Upgrading Cisco Unified CallManager Release 5.1(3)

The 5.0(x) release of Cisco Unified CallManager uses a different installation framework than previous releases of Cisco Unified CallManager. Before upgrading to Cisco Unified CallManager 5.1(3), review all installation instructions carefully.

This document includes information about the following types of upgrades:

- Upgrading to Cisco Unified CallManager 5.1(3) from a Cisco Unified CallManager 4.x release
- Upgrading to Cisco Unified CallManager 5.1(3) from a Cisco Unified CallManager 5.x release
- Installing a software patch during the upgrade process
- Upgrading from Cisco Unified CallManager 5.1(3) to a later release.

Contents

This document contains the following topics:

Cisco Systems

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

Upgrade Overview

This section describes the types of upgrade that are described in this document.

Upgrading from a Cisco Unified CallManager 5.x Release

To upgrade from a Cisco Unified CallManager 5.x release to Release 5.1(3), or to upgrade to a later release after installing Release 5.1(3), see the "Upgrading from a Cisco Unified CallManager 5.x Release to Release 5.1(3) and Installing Upgrade Software After Upgrading to Cisco Unified CallManager 5.1(3)" section on page 33.

Upgrading from a Cisco Unified CallManager 4.x Release

Cisco Unified CallManager 5.1(3) uses a different installation framework than 4.x and older releases. The installation process allows you to perform a basic installation, upgrade from Cisco Unified CallManager 4.x to Cisco Unified CallManager 5.1(3), 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 CallManager 5.1(3) installation, which installs the software from the installation disc and does not use any imported data.
Applying a Patch	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 and perform both during the installation process.
Import Windows Data	This option allows you to import database information from a Cisco Unified CallManager 4.x system by using a file that the Data Migration Assistant (DMA) tool produces.

Note For basic installation instructions, which do not include upgrading from a previous release, see *Installing Cisco Unified CallManager.*

Related Documentation

Refer to the *Cisco Unified Communications Manager Documentation Guide* for further information about related Cisco IP telephony applications and products.

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	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html
Cisco Unified CallManager service releases	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml

Important Considerations

Before you proceed with the Cisco Unified CallManager installation, consider the following requirements and recommendations:

- Be aware that when you install Cisco Unified CallManager 5.1(3) 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 CallManager software on the first node, or publisher, server first and then on the subsequent nodes. You must configure the subsequent nodes on the first node before you can install the subsequent node.
- Enter the same security password on all servers in the cluster.
- Before you can install subsequent, or subscriber, nodes, you must first configure them on the first, or publisher, node.
- Install the Cisco Unified CallManager 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.
- You must have access to an SFTP server to back up Cisco Unified CallManager over a network.
- Do not attempt to perform any configuration tasks during the installation.
- Do not install any Cisco-verified applications until you complete installing Cisco Unified CallManager 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 28 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.
- Carefully read the instructions that follow before you proceed with the installation

Frequently Asked Questions About the Cisco Unified CallManager Installation

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

What Passwords do I Need to Specify?

During the Cisco Unified CallManager installation, you must specify the following user names and passwords:

- Administrator account

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

  – Cisco Unified Communications Operating System Administration

  – Disaster Recovery System

  – Command Line Interface

  The Administrator login must start with an alphabetic character, be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores. You can change the Administrator password or add a new Administrator account by using the command line interface. See the *Cisco Unified Communications Operating System Administration Guide* for more information.

- Application User password

  You use the Application User password as the default password for applications that are installed on the system, including Cisco Unified CallManager.

  You can change the application user password by using the web interface for each application. See the online help for more information.

- Database Access 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 Database Access Security password must start with an alphanumeric character, 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 CallManager.

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

Which servers does Cisco support for this installation?

For information about the supported servers, refer to the release notes for your version of Cisco Unified CallManager.

May I install other software besides Cisco Unified CallManager 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 CallManager with Cisco Unified CallManager 5.1(3).

Browser Requirements

You can access Cisco Unified CallManager Administration, Cisco Unified CallManager Serviceability, and Cisco Unified Communications Administration by using the following browsers:

- Microsoft Internet Explorer version 6.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 CallManager application. 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, C:, Floppy	Boot order: CD, C:, Floppy

Table 3 BIOS Configuration Settings for HP and IBM Servers (continued)

HP Servers	IBM Servers
Post F1 prompt: Delayed	Post F1 prompt: Delayed
Hyperthreading: Enabled	Hyperthreading: Enabled

Table 4 RAID Settings

MCS 7825 Servers (HP and IBM)	MCS 7835 Servers (HP and IBM)	MCS 7845 Servers (HP and IBM)
Software RAID	Logical drives: 1	Logical drives: 2
Software RAID **Note** For the HP 7825H1 and the IBM 7825I1, SATA RAID gets enabled, and the RAID type specifies 1(1+0), with one logical drive.	RAID type: 1(1+0)	RAID type: 1(1+0)

Upgrading from a Cisco Unified CallManager 4.x Release

Ensure the Cisco Unified CallManager server with the publisher database is configured as the first node and Cisco Unified CallManager servers with subscriber databases are configured as subsequent nodes. This section contains the procedures for upgrading the first and subsequent nodes. Review the following sections carefully before you perform the upgrade:

Performing Pre-Upgrade Tasks

Perform the following tasks before you begin the upgrade:

	Pre-Upgrade Task	Important Notes
Step 1	Verify that you meet the system requirements for upgrading Cisco Unified CallManager 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	Verify the integrity of any new server hardware (such as hard drives and memory) by running any manufacturer-provided utilities.	
Step 3	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 4	Obtain and store COP files for any locales that are installed on the server.	You might need to reinstall locales after doing the replacement.
Step 5	Do not change computer names or IP addresses, or add more nodes to the cluster.	
Step 6	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 7	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.
Step 8	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.	
Step 9	Do not run Network Address Translation (NAT) or Port Address Translation (PAT) between Cisco Unified CallManager nodes.	
Step 10	Record all the critical services and their activation status by using the Cisco Unified CallManager Real-Time Monitoring Tool (RTMT).	
Step 11	Using the Syslog viewer in the Cisco Unified CallManager Real-Time Monitoring Tool (RTMT), locate any events that have a severity of Error or higher.	
Step 12	Record the details of all Trace and Log Central jobs.	
Step 13	Record CDR Management configuration and destinations, if applicable.	

	Pre-Upgrade Task	Important Notes
Step 14	From Cisco Unified CallManager Administration, determine the number of specific items that are configured on the server.	
Step 15	From Cisco Unified CallManager Administration, record all the phone loads and device types that display on the Firmware Load Information window.	
Step 16	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.	
Step 17	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.*
Step 18	Perform the recommended backup procedures on the publisher server. Back up every database that is associated with your Cisco Unified CallManager server.	Refer to *Cisco IP Telephony Backup and Restore System (BARS) Administration Guide*.
Step 19	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.	For more information on CAR, refer to the *CDR Analysis and Reporting Administration Guide.*
Step 20	If you do not need to carry over your CDR data to Cisco Unified CallManager 5.1(3), Cisco recommends that you purge the CDR data before you run DMA.	Purging the CDR data speeds up the migration process and decreases the size of the DMA TAR file.
Step 21	Export the data on the current Cisco Unified CallManager 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 two files: • 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 backup information file that contains Cisco Unified CallManager 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. For more information on data migration, refer to *Data Migration Assistant Administration Guide.* You will be choosing an installation option based on the location of the DMA output configuration file and TAR file.
Step 22	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 9.

	Pre-Upgrade Task	Important Notes
Step 23	Record the Host Name/IP Address value that is configured on the Server Configuration Settings window of the Cisco Unified CallManager 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 5.1(3) Server" section on page 13
Step 24	Familiarize yourself with the navigation options within the installation wizards.	See "Navigating Within the Installation Wizard" section on page 14.
Step 25	Make sure that you have the 5.1(3) 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 CUCM nodes can access.	See the "Applying a Patch" section on page 25 for more information.

Gathering Information for an Installation

Use Table 5 to record the information about your server. Gather this information for each Cisco Unified CallManager 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 should make copies of this table and record your entries for each server in a separate table.

Note Because some of the fields are optional, they may not apply to your configuration. For example, you may 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 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 passwords, but you cannot change the original administrator password.

Table 5 Node Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
Administrator Password Your entry:	This field specifies the password 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. 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 Password Your entry:	You use the Application User password as the default password for applications that are installed on the system, including Cisco Unified CallManager and Cisco Unified CallManager Serviceability. **Note** When you initially log in, use the default user name: CCMAdministrator.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set password**
Country Your entry:	Choose the appropriate country for your installation.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set web-security**
DHCP Your entry:	Choose **Yes** if you want to use DHCP to automatically configure the network settings on your server. 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 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**

Table 5 Node Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
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 hostnames) for all network devices in your Cisco Unified Communications network.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network dns**
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 CallManager.	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 CallManager.	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.
Gateway Address Your entry:	Enter the IP address of the network gateway. If you do not have a gateway, you must still fill in this field by setting it to 255.255.255.255. Not having a gateway may limit you to only being able to communicate with devices on your subnet.	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.	No, you cannot change the entry after installation.
IP Address Your entry:	Enter the IP address of your server.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network IP**
IP Mask Your entry:	Enter the IP subnet mask of this machine.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network ip eth0**

Table 5 Node Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
Location Your entry:	Choose the appropriate location for the server.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set web-security**
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 for your network in bytes. If you are unsure of the MTU setting for your network, use the default value. Default: 1500 bytes	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. **Note** You can enter up to five NTP servers.	Yes, you can change the entry after installation.
Organization Your entry:	Enter the name of your organization.	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**

Table 5 Node Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
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.	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**

Handling Network Errors During Installation

During the installation 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 (Check Install)**—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 5.1(3) 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 5.1(3) 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 5.1(3) 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 5.1(3) 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 5.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.
- If the Host Name/IP Address (Servername) was an IP address, the installation program compares this Servername to the provisioned IP Address for the 5.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 5.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 5.1(3) server without having to preserve the IP Address or Host Name. The IP Address and/or Host name of the 5.1(3) 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.

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)

Upgrading the First Cisco Unified CallManager Node

To upgrade and migrate data from a publisher server, you must perform the following tasks.

1. Verify that you have completed all pre-upgrade tasks. See the "Performing Pre-Upgrade Tasks" section on page 7.
2. Familiarize yourself with navigation within the installation wizard. See the "Navigating Within the Installation Wizard" section on page 14.
3. Know which installation options to choose. See Table 1.
4. Configure the hardware with the hardware configuration disc. See the "Configuring the Hardware" section on page 5.
5. Install the new operating system on the first node. See the "Installing the New Operating System and Application on the First Node" section on page 15
6. Perform the appropriate post-upgrade tasks. See the "Post-Upgrade Tasks" section on page 28.

Installing the New Operating System and Application on the First Node

Use this procedure to begin installing the operating system and Cisco Unified CallManager application on the first Cisco Unified CallManager node:

Caution Before beginning this procedure, ensure that you have backed up the data on your current Windows-based version of Cisco Unified CallManager. For more information, see the *Cisco Unified Communications Backup* and *Restore System Administration Guide* for your version of BARS.

Procedure

Step 1 Insert the installation DVD into the tray and restart the server, so it boots from the DVD. After the server completes the boot sequence, the DVD Found window displays.

Step 2 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 CallManager preinstalled, you do not need to install from a DVD, unless you want to reimage the server with a later product release. Go directly to the "If You Choose Skip" procedure on page 16.

Step 3 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 of the software from Cisco.com or obtain another disc directly from Cisco.

Step 4 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 warning:

```
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.

Step 5 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. To continue with the installation, choose **Yes**, or choose **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.

Step 6 To configure the platform now, choose **Proceed**. If you want to configure the platform later, choose **Skip.**

- If you want to install and configure the software at this time, choose **Proceed** and skip to the "If You Choose Proceed" section on page 17.
- If you want to install the software now and configure it later, choose **Skip** and continue with the "If You Choose Skip" section on page 16.

Note Choosing **Skip** allows you to lay down the operating system on the machine first and enter the configuration information later. With this method, your total time required to complete the installation time may increase.

If You Choose Skip

Start here if you have a server that has Cisco Unified CallManager preinstalled or if you chose **Skip** on Platform Installation Wizard window.

Step 7 After the system restarts, the Preexisting Installation Configuration window displays. If you have configuration information on a USB drive or on a diskette, insert it now.

Note If a popup window states that the system detected new hardware, press any key and then choose **Install** from the next window.

Note If you have a file that the Data Migration Assistant created, see the *Data Migration Assistant User Guide* for more information.

Step 8 To continue, choose **OK**.

The Platform Installation Wizard window displays.

Step 9 To continue with the installation, choose **Proceed**.

The Upgrade During Install window displays. Continue with the "If You Choose Proceed" section on page 17.

If You Choose Proceed

Step 10 Choose the type of installation to perform by doing the following steps. See Table 1 for more information on installation options:

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 25.
- To skip this step, choose **No**.
- To return to the previous window, choose **Back**.

b. In the Import windows Data window, choose **Yes**. Continue with the "Windows Upgrade" section on page 17.

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

Windows Upgrade

When you choose Import Windows Data, 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 11 In the Import Windows Data window, choose **Yes**.

The Timezone Configuration window displays.

Step 12 Choose the appropriate time zone for the server and then choose **OK**.

The Auto Negotiation Configuration window displays.

Step 13 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** and continue with Step 15.

  The MTU Configuration window displays.

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

- To disable automatic negotiation, choose **No** and continue with Step 14.

  The NIC Speed and Duplex Configuration window displays.

Step 14 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 15 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, which is 1500 bytes.

Caution If you configure the MTU size incorrectly, 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 16 For network configuration, you can choose to either set up a 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** and continue with Step 19.

  The Administrator Login Configuration window displays.

- If you want to configure a static IP address for the node, choose **No** and continue with Step 17.

  The Static Network Configuration window displays.

Step 17 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 18 To enable DNS, choose **Yes**, enter your DNS client information, and choose **OK**. See Table 5 for field descriptions.

The Administrator Login Configuration window displays.

Step 19 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 Information window displays.

Step 20 Enter your certificate signing request information and choose **OK**.

The First Node Configuration window displays.

Step 21 You must configure this node as the first node in the cluster. To continue, choose **Yes**.

The Network Time Protocol Client Configuration window displays.

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 stratums 1-9). Subsequent nodes in the cluster will get their time from the first node.

Step 22 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 the external NTP server is stratum 9 or higher (meaning stratums 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. Choose **Proceed** to continue with the installation.

  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 23 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 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 24 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 25 Choose **OK**.

The DMA Retrieval Mechanism Configuration window displays.

Step 26 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 the 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.

Step 27 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 DMA file is located on a Windows server, check with your system administrator for the correct directory path.

The Platform Configuration Confirmation window displays.

Step 28 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 29 Enter the Application User Password from Table 5 and confirm the password by entering it again.

Step 30 Choose **OK**.

The End User Password/PIN Configuration window displays.

Step 31 Enter 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 32 To continue, choose **OK**, or to choose a different DMA file, choose **Back**.

When you choose **OK**, the Installation program assigns a Host Name/ IP Address (Servername) to the 5.1(3) server by comparing the value in the DMA file to the value that is configured on the 5.1(3) system. For more information, refer to the "Assigning the Host Name/IP Address (Servername) to the 5.1(3) Server" section on page 13.

Step 33 If a mismatch exists between these values, you are prompted to Proceed or Cancel. Select **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 34 If no mismatch exists, or you select **Proceed**, the Platform Configuration Confirmation window displays.

Step 35 To continue, choose **OK**.

Step 36 When the installation process completes, you get prompted to log in by using the Administrator account and password.

Step 37 Complete the post-upgrade tasks that are listed in the "Post-Upgrade Tasks" section on page 28.

Upgrading Subsequent Nodes in the Cluster

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

On a subsequent node, you can either install the software version on the disc or retrieve a more recent service release from a remote server. The subsequent nodes will retrieve data from the first node at the end of the installation.

To upgrade a subsequent node in the cluster from Cisco Unified CallManager 4.x to Cisco Unified CallManager 5.1(3), perform the following steps:

1. Upgrade the first node, the Cisco Unified CallManager 4.x publisher server, to Cisco Unified CallManager 5.1(3). See the "Installing the New Operating System and Application on the First Node" section on page 15.
2. Using Cisco Unified CallManager Administration on the first node, configure the subsequent nodes.
3. Ensure that the subsequent nodes have network connectivity to the first node.
4. Install the new operating system and Cisco Unified CallManager application from a DVD on the subsequent node, upgrading to a Service Release as needed. See the "Install the New Operating System and Application on Subsequent Nodes" section on page 21.s

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

Install the New Operating System and Application on Subsequent Nodes

Use this procedure to begin installing the operating system and Cisco Unified CallManager application on a subsequent node.

Caution Before beginning this procedure, ensure you have already upgraded the Cisco Unified CallManager 4.x publisher server, configured the subsequent node on the Cisco Unified CallManager 5.1(3) first node, and have network connectivity to the first node. Failure to meet these conditions can cause the installation to fail.

Step 1 Insert the installation DVD into the tray and restart the server, so it boots from the DVD. After the server completes the boot sequence, the DVD Found window displays.

Step 2 To perform the media check, choose **Yes**, or to skip the media check, choose **No**.

Step 3 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 CallManager preinstalled, you do not need to install from a DVD, unless you want to reimage the server with a later product release. Go directly to the "If You Choose Skip" procedure on page 22.

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 of the software from Cisco.com or obtain another disc directly from Cisco.

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 warning:

```
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 to Cisco support.
- The installation process next verifies RAID configuration and BIOS settings.

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

Step 6 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. To continue with the installation, choose **Yes**, or choose **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.

Step 7 To configure the platform now, choose **Proceed**. If you want to configure the platform later, choose **Skip.**

- If you want to install and configure the software at this time, choose **Proceed** and skip to the "If You Choose Proceed" section on page 23.
- If you want to install the software now and configure it later, choose **Skip** and continue with the "If You Choose Skip" section on page 22.

Note Choosing **Skip** allows you to lay down the operating system on the machine first and enter the configuration information later. With this method, your total time required to complete the installation time may increase.

If You Choose Skip

Start here if you have a server that has Cisco Unified CallManager preinstalled or if you chose **Skip** on Platform Installation Wizard window.

Step 8 After the system restarts, the Preexisting Installation Configuration window displays. If you have configuration information on a USB drive or on a diskette, insert it now.

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

Step 9 To continue, choose **OK**.

The Platform Installation Wizard window displays.

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

The Install During Upgrade window displays. Continue with the "If You Choose Proceed" section on page 23.

If You Choose Proceed

Step 11 choose the type of installation to perform by doing the following steps. See Table 5 for more information on installation options:

a. In the Upgrade During Install 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 25.
- To skip this step, choose **No**.
- To return to the previous window, choose **Back**.

b. In the Windows Upgrade window, choose **No**.

c. In the Basic Install window, choose **Continue** to install the software version on the DVD or configure the preinstalled software with the basic installation. Continue with the "Basic Installation" section on page 23.

Basic Installation

The Timezone Configuration window displays.

Step 12 Choose the appropriate time zone for the server and then choose **OK**.

The Auto Negotiation Configuration window displays.

Step 13 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** and continue with Step 15.

  The MTU Configuration window displays.

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

- To disable automatic negotiation, choose **No** and continue with Step 14.

  The NIC Speed and Duplex Configuration window displays.

Step 14 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 15 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, which is 1500 bytes.

Caution If you configure the MTU size incorrectly, 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 16 For network configuration, you can choose to either set up a 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** and continue with Step 19.

  The Administrator Login Configuration window displays.

- If you want to configure a static IP address for the node, choose **No** and continue with Step 17.

  The Static Network Configuration window displays.

Step 17 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 18 To enable DNS, choose **Yes**, enter your DNS client information, and choose **OK**. See Table 5 for field descriptions.

The Administrator Login Configuration window displays.

Step 19 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 Information window displays.

Step 20 Enter your certificate signing request information and choose **OK**.

The First Node Configuration window displays.

Step 21 To configure this server as a subsequent node in the cluster, choose **No**.

The First Node Access Configuration window displays.

Step 22 On the First Node Configuration window, read the Warning and make sure you have correctly configured the first node. Click **OK** to continue with the installation of the subsequent node.

The Network Connectivity Test Configuration window displays.

Step 23 During installation of a subsequent node, the system checks to ensure that the subsequent node can connect to the first node.

- To pause the installation after the system successfully verifies network connectivity, choose **Yes**.
- To continue the installation with a pause, choose **No**.

The First Node Access Configuration window displays.

Step 24 Enter the first node connectivity information from Table 5 and choose **OK**.

The system checks for network connectivity.

If you chose to pause the system after the system successfully verifies network connectivity, the Successful Connection to First Node window displays. Choose **Continue**.

Note If the network connectivity test fails, the system always stops and allows you to go back and reenter the parameter information.

The SMTP Host Configuration window displays.

Step 25 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.

The Platform Configuration Confirmation window displays.

Step 26 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 27 To log in, enter the account name **CCMAdministrator** and the password that you entered during installation.

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

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 apply a patch installation.

Note You can upgrade to any higher release, so long as you have a full patch, not an ES or an SR, in which case you can only upgrade to a later service release of the same number.

If you are upgrading from Cisco Unified CallManager Release 5.x, the upgrade file name uses the following format:

```
cisco-ipt-k9-patchX.X.X.X-X.tar.gz.sgn
```

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

Note Do not rename the patch file before you install it because the system will not recognize it as a valid file.

Note Do not unzip or untar the file. If you do, the system may not be able to read the upgrade files.

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.

Note You can only apply one patch during the installation process.

Procedure

Step 1 The Install Upgrade Retrieval Mechanism Configuration window displays.

Step 2 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 27.
- **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 27.
- **LOCAL**—Retrieves the upgrade file from a local CD or DVD. Continue with the "Upgrading from a Local Disk" section on page 26.

Upgrading from a Local Disk

Before you can upgrade from a local disk, you must download the appropriate patch file from Cisco.com and copy the file to a CD or DVD. Because of the size of the patch files, you will need to copy it to a DVD in most cases.

Procedure

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

Note You only need to enter the patch directory when the patch is not stored in the root directory of the CD or DVD. If the patch is stored in the root directory, enter a slash (/) in the directory field.

The Install Upgrade Patch Selection Validation window displays.

Step 2 The window displays the patch file that is available on the CD or 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 running the upgraded software version.

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

Step 4 Choose Proceed to continue the installation.

The Platform Installation Wizard window displays.

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

If you choose **Proceed**, the Apply Patch window displays. Continue with Step 6.

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**.

Note You can only apply one patch during the upgrade process.

The Windows Upgrade window displays.

Step 7 Choose **No** and continue with upgrade procedure for the type of node that you are installing.

Upgrading from a Remote Server

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

Procedure

Step 1 In the Auto Negotiation Configuration window, 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 3.
- To disable automatic negotiation, choose **No**. The NIC Speed and Duplex Configuration window displays. Continue with Step 2.

Step 2 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 3 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, 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 4 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 7.
- If you want to configure static IP addresses for the node, choose **No**. The Static Network Configuration window displays.

Step 5 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 6 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 7 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, check with your system administrator for the correct directory path.

The Install Upgrade Patch Selection window displays.

Step 8 Choose the upgrade patch to install. The system downloads, unpacks, and installs the patch and then restarts the system that is running the upgraded software version.

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

Step 9 To continue the installation, choose **Proceed**.

The Platform Installation Wizard window displays.

Step 10 To continue the installation, choose **Proceed**, or click **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 11 When the Apply Patch window displays, choose **No**.

Note You can only apply one patch during the upgrade process.

The Windows Upgrade window displays.

Step 12 Choose **No** and continue with the installation procedure for the type of node that you are installing.

Post-Upgrade Tasks

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

Table 7 Post-Upgrade Tasks

Post-Upgrade Tasks	Important Notes
Upgrade your product licenses.	See the "Upgrading Product Licenses" section on page 32.
Verify that all appropriate Cisco Unified CallManager services started. Verify that you can make internal calls. Verify that you can place and receive a call across gateways.	Refer to the following documents: • *Cisco Unified CallManager Serviceability Administration Guide* • *Cisco Unified CallManager Serviceability System Guide* See the "Verifying Cisco Unified CallManager Services" section on page 33.

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. For information about performing these tasks and about Cisco Unified CallManager security, refer to the *Cisco Unified CallManager Security Guide*.
Using the Cisco Unified CallManager Real-Time Monitoring Tool (RTMT), make sure that all the registration information values match the values that you recorded before the server replacement.	
Using the Cisco Unified CallManager Real-Time Monitoring Tool (RTMT), make sure that all the critical services and their status match those that you recorded before the server replacement.	
Using the Syslog viewer in the Cisco Unified CallManager Real-Time Monitoring Tool (RTMT), locate any events that have a severity of Error or higher.	

Table 7 Post-Upgrade Tasks (continued)

Post-Upgrade Tasks	Important Notes
Using the Syslog viewer in the Cisco Unified CallManager 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: • 0 (Not Started)—No Subscribers exist or the Database Layer Monitor service is not running and has not been running since the subscriber was installed. • 1 (Started)—Replication is currently being setup. • 2 (Finished)—Replication setup was completed and is working. • 3 (Broken)—Replication failed during setup and is not working. 3=Data is not replicating correctly; 4 = Replication is not setup correctly).	To access the appropriate object and counter, use the following procedure: 1. Perform one of the following tasks: • In the Quick Launch Channel, click **Performance**; then, click the **Performance** icon. • Choose **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 CallManager Administration, 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.	
From the Firmware Load Information window in Cisco Unified CallManager Administration, make sure that the phone load and device type values match those that you recorded before the server replacement.	
From the Firmware Load Information window in Cisco Unified CallManager Administration, make sure that the phone load and device type values match those that you recorded before the server replacement.	If a device type is missing, you may need to reinstall the COP file enabler for that type. Then, reboot the cluster and start post-replacement checklist again.
Compare the system version on each node in your cluster by using Cisco Unified Communications Operating System Administration and make sure that it matches the version that you recorded before the replacement.	
Reconfigure CDR destinations, if applicable.	
Reconfigure all Trace and Log Central jobs.	

Table 7 Post-Upgrade Tasks (continued)

Post-Upgrade Tasks	Important Notes
Perform any system tests that you performed before the replacement and verify that all test calls succeed.	
Configure the backup settings. Remember to back up your Cisco Unified CallManager 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 CallManager 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 CallManager System Guide.* For more information on enabling synchronization, refer to the *Cisco Unified CallManager Administration Guide.*
Upgrade subscriber servers as subsequent Cisco Unified CallManager 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 20
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 CallManager nodes to Cisco Unified CallManager Administration. For more information, refer to *Cisco Unified CallManager Administration Guide.* 2. Install the new application and configure subsequent Cisco Unified CallManager nodes in the cluster. See the "Upgrading Subsequent Nodes in the Cluster" section on page 20. Remember to enter the same security password that you used for the first node.
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.

Table 7 Post-Upgrade Tasks (continued)

Post-Upgrade Tasks	Important Notes
Install the required client-side plug-ins, such as Cisco Unified CallManager Real-Time Monitoring Tool and Cisco CallManager Attendant Console.	From Cisco Unified CallManager Administration, choose **Application>Plugins**. For more information, see the *Cisco Unified CallManager Administration Guide*.
Inform end users that they must reconfigure their ring tones and background images after the upgrade.	These settings do not get migrated.

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 Cisco Unified CallManager 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 CallManager Administration. You receive these licenses free of cost because you are already using these phones for a Cisco Unified CallManager 4.x release.

Note You need to upgrade product licenses only if you upgrade from a 4.x release to the 5.1(3) release. You do not need to upgrade licenses if you upgrade from a 5.x release to release 5.1(3).

Use the following procedure to obtain licenses for Cisco Unified CallManager when upgrading from supported 4.x releases.

Procedure

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

The License File Upload window displays.

Step 2 Choose the license XML file from the Existing Files drop-down list, and click **View File**. A pop-up window displays that has the license information for existing devices and nodes. Copy this information. To copy the contents on this window, you can use **Ctrl-A** (Select All) and **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 the MAC address of the Ethernet 0 NIC of the first node of the Cisco Unified CallManager cluster.

Step 5 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 6 Enter a valid e-mail address and click **Continue**. A license file generates.

The system sends the license file to you via E-mail using the E-mail address that you provided.

Step 7 You must upload the license file to the server with the matching MAC address that you provided in Step 4. See the "Upgrading Product Licenses" section on page 32.

Step 8 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 *Installing Cisco Unified CallManager.*

Verifying Cisco Unified CallManager Services

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

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

Procedure

Step 1 Open a web browser on a computer with network access to the Cisco Unified CallManager server.

Step 2 Enter the following URL:

http://*ccm_server***:8080/ccmadmin**

where *ccm_server* specifies the IP address or hostname of the Cisco Unified CallManager server.

Step 3 Enter the Cisco Unified CallManager Administrator user name and password.

Step 4 From the Navigation menu, choose Cisco Unified CallManager Serviceability and click **Go**.

Step 5 Navigate to **Tools>Service Activation**.

Step 6 Verify that all migrated services are running.

Upgrading from a Cisco Unified CallManager 5.x Release to Release 5.1(3) and Installing Upgrade Software After Upgrading to Cisco Unified CallManager 5.1(3)

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

When you install upgrade software, you install the software on the inactive partition. The system continues to function normally while you are installing the software. When you are ready, you activate the inactive partition and reboot the system with the new upgrade software. The current active partition will then get identified as the inactive partition when the system restarts. The current software remains in the inactive partition until the next upgrade. You must activate new software on the first node before activating it on all other nodes.

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

Upgrading the System

You can install a patch or upgrade version from a DVD (local source) or from a computer (remote source) that the Cisco Unified CallManager server can access.

You must install the upgrade patch on the first node before installing it on subscriber nodes. You can install the upgrade patch on multiple subscriber servers at the same time. When you are ready to activate the new version, you must activate the new software on the first node before activating it on all other nodes.

From Local Source

You can install software from a CD or DVD that is located in the local disc drive and then start the upgrade process.

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

To install or upgrade software from a CD or DVD, follow this procedure:

Procedure

Step 1 Download the appropriate upgrade file from Cisco.com.

Note Do not unzip or untar the file. If you do, the system may not be able to read the upgrade files.

Step 2 Copy the upgrade file to a writeable CD or DVD.

Step 3 Insert the new CD or DVD into the disc drive on the local server that is to be upgraded.

Note Because of their size, some upgrade files may not fit on a CD and will require a DVD.

Step 4 Open Cisco Unified Communications Operating System Administration directly by entering the following URL:

http://*server-name*/**iptplatform**

where *server-name* specifies the host name or IP address of the Cisco Unified CallManager server.

Step 5 Enter your Administrator username and password.

Step 6 Choose **Software Upgrades>Install/Upgrade**.

Step 7 For the software location source, choose **DVD/CD**.

Step 8 If you burned the patch file to a subdirectory on the CD or DVD, enter the path in the Directory field.

Step 9 To continue the upgrade process, click **Next**.

Step 10 Choose the upgrade version that you want to install and click **Next**.

Step 11 In the next window, monitor the progress of the download, which includes the filename and the number of megabytes that are getting transferred.

When the download completes, the Checksum window displays.

Step 12 Verify the checksum value against the checksum for the file that you downloaded that is shown on Cisco.com.

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

Step 13 After determining that the checksums match, click **Next** to proceed with the software upgrade.

A Warning window displays the current and upgrade software versions.

Step 14 To continue with the software upgrade, click **Next**.

The Post Installation Options window displays.

Step 15 Choose whether you want the system to automatically reboot to the upgraded partition after installing the upgrade software:

- To install the upgrade and automatically reboot to the upgraded partition, choose **Reboot to upgraded partition**.
- To install the upgrade and then manually reboot to the upgraded partition at a later time, choose **Do not reboot after upgrade**.

Step 16 Click **Upgrade**.

The Upgrade Status windows displays and displays the Upgrade log.

Step 17 When the installation completes, click **Finish**.

Step 18 To restart the system and activate the upgrade, choose **Restart>Switch Versions**.

The Switch Software Version window displays.

Step 19 To switch software versions and restart the system, click **Switch Versions**.

The Switch Software Version window displays.

When you verify that you want to restart the system, the system restarts by running the upgraded software.

From Remote Source

To install software from a network drive or remote server, use the following procedure.

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

Procedure

Step 1 Navigate to **Software Upgrades>Install**.

Step 2 For the Software Location Source, choose **Remote File System**.

Step 3 Enter the directory name for the software upgrade, if required.

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, check with your system administrator for the correct directory path.

Step 4 Enter the required upgrade information as described in the following table:

Field	Description
Remote Server	Host name or IP address of the remote server from which software will be downloaded.
Remote User	Name of a user who is configured on the remote server.
Remote Password	Password that is configured for this user on the remote server.
Download Protocol	Choose sftp or ftp.

Note You must choose **Remote File System** to enable the remote server configuration fields.

Step 5 Click **Next**.

The system checks for available upgrades.

Step 6 Choose the upgrade or option that you want to install and click **Next**.

Step 7 In the next window, monitor the progress of the download, which includes the filename and the number of megabytes that are getting transferred.

When the download completes, the Checksum window displays.

Step 8 Verify the checksum value against the checksum for the file that you downloaded that was shown on Cisco.com.

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

Step 9 After determining that the checksums match, click **Next** to proceed with the software upgrade.

A Warning window displays the current and upgrade software versions.

Step 10 To continue with the software upgrade, click **Next**.

The Post Installation Options window displays.

Step 11 Choose whether you want the system to automatically reboot to the upgraded partition after installing the upgrade software:

- To install the upgrade and automatically reboot to the upgraded partition, choose **Reboot to upgraded partition**.

– To install the upgrade and then manually reboot to the upgraded partition at a later time, choose **Do not reboot after upgrade**.

Step 12 Click **Upgrade**.

The Upgrade Status window, which shows the Upgrade log, displays.

Step 13 When the installation completes, click **Finish**.

Step 14 To restart the system and activate the upgrade, choose **Restart>Switch Versions**.

The Switch Software Version window displays.

When you verify that you want to restart the system, the system restarts by running the upgraded software.

Reverting to a Previous Version

If an upgrade seems unstable or for some other reason you want to revert to the software version before the upgrade, you can restart your system and switch to the software version on the inactive partition.

Procedure

Step 1 Open Cisco Unified Communications Operating System Administration directly by entering the following URL:

http://*server-name*/**iptplatform**

where *server-name* is the host name or IP address of the Cisco Unified CallManager server.

Step 2 Enter your Administrator username and password.

Step 3 Choose **Restart>Switch Versions**.

The Switch Software Version window displays.

When you verify that you want to restart the system, the system restarts running the upgraded software.

Using the Cisco Unified CallManager Recovery Disc

In case of a system emergency, you can use the Cisco Unified CallManager Recovery disc to revert to a Windows-based version of Cisco Unified CallManager or to force the system to restart on the inactive partition.

Reverting to a Previous Version of Cisco Unified CallManager

If the upgrade from Cisco Unified CallManager 4.x to Cisco Unified CallManager 5.1(3) is unsuccessful, you can use the Cisco Unified CallManager Recovery disc to revert to a Windows-based version of Cisco Unified CallManager.

Caution If you revert to a previous version of Cisco Unified CallManager, you will lose any configuration changes that you made by using Cisco Unified CallManager 5.1(3).

To use the Cisco Unified CallManager Recovery disk, use this procedure:

Procedure

Step 1 Insert the Cisco Unified CallManager 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 preinstallation 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 Cisco Unified CallManager Recovery disc formats your hard drive, so you can reinstall a Windows-based version of Cisco Unified CallManager.

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

Step 5 Using the Cisco Unified Communications Backup and Restore System (BARS), restore the previously backed-up data to the servers. For more information, see the *Cisco Unified Communications Backup and Restore System Administration Guide* for your version of BARS.

Switching Partitions

If the system cannot start on the current partition, you can use the Cisco Unified CallManager Recovery disc to force it to switch to the inactive partition and start running the software version on that partition.

Caution If you force the system to restart on the inactive partition, you will lose any configuration changes that you made after you upgraded to the current partition.

To force the system to switch partitions and restart, follow this procedure:

Procedure

Step 1 Insert the Cisco Unified CallManager 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 To restart the server, so it is running the software on the currently inactive partition, enter **S**.

Step 3 Press **Enter**.

The server restarts.

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 CallManager Real-Time Monitoring Tool (RTMT). For more information on using and installing the Cisco Unified CallManager RTMT, refer to the *Cisco Unified CallManager Serviceability 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.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html. If you require further assistance please contact us by sending email to export@cisco.com.
