



Installing Cisco Unified Communications Manager Release 6.0(1)

Because the 6.0(1) release of Cisco Unified Communications Manager uses a different installation framework than previous releases of Cisco Unified Communications Manager, review all installation instructions carefully before you install Cisco Unified Communications Manager 6.0(1).

This document includes information about installing Cisco Unified Communications Manager Release 6.0(1) on one server or many servers in a cluster environment.

For information about upgrading from a Windows-based release (4.x) of Cisco Unified Communications Manager to an appliance-based release (5.0 and higher), refer to *Upgrading Cisco Unified Communications Manager*.

Contents

This document contains the following topics:

- [Related Documentation](#)
- [Important Considerations](#)
- [Frequently Asked Questions About the Installation](#)
- [Browser Requirements](#)
- [Configuring the Hardware](#)
- [Gathering Information for an Installation](#)
- [Using the Cisco Unified Communications Answer File Generator](#)
- [Handling Network Errors During Installation](#)
- [Installation Overview](#)
- [Installing the New Operating System and Application](#)
- [Post-Installation Tasks](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines](#)



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

© 2007 Cisco Systems, Inc. All rights reserved.

Related Documentation

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

[Table 1](#) lists URLs for software and additional documentation.

Table 1 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 installation, consider the following requirements and recommendations:

- Be aware that when you install on an existing server, the hard drive gets formatted, and all existing data on the drive gets overwritten.
- Install the Cisco Unified Communications Manager software on the first node or publisher server first and then on the subsequent nodes.
- Make sure that the subsequent node servers that you are installing can connect to the first node server during the installation.
- Enter the same security password on all servers in the cluster.
- Install the software during off-peak hours or a maintenance window to avoid impact from 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 attempt to perform any configuration tasks during the installation.
- Do not install any Cisco-verified applications until you complete the installation.
- Directory names and filenames that you enter while running the installation program are case-sensitive.
- Carefully read the instructions that follow before you proceed with the installation.

Frequently Asked Questions About the Installation

The following section contains information about commonly asked questions and responses. Review this section carefully before you begin the installation.

The entire installation process, excluding pre- and post-installation tasks, takes 45 to 90 minutes per server, depending on your server type. Before you install Cisco Unified Communications Manager, consider the size of your cluster.

What Passwords do I Need to Specify?

During the 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 for as the default password for applications that are installed on the system.

You can change the application user password 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.

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 Communications Manager.

May I install other software 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 6.0(1).

Browser Requirements

You can access Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, Cisco Unified Communications Operating System Administration, and Disaster Recovery System 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 Communications Manager application. See [Table 2](#) for the BIOS settings and [Table 3](#) 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 that are found on both the IBM and HP servers to manually configure the RAID and BIOS settings, as shown in [Table 2](#) and [Table 3](#).

Table 2 *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
Post F1 prompt: Delayed	Post F1 prompt: Delayed
Hyperthreading: Enabled	Hyperthreading: Enabled

Table 3 *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	RAID type: 1(1+0)	RAID type: 1(1+0)
Note For the HP 7825H1 and the IBM 7825I1, SATA RAID is enabled, and the RAID type specifies 1(1+0), with one logical drive.		

Gathering Information for an Installation

Use [Table 4](#) to record the information about your 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 should 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.



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 4 Configuration Data

Configuration Data	Your Entry	Can Entry Be Changed After Installation
Administrator Password		Yes. CLI > set password admin
Application User Password		Yes CLI: set password
Country		Yes CLI > set web-security
DHCP		Yes CLI > set network dhcp
DNS Primary		Yes CLI > set network dns
DNS Secondary		Yes CLI > set network dns
Domain		Yes CLI > set network domain
Domain Name Service DNS Enable		No
Gateway Address		Yes. Use OS Administration > Settings>IP or CLI > set network gateway

Table 4 Configuration Data (continued)

Configuration Data	Your Entry	Can Entry Be Changed After Installation
Host Name		No
IP Address		Yes Use OS Administration > Settings>IP or CLI> set network IP
IP Mask		Yes. Use OS Administration > Settings>IP or CLI > set network ip eth0
Location		Yes CLI> set web-security
Master Administrator ID		No
NTP Server IP Address Note You can enter up to five NTP servers.		Yes Use OS Administration > Settings>NTP Servers
Organization		Yes CLI> set web-security
Security Password		Yes CLI> set password security
SMTP Location		Yes CLI> set smtp
State		Yes CLI> set web-security
Time Zone		Yes CLI> set timezone
Unit		Yes CLI> set web-security

For more detailed descriptions of each installation field, see [Table 5](#).


Table 5 **Installation Field Definitions**

Field	Description	Usage
Administrator ID	This field specifies the name that you want to assign to this account.	Ensure the name is unique; it can contain lowercase, alphanumeric characters, hyphens, and underscores. It must start with a lowercase alphanumeric character. For this mandatory field, you should record it for use when logging in to the CLI or into Cisco Unified Communications Operating System Administration.
Administrator Password	This field specifies the password that you use for logging into the the CLI on the platform and for logging into Cisco Unified Communications Operating System Administration.	Ensure the password is at least six characters long; it can contain alphanumeric characters, hyphens, and underscore. For this mandatory field, you should record it for use when logging in to the CLI or into Cisco Unified Communications Operating System Administration.
DHCP	Dynamic Host Configuration Protocol	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.
DNS Enabled	A DNS server represents a device that resolves a hostname into an IP address or an IP address into a hostname.	If you do not have a DNS server, enter No . When DNS is not enabled, you should only enter IP addresses (not hostnames) for all network devices in your Cisco Unified Communications network. If you have a DNS server, Cisco recommends that you enter Yes to enable DNS. Disabling DNS limits the system ability to resolve some domain names.
DNS Primary	The server contacts this DNS server first when it attempts to resolve host names.	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 where ddd can have a value between 0 and 255 (except 0.0.0.0). Consider this field mandatory if DNS is set to yes .
DNS Secondary	When a primary DNS server fails, the server will attempt to connect to the secondary DNS server.	In this optional field, enter the IP address of the secondary DNS. Enter the IP address in dotted decimal format as ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0).
Domain	This field represents the name of the domain in which this machine is located.	Consider this field mandatory if DNS is set to yes .

Table 5 *Installation Field Definitions (continued)*

Field	Description	Usage
First Cisco Unified Communications Manager Node	<p>This field specifies the first Cisco Unified Communications Manager node that contains the database.</p> <p>Subsequent nodes connect to the first node to access database content.</p> <p>The first node also synchronizes with an external NTP server and provides time to the other nodes.</p>	<p>Choose Yes if you are configuring the first Cisco Unified Communications Manager node in the cluster.</p> <p>If you are configuring subsequent nodes, see Table 5 for information on the different fields.</p>
Gateway Address	<p>A gateway represents a network point that acts as an entrance to another network. Outbound packets get sent to the gateway that will forward them to their final destination.</p>	<p>Enter the IP address of the gateway in the format ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0)</p> <p>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.</p>
Hostname	<p>A host name represents an alias that is assigned to an IP address to identify it.</p>	<p>Enter a host name that is unique to your network.</p> <p>The host name can comprise up to 64 characters and can contain alphanumeric characters and hyphens.</p> <p>If DHCP is set to No, consider this field mandatory.</p>
IP Address	<p>This field specifies the IP address of this machine. It will uniquely identify the server on this network. Ensure another machine in this network does not use this IP address.</p>	<p>Enter the IP address in the form ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0).</p> <p>If DHCP is set to No, consider this field mandatory.</p>
IP Mask	<p>This field specifies the IP subnet mask of this machine. The subnet mask together with the IP address define the network address and the host address.</p>	<p>Enter the IP mask in the form ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0).</p> <p>A valid mask should have contiguous '1' bits on left side and contiguous '0' bits on the right.</p> <p>For example, a valid mask follows: 255.255.240.0 (11111111.11111111.11110000.00000000)</p> <p>An invalid mask follows: 255.255.240.240 (11111111.11111111.11110000.11110000)</p>
NIC Speed	<p>This field specifies the speed of the server network interface card (NIC) in megabits per second.</p>	<p>The possible speeds include 10 or 100.</p>
NIC Duplex	<p>This field specifies the duplex setting of the server NIC.</p>	<p>The possible settings include half and full.</p>

Table 5 **Installation Field Definitions (continued)**

Field	Description	Usage
NTP Server	This field identifies the NTP servers with which you want to synchronize.	Enter the hostname or IP address of one or more NTP server(s). Note You can add additional NTP servers or make changes to the NTP server list at a later time
NTP Server Enable	When enabled, this server will act as a NTP server and provide time updates to the subsequent nodes in the cluster.	Choose Yes if you want to enable this machine to be an NTP server. This option is available only on the first node in a cluster.
Security Password	Servers in the cluster use the security password to communicate with one another. You will be asked to enter the same security password for each subsequent node in the cluster.	Enter the security password. Enter the same password in the confirm password field. The password must contain at least six alphanumeric characters. It can contain hyphens and underscores, but it must start with an alphanumeric character.  Caution You must enter the same password for all nodes in the cluster.
Set Hardware Clock	This field specifies the date and local time for the machine. Note If you set the hardware clock manually, the node does not use an external NTP server for time synchronization.	Choose Yes if you want to set the date and local time for the time zone that you chose. Enter the hours based on a 24-hour format. Note If you configure an external NTP server, the hardware clock gets set automatically.
SMTP	This field specifies the name of the SMTP host that is used for outbound e-mail.	Enter the hostname or dotted IP address for the SMTP server. For a host, it can contain alphanumeric characters, hyphens, or periods. For a host name, it must start with an alphanumeric character. You must fill in this field if you plan to use electronic notification. If not, you can leave it blank.
Subnet IP Address	By entering a subnet address, you can specify a range of IP Addresses that will be granted access to query this NTP server.	Enter an IP subnet that will be granted access to the NTP server During installation, you can only enter two subnets.
Subnet Mask	This field specifies the subnet mask for the subnet address.	Enter the subnet mask for the IP subnet.
Time zone	This field specifies the local time zone and offset from Greenwich Mean Time (GMT).	Choose Yes if you want to change the time zone. Choose the time zone that most closely matches the location of your machine.

Using the Cisco Unified Communications Answer File Generator

Cisco Unified Communications Answer File Generator, a web application, generates answer files for unattended installations of Cisco Unified Communications Manager Business Edition. Individual answer files get copied to a USB key or a floppy diskette that accompanies the Cisco Unified Communications Manager Business Edition DVD during the installation process.

The web application supports the following features:

- Allows simultaneous generation and saving of answer files for unattended installs on the publisher server and all subscriber servers.
- Provides syntactical validation of data entries.
- Provides online help and documentation.

The following usage requirements apply:

- The web application supports only fresh installs (for example, it does not include upgrades).
- If DHCP client is being used on the publisher server, and subscriber server answer files are also being generated, you must specify the publisher server IP address.

You can access the Cisco Unified Communications Answer File Generator at the following URL:

http://www.cisco.com/web/cuc_afg/index.html

The Cisco Unified Communications Answer File Generator supports Internet Explorer version 6.0 or higher and Mozilla version 1.5 or higher.

If a USB key is being used to perform an unattended installation of Cisco Unified Communications Manager Business Edition, you may need to reformat the USB key to the FAT32 file system beforehand. You need to reformat especially in the case of USB keys with larger storage capacity (for example, 1 Gigabyte) that are formatted with the FAT file system.

You can use the Windows XP Disk Management Utility to reformat a USB key to the FAT32 file system as follows (you might need to be logged in as an administrator or a member of the Administrators group to perform these tasks):

-
- Step 1** Insert the USB key into a USB slot on the Windows XP PC.
 - Step 2** Choose **Start > Control Panel > Administrative Tools** and then double-click Computer Management.
 - Step 3** Expand the Storage tree and click **Disk Management**.
 - Step 4** Right-click the **Removable Disk** icon and click **Format**.
 - Step 5** You may be asked whether you are sure that you want to format this partition; click **Yes**.
 - Step 6** Click the **File System:** pull down and select **FAT32**.
 - Step 7** Click **OK**. When prompted to format the volume, click **OK** again.

The Removable Disk icon text should now show the file system format as FAT32.

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 connect, a message displays, and you get 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)**—This option allows you to review and modify the networking configuration. The installation program returns to the network configuration windows.
Networking gets validated after you complete each networking window, so 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.

Installation Overview

Cisco Unified Communications Manager 5.0(x) uses a different installation framework than previous releases. The installation process allows you to perform a basic installation, upgrade to a newer service release during the installation, and upgrade from Cisco Unified Communications Manager 4.x to Cisco Unified Communications Manager 6.0(1).

For a more detailed description of the different installation types, see [Table 6](#).

Table 6 **Installation Options**

Installation Types	Description
Basic Install	This option represents the basic Cisco Unified Communications Manager 6.0(1) installation, which installs the software from the installation disc and does not use any imported data.
Upgrade During Install	This option allows you to upgrade the software version that is contained on the installation disc with a later release. You can also choose Upgrade During Install followed by a Windows Upgrade and perform both during the installation process. Note Ensure that you have the software image available on DVD or on a remote server prior to choosing this option.
Windows Upgrade	This option allows you to import database information from a Cisco Unified Communications Manager 4.x system by using a file that the Data Migration Assistant (DMA) tool produces. Note Before upgrading from a Windows-based release, ensure you have all software licenses ready to ensure successful operation after the upgrade.



Note

This document describes only the first two installation types: Basic Install and Upgrade During Install. For information on performing a Windows Upgrade, refer to *Upgrading Cisco Unified Communications Manager*.

Installing the New Operating System and Application

This section describes how to install the operating system and Cisco Unified Communications Manager Business Edition application. You install the operating system and application by running one installation program. This document divides the procedure for using this installation program into the following major topics:

- “Navigating Within the Installation Wizard” section on page 12
- “Starting the Installation” section on page 12
- “Entering Preexisting Configuration Information” section on page 14
- “Upgrading During Installation” section on page 15
- “Performing the Basic Installation” section on page 17
- “Configuring the First Node” section on page 18
- “Configuring a Subsequent Node” section on page 20

Navigating Within the Installation Wizard

For instructions on how to navigate within the installation wizard, see [Table 7](#).

Table 7 *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)

Starting the Installation

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 Communications Manager Business Edition preinstalled, you do not need to install from a DVD, unless you want to reimage the server with a later product release. You can go directly to the “[Entering Preexisting Configuration Information](#)” procedure on page 14.

Step 3 If you choose **Yes** to perform the media check, the Media Check Result window displays. 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.

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.

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

Step 5 In the Product Deployment Selection window, select the product to install; then, choose **OK**. You can choose from the following options:

- Cisco Unified Communications Manager
- Cisco Unity Connection
- Cisco Unified Communications Manager Business Edition (includes Cisco Unified Communications Manager and Cisco Unity Connection)



Note Only the products that are supported on your server appear in the list.

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. 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.

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 continue with this procedure.
- If you want to install the software now and configure it later or if you have a server that has Cisco Unified Communications Manager Business Edition preinstalled, choose **Skip** and continue with the [“Entering Preexisting Configuration Information”](#) section on page 14.

- Step 8** Choose the type of installation to perform by doing the following steps. See [Table 6](#) for more information on installation options:
- a. In the Apply Additional Release window, choose one of the options:
 - To upgrade to a later Service Release of the software during installation, choose **Yes**. Continue with the [“Upgrading During Installation”](#) section on page 15.
 - To skip this step, choose **No**.
 - To return to the previous window, choose **Back**.
 - b. In the Import Windows Data window, choose **No**.



Note To perform a Windows Upgrade, that is, to upgrade from a Windows version of Cisco Unified Communications Manager to Cisco Unified Communications Manager 6.0(1), see *Upgrading Cisco Unified Communications Manager* for more information.

- Step 9** In the Basic Install window, choose **Continue** to install the software version on the DVD or configure the preinstalled software. Continue with the [“Performing the Basic Installation”](#) section on page 17.
-

Entering Preexisting Configuration Information

Start here if you have a server that has the product preinstalled or if you chose **Skip** in the Platform Installation Wizard window.

- Step 1** After the system restarts, the Preexisting Installation Configuration window displays.
- Step 2** If you have preexisting configuration information, generated by the Answer File Generator, that is stored on a floppy disc or a USB key, insert the disc or the USB key now and choose **Continue**. The installation wizard will read the configuration information during the installation process.



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

The Platform Installation Wizard window displays.

- Step 3** To continue with the Platform Installation Wizard, choose **Proceed**.
- Step 4** Choose the type of installation to perform by doing the following steps. See [Table 6](#) for more information on installation options:
- a. In the Apply Additional Release window, choose one of the options:
 - To upgrade to a later Service Release of the software during installation, choose **Yes**. Continue with the [“Upgrading During Installation”](#) section on page 15.
 - To skip this step, choose **No**.
 - To return to the previous window, choose **Back**.
 - b. In the Import Windows Data window, choose **No**.



Note To perform a Windows Upgrade, that is, to upgrade from a Windows version of Cisco Unified Communications Manager to Cisco Unified Communications Manager 6.0(1), see *Upgrading Cisco Unified Communications Manager* for more information.

Step 5 In the Basic Install window, choose **Continue**. Continue with the “[Performing the Basic Installation](#)” section on page 17.

Upgrading During Installation

If you choose **Yes** in the Upgrade During Install 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.

If you are upgrading from Cisco Unified Communications Manager release 5.x, the upgrade file name has 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.

If you are upgrading from Cisco Unified Communications Manager release 6.x, the upgrade file has the extension `sgn.iso`.

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.

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

The Upgrade During Install 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 16.
- **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 16.

- **LOCAL**—Retrieves the upgrade file from a local CD or DVD. Continue with the [“Upgrading from a Local Disk”](#) section on page 16.

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.

- If you are using an upgrade file with the tar.gz.sgn extension, copy the upgrade file to a writeable CD or DVD.
- If you are using an upgrade file with the sgn.iso extension, you must create an ISO image on the DVD from the upgrade file.

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.



Note This step does not apply if you are using an upgrade file with the sgn.iso extension.

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. Skip to the [“Entering Preexisting Configuration Information”](#) section on page 14.

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.

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.

- 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 3** 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 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 running the upgraded software version.
- After the system restarts, the Preexisting Configuration Information window displays. Continue with the [“Entering Preexisting Configuration Information”](#) section on page 14.

Performing the Basic Installation

- Step 1** When the Timezone Configuration displays, choose the appropriate time zone for the server and then choose **OK**.
- 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.
- 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 3 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 4 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 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.

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

Step 7 Enter your Administrator login and password from [Table 4](#).



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 8 Enter your certificate signing request information and choose **OK**.




The First Node Configuration window displays.

Step 9 You can configure this server as either the first node in a Cisco Unified Communications Manager cluster or as a subsequent node.

- To configure this server as the first Cisco Unified Communications Manager node, choose **Yes** and continue with the [“Configuring the First Node” section on page 18](#).
 - To configure this server as a subsequent node in the cluster, choose **No** and continue with the [“Configuring a Subsequent Node” section on page 20](#).
-

Configuring the First Node

After you finish the basic installation, follow this procedure to configure the server as the first node in the cluster.

-
- Step 1** The Network Time Protocol Client Configuration window displays.
- 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 stratum 1-9). Subsequent nodes in the cluster will get their time from the first node.
- Step 2** Choose whether you want to configure an external NTP server or manually configure the system time.
- 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 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 3** Enter the Database Access Security password from [Table 4](#).
-  **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. The system uses this password to authorize communications between nodes, and you must ensure this password is identical on all nodes in the cluster.
-
- The SMTP Host Configuration window displays.
- Step 4** 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.
-
- Step 5** Choose **OK**. The Application User Configuration window displays.
- Step 6** Enter the Application User Username and Password from [Table 4](#) and confirm the password by entering it again.
- Step 7** Choose **OK**. The Platform Configuration Confirmation window displays.
- Step 8** To continue with the installation, choose **OK**; or to modify the platform configuration, choose **Back**.
- The system installs and configures the software. The DVD drive ejects and the server reboots. Do not reinsert the DVD.
- Step 9** When the installation process completes, you get prompted to log in by using the Administrator account and password.
- Step 10** Complete the post-upgrade tasks that are listed in the [“Post-Installation Tasks”](#) section on page 20.
-

Configuring a Subsequent Node

To configure a subsequent node in the cluster, follow these steps.



Caution

You must configure a subsequent node on the first node using Cisco Unified Communications Manager Administration before you install the subsequent node. For more information, see the *Cisco Unified Communications Manager Administration Guide*.

- Step 1** The First Node Access Configuration window displays.
- Step 2** Enter the First Node Access Configuration information from [Table 4](#).
The SMTP Host Configuration window displays.
- Step 3** 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 4** To start installing the software, choose **OK**, or, if you want to change the configuration, choose **Back**.
- Step 5** When the installation process completes, you get prompted to log in by using the Administrator account and password.
- Step 6** Complete the post-upgrade tasks that are listed in the “[Post-Installation Tasks](#)” section on [page 20](#).

Post-Installation Tasks

After installing Cisco Unified Communications Manager Business Edition on your server, you must set some configuration parameters and perform other post-installation tasks before you can begin using it. Perform these tasks for the server that you install and complete the tasks before other servers in the cluster are installed.

For post-installation tasks that you must complete after the installation, see [Table 8](#).

Table 8 *Post-Installation Tasks*

Post-Installation Tasks	Important Notes
Log in as the Cisco Unified Communications Manager Business Edition Application User and change the Application User passwords.	See the “Changing the Default Application User Passwords” section on page 22.
<p>Activate Cisco Unified Communications Manager Business Edition feature services that you want to run.</p> <p>Before you activate feature services, you must perform required preactivation tasks. For service activation requirements, refer to the <i>Cisco Unified Serviceability Administration Guide</i>.</p> <p> Caution You must activate Cisco Unified Communications Manager Business Edition services in Cisco Unified Serviceability.</p>	<p>Refer to <i>Cisco Unified Serviceability Administration Guide</i>.</p> <p>See the “Accessing Cisco Unified Serviceability” section on page 22.</p>
<p>Configure the backup settings.</p> <p>Remember to back up your Cisco Unified Communications Manager Business Edition data daily.</p>	Refer to <i>Disaster Recovery System Administration Guide</i> .
The locale English_United_States installs automatically on the server; however, you can add new locales to the server, if required.	Refer to <i>Cisco Unified Communications Operating System Administration Guide</i> .
Cisco recommends that you implement authentication and encryption in your Cisco IP Telephony network.	Refer to <i>Cisco Unified Communications Manager Security Guide</i> .
If necessary, you can add subsequent Cisco Unified Communications Manager nodes to the cluster.	<p>You must add subsequent Cisco Unified Communications Manager nodes to the cluster by performing the following tasks:</p> <ol style="list-style-type: none"> 1. Define all subsequent nodes in the cluster by adding the hostname or IP address of the subsequent Cisco Unified Communications Manager nodes to Cisco Unified Communications Manager Administration. For more information, refer to <i>Cisco Unified Communications Manager Administration Guide</i>. 2. Install the new application and configure subsequent Cisco Unified Communications Manager nodes in the cluster. See Installing the New Operating System and Application, page 12. <p>Remember to enter the same security password on all nodes.</p>

Changing the Default Application User Passwords

The installation sets all Application User passwords to the same Application User password that you entered during installation. Cisco recommends that you log in to Cisco Unified Communications Manager Administration and change these passwords. Refer to *Cisco Unified Communications Manager Administration Guide* for the procedure for changing a password.

Accessing Cisco Unified Serviceability

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.

Even though all services are installed on each server in the cluster, you must manually activate the services that you want to run on each server in the cluster through Cisco Unified Serviceability. For service recommendations and more information, refer to *Cisco Unified Serviceability Administration Guide*.

Configuring the Database

After installing Cisco Unified Communications Manager, you use Cisco Unified Communications Manager Administration to begin configuring the database. The Cisco Unified Communications Manager database contains information and parameters that relate to the system as a whole, to connected devices, and to individual users. The following list describes a few tasks that you must perform in Cisco Unified Communications Manager Administration or Cisco Unified Serviceability:

1. In Cisco Unified Serviceability, activate the services that you want to run on each server in the cluster.
2. Configure system-level settings, such as Cisco Unified Communications Manager Groups.
3. Design and configure your dialing plan.
4. Configure media resources for conferences, music on hold, and so on.
5. Configure systemwide features, Cisco Unified IP Phone services, Cisco Unified Communications Manager Extension Mobility, Cisco Unified Communications Manager Attendant Console, and Cisco Unified Communications Manager Assistant.
6. Install and configure the gateways.
7. Enable computer telephony integration (CTI) application support; then, install and configure the desired CTI applications.
8. Configure the users.
9. Configure and install the phones; then, associate users with the phones.

For more information about configuring the Cisco Unified Communications Manager database, refer to the *Cisco Unified Communications Manager Administration Guide*, the *Cisco Unified Communications Manager System Guide*, or online help in the Cisco Unified Communications Manager application.

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

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)

Copyright © 2007. Cisco Systems, Inc. All rights reserved.

