you run utils dbreplication status on the CLI to determine the location and cause of the failure. • 2—Good Replication. • 3—Bad Replication. When the counter displays a value of 3, consider replication in the cluster as bad. It does not mean that replication failed on a particular node. Cisco recommends that you run utils dbreplication status on the CLI to determine the location and cause of the failure. • 4—Replication setup did not succeed.	To access the appropriate object and counter, use the following procedure: 1. Perform one of the following tasks: • In the Quick Launch Channel, click **System**, click **Performance** and then, click the **Performance** icon. • Choose **System > Performance > Open Performance Monitoring**. 2. Double-click the name of the server where you want to add a counter to monitor. 3. Double-click the **Number of Replicates Created and State of Replication** object. 4. Double-click the **Replicate_State** counter. 5. Choose the **ReplicateCount** instance and click **Add**.
From Cisco Unified Reporting, make sure that the number of phones, gateways, trunks, users, and route patterns that are configured in the database matches the numbers that you recorded before the server replacement.	See the "Determining System Configuration Counts" section on page 16.
From the Firmware Load Information window in Cisco Unified Communications Manager Administration, make sure that the phone load type value matches the value that you recorded before the server replacement.	See the "Firmware Information" section on page 17.

Table 7 Post-Upgrade Tasks (continued)

Post-Upgrade Tasks	Important Notes
Reinstall the COP file enablers for any custom device types that do not ship with Cisco Unified Communications Manager.	Then, reboot the cluster and start post-replacement checklist again.
Compare the system version on each node in your cluster by using Cisco Unified Reporting and make sure that each node runs the same version.	See the "Obtaining System Version Information" section on page 17.
Reconfigure CDR destinations, if applicable.	See the "Accessing CDR Management Configuration" section on page 15.
Reconfigure all Trace and Log Central jobs.	See the "Recording Trace and Log Central Job Details" section on page 15.
Perform any system tests that you performed before the upgrade and verify that all test calls succeed.	
Configure the backup settings. Remember to back up your Cisco Unified Communications Manager data daily.	Refer to the *Disaster Recovery System Administration Guide*.
The locale, English_United_States, installs automatically on the server. If required, you can add new locales to the server.	Refer to the *Cisco Unified Communications Operating System Administration Guide*.
Cisco recommends that you implement authentication and encryption in your Cisco IP Telephony network.	Refer to the *Cisco Unified Communications Manager Security Guide*.
If you are using Microsoft Active Directory or Netscape Directory, enable synchronization with the LDAP server.	For more information on directories, refer to the *Cisco Unified Communications Manager System Guide*. For more information on enabling synchronization, refer to the *Cisco Unified Communications Manager Administration*.
Upgrade subscriber servers as subsequent Cisco Unified Communications Manager nodes in the cluster.	Subscriber servers automatically get defined as subsequent nodes in the database. Remember to enter the same security password for the first node. See the "Upgrading Subsequent Nodes in the Cluster" section on page 37

Table 7 Post-Upgrade Tasks (continued)

Post-Upgrade Tasks	Important Notes
If necessary, you can add additional, subsequent nodes to the cluster.	You must add additional subsequent nodes to the cluster by performing the following tasks: 1. Define all subsequent nodes in the cluster by adding the host name or IP address of subsequent Cisco Unified Communications Manager nodes to Cisco Unified Communications Manager Administration. For more information, refer to *Cisco Unified Communications Manager Administration Guide.* 2. Install the new application and configure subsequent Cisco Unified Communications Manager nodes in the cluster. See the "Upgrading Subsequent Nodes in the Cluster" section on page 37. Remember to enter the same security password that you used for the first node.
Configure netdump utility.	The netdump utility allows you to send data and memory crash dump logs from one server on the network to another. Servers that are configured as netdump clients send the crash logs to the server that is configured as the netdump server. The log file gets sent to the crash directory of the netdump server. In a Cisco Unified Communications Manager cluster, you must configure at least two nodes as netdump servers, so the first node and subsequent nodes can send crash dump longs to each other. Refer to the "Troubleshooting "Tools" section of the *Troubleshooting Guide* for details about how to use the netdump utility.
Reinstall customer background images, custom TFTP files, custom MoH files, and customer ring tones.	To upload these files, log in to Cisco Unified Communications Operating System Administration and navigate to the **Software Upgrades>Upload TFTP Server File** menu. See the *Cisco Unified Communications Operating System Administration Guide* for more information.
Install the required client-side plug-ins, such as Cisco Unified Communications Manager Cisco Unified Real-Time Monitoring Tool and Cisco Unified Communications Manager Attendant Console.	From Cisco Unified Communications Manager Administration, choose **Application > Plugins**. For more information, see the *Cisco Unified Communications Manager Administration Guide*.
Inform end users that they must reconfigure their ring tones and background images after the upgrade.	These settings do not get migrated.

Table 7 Post-Upgrade Tasks (continued)

Post-Upgrade Tasks	Important Notes
Assign the CAR administrator privileges after the upgrade.	After you use DMA to upgrade Cisco Unified Communications Manager, CAR users no longer have CAR administrator privileges after the upgrade and become standard end users. Refer to the "Configuring CAR Administrators, Managers, and Users" section in the *CDR Analysis and Reporting Administration Guide* for more information on how to configure CAR administrators.
Assign a value to the Phone Configuration setting Owner User ID.	The User ID gets recorded in the call detail record (CDR) for all calls made from this device. You must modify the Owner User ID to get proper reporting from the CAR window. **Note** Do not configure this field if you are using extension mobility. Extension mobility does not support device owners.

Uploading Licenses

After upgrading to Cisco Unified Communications Manager 7.1(2), you must obtain and upload a software feature license and upgrade the licenses for your nodes and devices. Only devices that are configured will receive licenses. You must have a valid login to Cisco.com to obtain licences.

Note Within your upgraded system's Cisco Unified Communications Manager Administration, check **System > Licensing > License Unit Report > Software License Version > SW Version** and verify that the software version that Cisco Unified Communications Manager Administration displays matches the version you upgraded to.

See the following sections for more information:

- Obtaining Software Feature Licenses, page 45
- Upgrading Product Licenses, page 46

Obtaining Software Feature Licenses

You must obtain a software feature license after the upgrade from Cisco Unified CallManager 4.x releases. A software feature license activates features on your system for the specified license version.

Use this procedure to obtain a software feature license:

Procedure

Step 1 Navigate to the License Registration web tool at http://www.cisco.com/go/license.

Step 2 Enter the Product Authorization Key (PAK) that you received with your Cisco Unified Communications Manager upgrade.

Step 3 Click **Submit**.

Step 4 Follow the system prompts. You must enter the MAC address of the Ethernet 0 NIC of the first node of the Cisco Unified Communications Manager cluster. You must also enter a valid e-mail address. The system sends the license file to you via e-mail by using the e-mail address that you provided.

Step 5 You must upload the software license file to the server with the matching MAC address that you provided in Step 4. See the "Uploading a License File" section on page 47.

Step 6 After uploading the license file, you must obtain and upload license files for existing nodes and devices, as described in "Upgrading Product Licenses" section on page 46.

Related Topics

- Uploading a License File, page 47
- Upgrading Product Licenses, page 46
- Post-Upgrade Tasks, page 39

Upgrading Product Licenses

When you upgrade from supported Cisco Unified CallManager Manager 4.x releases, the system calculates the licenses that are required for existing devices and nodes and generates an intermediate file (XML file) that contains this information. You use this file to obtain license files that you can upgrade into Cisco Unified Communications Manager Administration. You receive these licenses free of cost because you are already using these phones for a Cisco Unified CallManager 4.x release. Refer to the following instructions for Procedure 1.

As an alternative, you can obtain your product license directly from DMA. This enables you to have the license file immediately and not wait to receive it through e-mail. Refer to the following instructions for Procedure 2.

Use either Procedure 1 or Procedure 2 to obtain licenses for Cisco Unified Communications Manager when you are upgrading from supported 4.x releases.

Procedure 1

Step 1 After you complete the Cisco Unified Communications Manager upgrade process, navigate to Cisco Unified Communications Manager Administration and choose **System > Licensing > License File Upload**.

The License File Upload window displays.

Step 2 Choose the license file **licupgrade_7.1.lic** from the Existing Files drop-down list and click **View File**. The window refreshes and displays the information for the selected license. Copy all the information in this file. To copy the contents on this window, choose the appropriate text and choose **Ctrl-C** (Copy).

Step 3 Navigate to the License Registration web tool at https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet?FormId=806.

Step 4 Enter your login credentials.

Step 5 Enter the MAC address of the Ethernet 0 NIC of the first node of the Cisco Unified Communications Manager cluster.

Step 6 In the text box that is provided, paste the license file contents that you copied in Step 2 by using the appropriate keyboard shortcuts, such as **Ctrl-V**.

Step 7 Enter a valid e-mail address and click **Continue**. A license file generates.

The system sends the license file to you through e-mail using the e-mail address that you provided.

Step 8 You must upload the license file to the server with the matching MAC address that you provided in Step 5. See the "Uploading a License File" section on page 47.

Step 9 You can obtain licenses for new devices that you are adding to the upgraded system, if your system requires additional device license units. For more information, refer to the document *Cisco Unified Communications Manager Administration Guide*.

Procedure 2

Step 1 To specify a local directory destination for the license file licupgrade.lic, use the Data Migration Assistant's **Export > Storage Location > Destination Option for License File** tool.

Note Do not specify a mapped network directory for the Local Directory. If you do, DMA may not be able to create the destination folder.

Step 2 Upload the software license file to the server of the first node of the Cisco Unified Communications Manager cluster.

Step 3 After you upload the license file, you must obtain and upload license files for existing nodes and devices, as described in "Upgrading Product Licenses" section on page 46.

Related Topics

- Uploading a License File, page 47
- Obtaining Software Feature Licenses, page 45
- Post-Upgrade Tasks, page 39

Uploading a License File

Use the following procedure to upload a license file to the Cisco Unified Communications Manager server with the matching MAC address that is provided when a license file is requested. For information about obtaining a license file, see the "Obtaining Software Feature Licenses" section on page 45 and "Upgrading Product Licenses" section on page 46. The Cisco Unified Communications Manager server where the license file is loaded takes on the functionality of the license manager.

Note Upload the license file only on the first node of Cisco Unified Communications Manager cluster.

Procedure

Step 1 Choose **System > Licensing > License File Upload**.

The License File Upload window displays.

Step 2 The Existing License Files drop-down list box displays the license files that are already uploaded to the server.

Note To view the file content of any existing files, choose the file from the drop-down list box and click **View File**.

Step 3 To choose a new license file to upload, click **Upload License File**.

The Upload File pop-up window displays.

Step 4 To upload to the server, click **Browse** to choose a license file.

Note The format of the license file that you receive specifies CCM<timestamp>.lic. If you retain the *.lic extension, you can rename the license file. You cannot use the license if you edit the contents of the file in any way.

Step 5 Click **Upload**.

After the upload process is complete, the Upload Result file displays.

Step 6 Click **Close**.

Step 7 In the License File Upload window, the status of the uploaded file displays.

Note The system uploads the license file into the database only if the version that is specified in the license file is greater than or equal to the Cisco Unified Communications Manager version that is running in the cluster. If the version check fails, an alarm gets generated, and you should get a new license file with the correct version. The system bases the version check only on major releases.

Step 8 Restart the Cisco CallManager service after uploading the license file. For more information on restarting services, refer to the *Cisco Unified Serviceability Administration Guide*.

Related Topics

Post-Upgrade Tasks, page 39

Verifying Cisco Unified Communications Manager Services

To access Cisco Unified Communications Manager Administration or Cisco Unified Serviceability, you will need to use a web browser from a PC with network access to the Cisco Unified Communications Manager server.

To review service activation procedures and service recommendations, refer to the*Cisco Unified Serviceability Administration Guide*.

Related Topics

Post-Upgrade Tasks, page 39

Reverting to a Previous Version of Cisco Unified Communications Manager

If the upgrade from Cisco Unified Communications Manager Release 4.x to Cisco Unified Communications Manager Release 7.1(2) is unsuccessful, you can use the Disaster Recovery Disc to revert to a Windows-based version of Cisco Unified Communications Manager.

Caution If you revert to a previous version of Cisco Unified Communications Manager, you will lose any configuration changes that you made by using Cisco Unified Communications Manager 7.1(2).

To use the Disaster Recovery Disk, use this procedure:

Procedure

Step 1 Insert the Disaster Recovery disc and restart the system, so it boots from the CD. After the server completes the boot sequence, the Disaster Recovery menu displays.

Step 2 For Windows installation setup, enter **W**.

Step 3 To continue, enter **Yes**.

Caution If you continue, you will lose all the data that is currently on your hard drive.

The Disaster Recovery disc formats your hard drive, so you can reinstall a Windows-based version of Cisco Unified Communications Manager.

Step 4 Following the instructions in the installation guide for your Windows-based version of Cisco Unified Communications Manager, install Cisco Unified Communications Manager on the publisher server first and then on the subscriber nodes.

Step 5 Using the Backup and Restore Utility, restore the previously backed-up data to the servers. For more information, see the Backup and Restore Utility documentation for your version of BARS.

Examining Log Files

If you encounter problems with the installation, you can obtain and examine the install log files by entering the following commands in Command Line Interface.

To obtain a list of install log files from the command line, enter

```
CLI>file list install
```

To view the log file from the command line, enter

```
CLI>file view install log_file
```

where *log_file* is the log file name.

You can also view logs by using the Cisco Unified Communications Manager Cisco Unified Real-Time Monitoring Tool (RTMT). For more information on using and installing the Cisco Unified Communications Manager RTMT, refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations may be found at http://www.access.gpo.gov/bis/ear/ear_data.html.
