



Home

Welcome to the Cisco Unified Communication Manager Upgrade Center

This Upgrade Center includes information about upgrading to Cisco Unified Communication Manager 5.1(1) (Cisco Unified CM, formerly Cisco Unified CallManager) from a Cisco Unified CM 4.x release. This site also provides instructions for installing software patches and upgrade software after you have upgraded to Cisco Unified CM 5.1(1).

To get started with your upgrade, read the Upgrade Overview. Use the Master Installation Checklist to track your completion of other checklists.

To see when this site was most recently updated, click the History link at the top of the window.

Before You Begin

Make sure you or the person doing the installation meets the skills in the Minimum Skills/Knowledge Checklist.

Using This Site

Click the Help link at the top of the window for tips on navigating this site.

Upgrade Overview

Ensure the Cisco Unified Communication Manager server with the publisher database is configured as the first node and Cisco Unified Communication Manager servers with subscriber databases are configured as subsequent nodes. Review the following sections carefully before you perform the upgrade:

- Pre-Upgrade Checklist
- Installation Information Worksheet, page 2-4
- Handling Network Errors During Installation, page 2-10
- Checklist for Upgrading the First Cisco Unified CM Node
- Navigating Within the Installation Wizard, page 3-2
- Selecting an Installation Option, page 3-2

- Installing the New OS and Application on the First Node, page 3-4
- Checklist for Upgrading Subsequent Nodes in the Cluster, page 3-11
- Post-Upgrade Checklist, page 4-2

Master Installation Checklist

Use this master checklist to check off your work on other checklists. You can also click to go directly to a checklist.

Table 1-1 *Master Installation Checklist*

	Checklist
<input type="checkbox"/>	Minimum Skills/Knowledge Checklist - Check your skills
<input type="checkbox"/>	Pre-Upgrade Checklist
<input type="checkbox"/>	Checklist for Upgrading the First Cisco Unified CM Node
<input type="checkbox"/>	Checklist for Upgrading Subsequent Nodes in the Cluster
<input type="checkbox"/>	Post-Upgrade Checklist

Minimum Skills/Knowledge Checklist

For a successful installation, ensure that the installer has the following prerequisite skills.

Table 1-2 *Minimum Skills/Knowledge Checklist*

	Skill or Knowledge
<input type="checkbox"/>	<p>Cisco Certified Learning</p> <ul style="list-style-type: none"> • Completion or solid knowledge of the CIPT 4.2/5.0 course <p>or</p> <ul style="list-style-type: none"> • Completion of a Cisco Unified Communications Manager bootcamp course

Table 1-2 Minimum Skills/Knowledge Checklist

	Skill or Knowledge
<input type="checkbox"/>	<p>Experience with upgrade, backup, and restore procedure</p> <ul style="list-style-type: none"> • Experience upgrading, restoring, and backing up a lab or test Cisco Unified Communications Manager <p>or</p> <ul style="list-style-type: none"> • Completion of an online bootcamp with a virtual backup and restore of a Cisco Unified Communications Manager <p>Example: Cisco Partner E-Learning Connection has an online bootcamp lab, “Cisco CallManager 5.0 Bootcamp Lab 3-4: Backing Up and Restoring Cisco CallManager 5.0” [cannot find in Partner E-Learning connection - found an instructor led class, Advanced Services' Deploying Cisco CallManager (CMBC) 5.0</p>
<input type="checkbox"/>	<p>Reviewed official Cisco CallManager Upgrade Procedures</p> <p>Complete the Quick Learning Modules for your upgrade scenario:</p> <ul style="list-style-type: none"> • 4.x to 5.x: Training Available to Partners • 5.0 to 5.x: Training Available to Partners • 5.x to 6.0: Training Available to Partners



Pre-Install

Introduction

In this section you will use the Pre-Upgrade Checklist to complete all the tasks necessary before you actually do the upgrade.

Before You Begin

You should have completed the Minimum Skills/Knowledge Checklist.

When You Are Done

You will have completed the Pre-Upgrade Checklist. Go on to Install.

Pre-Upgrade Checklist

Perform the following tasks before you begin the upgrade. Clicking a link in the “Task Details” column opens the referenced procedure in a popup window. Notes indicate where there are other sections of the referenced document important for background information or context.

	Pre-Upgrade Task	Task Details (Links) and Notes
<input type="checkbox"/>	Step 1 Verify that your system meets the system requirements for upgrading Cisco Unified Communication Manager nodes in the cluster.	To find which servers support Cisco Communication Manager 5.x releases, refer to the Guide to Cisco Communication Manager Upgrades and Server Migrations at http://www.cisco.com/en/US/partner/products/hw/voiceapp/ps378/prod_brochure_list.html .
<input type="checkbox"/>	Step 2 Run Cisco Unified Communication Manager Upgrade Utility on the server to verify that the system is ready for upgrade.	Refer to <i>Using Cisco Unified Communication Manager Upgrade Utility</i> . Note Review the document to install the utility and to understand what checks the utility performs.

Pre-Upgrade Task	Task Details (Links) and Notes
<input type="checkbox"/> Step 3 Perform the recommended backup procedures on the publisher server. Back up every database that is associated with your Cisco Unified Communication Manager server.	<p>Refer to <i>Cisco IP Telephony Backup and Restore System (BARS) Administration Guide</i>.</p> <p>Note Review the document overview for information on the versions of applications that BARS supports and for instructions on installing BARS.</p>
<input type="checkbox"/> Step 4 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.	<p><i>Cisco IP Telephony Backup and Restore System (BARS) Administration Guide</i>.</p> <p>Note Review the document overview for information on the versions of applications that BARS supports and for instructions on installing BARS.</p>
<input type="checkbox"/> Step 5 If you do not need to carry over your CDR data to Cisco Unified Communication Manager 5.1(1), Cisco recommends that you purge the CDR data before you run DMA.	<p>Purging the CDR data speeds up the migration process and decreases the size of the DMA TAR file.</p> <p>Purging CDR: Refer to “Using Manual Database Purge” in <i>Cisco CallManager Serviceability Administration Guide, Release 4.1(3)</i>.</p>
<input type="checkbox"/> Step 6 (If your systems are using centralized TFTP) Upgrade off-clusters in the centralized TFTP environment.	<p>When upgraded to 5.x, the other clusters participating in Centralized TFTP must be running a supported version (see list below) of Cisco Unified CM.</p> <p>Configuring Centralized TFTP: Refer to “Cisco TFTP” in the <i>Cisco Unified CallManager System Guide 5.0(4)</i></p> <p>Note The referenced procedure in the 5.0(4) System Guide applies to 5.1(1) as well.</p> <p>Supported versions of Cisco Unified CM:</p> <ul style="list-style-type: none"> • 3.3(5)sr2 • 4.1(3)sr2 • 4.2 • 4.3 • 5.0 • 5.1 • 6.0 <p>These Cisco Unified CM versions are not supported:</p> <ul style="list-style-type: none"> • 4.0(1) • 4.0(2) • 4.1(1) • 4.1(2)

	Pre-Upgrade Task	Task Details (Links) and Notes
<input type="checkbox"/>	<p>Step 7 Export the data on the current Cisco Unified Communication Manager Publisher server by running the Data Migration Assistant (DMA).</p> <p>Ensure the configuration files and exported data files are located in one of the following locations:</p> <ul style="list-style-type: none"> • Hard drive (for DMABackupInfo.inf only) • Floppy drive (for DMABackupInfo.inf only) • Tape drive • Remote drive <p>Note Running DMA is required for obtaining the license file (see Checklist for Upgrading the First Cisco Unified CM Node).</p>	<p>DMA generates two files:</p> <ul style="list-style-type: none"> • 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 Communication Manager configuration data, named DMABackupInfo.inf. The system saves it in the D:\DMA folder as part of the TAR file. <p>Note Do not change the configuration data filename. The upgrade fails if it does not find a file with the exact filename and format.</p> <p>For more information on data migration, refer to <i>Data Migration Assistant Administration Guide</i>. You will be choosing an installation option based on the location of the DMA output configuration file and TAR file.</p> <p>Note Review the pre installation guidelines and installation procedures</p>
<input type="checkbox"/>	<p>Step 8 Before the upgrade, obtain the necessary information for configuring the platform and Cisco Unified CM on the first and subsequent nodes.</p>	<p>See the “Installation Information Worksheet” section on page 2-4.</p>
<input type="checkbox"/>	<p>Step 9 Record the Host Name/IP Address value that is configured on the Server Configuration Settings window of the Cisco Unified CallManager 4.x server.</p>	<p>To access the Host Name/IP Address field on the 4.x server, navigate to System > Server.</p> <p>For more information, see Assigning the Host Name or IP Address to the Server</p>
<input type="checkbox"/>	<p>Step 10 Match the server’s NIC speed and duplex settings with the switch port’s configuration. For servers or switch ports that can support GigE (1000BaseT), use auto-negotiation on both sides.</p>	<p>For more information, see “NIC and Switch port Speed and Duplex” in Installation Field Definitions.</p>
<input type="checkbox"/>	<p>Step 11 Enable PortFast on all switch ports connected to Cisco Unified servers.</p>	<p>With PortFast enabled, [the switch] immediately brings a port from the blocking state into the forwarding state by eliminating the forwarding delay (the amount of time a port waits before changing from its Spanning-Tree Protocol (STP) learning and listening states to the forwarding state.</p>

	Pre-Upgrade Task	Task Details (Links) and Notes
<input type="checkbox"/>	Step 12 (If you are using NIC teaming) Be aware that the NIC teaming configuration will be lost during the upgrade. You will need to set it up on each server after the upgrade.	After the upgrade, be sure to complete Step 1 in the Post-Upgrade Checklist.
<input type="checkbox"/>	Step 13 Familiarize yourself with the navigation options within the installation wizards.	See Navigating Within the Installation Wizard.

Installation Information Worksheet

Use Table 2-1 to record the information about your Cisco Unified Communication Manager server. Gather this information for each Cisco Unified Communication Manager server that you are installing in the cluster. You may not need to obtain all the information; gather only the information that is pertinent to your system and network configuration. You can make copies of this table and record your entries for each server in a separate table, even if you are planning to use the DMABackupInfo.inf file to configure your system.



Note

Alternatively, download and use a Microsoft Word version of the worksheet.



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 platform administration or through the Command Line Interface (CLI).

Table 2-1 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

Table 2-1 Configuration Data

Configuration Data	Your Entry	Can Entry Be Changed After Installation
DNS Secondary		Yes CLI> set network dns
Domain		Yes CLI> Set Network Domain
Domain Name Service DNS Enable		No
Gateway Address		Yes. Use Platform Administration > Settings>IP or CLI > set network gateway
Host Name		No
IP Address		Yes Use Platform Administration > Settings>IP or CLI> set network IP
IP Mask		Yes. Use Platform Administration > Settings>IP or CLI > set IP
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 Platform 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

Table 2-1 Configuration Data

Configuration Data	Your Entry	Can Entry Be Changed After Installation
Time Zone		Yes CLI> Set Timezone
Unit		Yes CLI> set web-security
End-User Password		Yes See “End User Configuration” in the <i>Cisco Unified Communication Manager Administration Guide</i> .
End-User PIN		Yes See “End User Configuration” in the <i>Cisco Unified Communication Manager Administration Guide</i> .

For more detailed descriptions of each installation field, see Table 2-2.

Table 2-2 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 you log in to the CLI on the platform or into Platform Administration. Note You cannot change this field after installation.
Administrator Password	This field specifies the password that you use for logging in to the CLI on the platform and for logging in to 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 you log in to the Cisco Unified CallManager.

Table 2-2 Installation Field Definitions (continued)

Field	Description	Usage
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. Note You cannot change the DNS settings after the installation is complete. To change DNS settings, you must reinstall Cisco Unified Communication Manager.	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 entering Yes to enable DNS. Disabling DNS limits the system ability to resolve some domain names.
DNS Primary	Cisco Unified Communication Manager 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, Cisco Unified Communication Manager 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 .
First Cisco Unified Communication Manager Node	The first Cisco Unified Communication Manager node contains the database. Subsequent nodes connect to the the first node to access database content. The first node also synchronizes with an external NTP server and provides time to the other nodes.	Choose Yes if you are configuring the first Cisco Unified Communication Manager node in the cluster. If you are configuring subsequent nodes, see Table 2-2 for information on the different fields.


Table 2-2 Installation Field Definitions (continued)

Field	Description	Usage
Gateway Address	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.	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) 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 communicating only with devices on your subnet.
Hostname	A host name represents an alias that is assigned to an IP address to identify it.	Enter a host name that is unique to your network. 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.
IP Address	This field specifies the IP address of this machine. It will uniquely identify the server on this network. Another machine in this network should not be using this IP address.	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). If DHCP is set to No , consider this field mandatory.
IP Mask	This field specifies the IP subnet mask of this machine. The subnet mask together with the IP address defines the network address and the host address.	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). A valid mask should have contiguous '1' bits on left side and contiguous '0' bits on the right. For example, a valid mask follows: 255.255.240.0 (11111111.11111111.11110000.00000000) An invalid mask follows: 255.255.240.240 (11111111.11111111.11110000.11110000)

Table 2-2 Installation Field Definitions (continued)

Field	Description	Usage
NIC and Switch port Speed and Duplex	<p>NIC Speed specifies the speed of the server network interface card (NIC) in megabits per second.</p> <p>NIC Duplex specifies the duplex setting of the server NIC.</p>	<p>Speed: 10, 100, or 1000</p> <p>Duplex: Half or full.</p> <p>Note For GigE (1000/FULL), NIC and switch port settings must be handled differently than they were in Windows, where setting hard values and not using Autonegotiation was strongly recommended. For Linux-based Cisco Unified CM 5.x, set the NIC and switch port to Auto/Auto for 1000/FULL operation. Do not set hard values. The NIC and switch port sides must both be set to Auto.</p> <p>Note If you are using NIC Teaming, be aware that the NIC Teaming configuration will be lost during the upgrade. You will need to set it up on each server after the upgrade. After the upgrade, see NIC teaming in the Post-Upgrade Checklist.</p>
NTP Server	<p>This field identifies the NTP server with which you want to keep time synchronization.</p>	<p>Enter the hostname or IP Address of NTP server(s).</p> <p>If you enabled the system to be NTP client, you must enter the hostname or IP address of at least one NTP server.</p> <p>Note You can add additional NTP servers or make changes to the NTP server list at a later time</p>

Table 2-2 Installation Field Definitions (continued)

Field	Description	Usage
Security Password	<p>Cisco Unified Communication Manager servers in the cluster use the security password to communicate with one another.</p> <p>You will be asked to enter the same security password for each subsequent node in the cluster.</p>	<p>Enter the security password.</p> <p>Enter the same password in the confirm password field.</p> <p>The password must contain at least six alphanumeric characters. It can contain hyphens and underscores, but it must start with an alphanumeric character.</p> <p> Caution You must enter the same password for all nodes in the cluster.</p>
Set Hardware Clock	<p>The field specifies the date and local time for the machine.</p> <p>Note If you set the hardware clock manually, the node does not use an external NTP server for time synchronization.</p>	<p>Choose Yes if you want to set the date and local time for the time zone that you chose.</p> <p>Enter the hours based on a 24-hour format.</p> <p>Note If you configure an external NTP server, the hardware clock gets set automatically.</p>
SMTP	<p>This field specifies the name of the SMTP host that is used for outbound e-mail.</p>	<p>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.</p> <p>You must fill in this field if you plan to use electronic notification. If not, you can leave it blank.</p>
Time zone	<p>This field specifies the local time zone and offset from Greenwich Mean Time (GMT)</p>	<p>Choose Yes if you want to change the time zone.</p> <p>Choose the time zone that most closely matches the location of your machine.</p>

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.

Networking is 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 appears 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.

Related Training

Please check back for updated training links.



Install

Introduction

In this section you will complete the two major upgrade tasks using the following checklists:

Checklist for Upgrading the First Cisco Unified CM Node

Checklist for Upgrading Subsequent Nodes in the Cluster

Before You Begin

You should have completed the Pre-Upgrade Checklist.

When You Are Done

You will have completed the Checklist for Upgrading the First Cisco Unified CM Node and Checklist for Upgrading Subsequent Nodes in the Cluster.

Go on to the Post-Upgrade Checklist.

Checklist for Upgrading the First Cisco Unified CM Node

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

	Task	Task Details (Links) and Notes
<input type="checkbox"/>	Step 1 Verify that you have completed all pre-upgrade tasks.	See Pre-Upgrade Checklist.
<input type="checkbox"/>	Step 2 Familiarize yourself with navigation within the installation wizard.	See Navigating Within the Installation Wizard.
<input type="checkbox"/>	Step 3 Know which installation options to choose.	See Selecting an Installation Option.
	Step 4 Assign host name or IP address to the server.	See Assigning the Host Name or IP Address to the Server.
<input type="checkbox"/>	Step 5 Configure the hardware with the hardware configuration disc.	See Configuring the Hardware.

	Task	Task Details (Links) and Notes
<input type="checkbox"/>	Step 6 Install the new operating system on the first node.	See Installing the New OS and Application on the First Node.
<input type="checkbox"/>	Step 7 Obtain the necessary licensing details from the system and register for your license file on Cisco.com. Once you receive the license file and install it on your system, you may then make changes to the administration. Note Prior to obtaining the license information the system will run but administration changes can not be made.	See the Licensing chapter in <i>Cisco Unified CallManager System Guide, Release 5.0(4)</i> .

Navigating Within the Installation Wizard

For instructions on how to navigate within the installation wizard, see Table 3-1.

Table 3-1 Installation Wizard Navigation

To Do This	Press
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)

Selecting an Installation Option

After the platform software installation starts, you will be asked to select one of the options that Table 3-2 lists.

Table 3-2 Installation Options

Installation Options	Description
Basic Install	This option represents the basic installation and does not use any imported data.

Table 3-2 *Installation Options (continued)*

Installation Options	Description
Upgrade During Install	This option allows you to upgrade the preinstall software with the latest service release prior to configuring your system. You can also choose Upgrade During Install followed by the a Windows Upgrade and perform both during the installation process. Note You must 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 the TAR file that the DMA tool produced while upgrading an existing Cisco Unified Communication Manager server. Note If you choose to upgrade your server by using this option, you will need to provide the TAR file that contains the migrated data from the DMA tool on tape or a remote drive.

Assigning the Host Name or IP Address to the Server

In this task you assign the Host Name/IP address to the 5.1(1) 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(1) 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(1) 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(1) 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(1) server without having to preserve the IP Address or Host Name. The IP Address and/or Host name of the 5.1(1) 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.

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 Communication Manager application. See Table 3-3 for the BIOS settings and Table 3-4 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 3-3 and Table 3-4.

Table 3-3 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
Post F1 prompt: Delayed	Post F1 prompt: Delayed
Hyperthreading: Enabled	Hyperthreading: Enabled

Table 3-4 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	RAID type: 1(1+0)	RAID type: 1(1+0)
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.		

Installing the New OS and Application on the First Node

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

**Caution**

Before beginning this procedure, ensure that you have backed up the data on your current Windows-based version of Cisco Unified Communication Manager. 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 Media Check window displays.

**Note**

If you have a new server with pre installed Cisco Unified Communication Manager, you do not need to install from a DVD. Go directly to the “If You Choose Skip” procedure on page 3-6.

Step 2 Verify that the checksum that displays on the Media Check matches the checksum for the release on Cisco.com.

When the media check completes, the Media Check Result window displays.

Step 3 If the Media Check Result displays Pass, choose **OK** to continue the installation.

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

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

Drivers not found, do you want to install manually?

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 then verifies RAID configuration and BIOS settings. If the installation process makes any changes to your hardware configuration settings, you will get prompted to restart your system.

After the hardware checks complete, the Overwrite Hard Drive window displays.

Step 4 The **Overwrite Hard Drive** window indicates the current software version on your hard drive, if any, 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 5 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 3-6.
- 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 3-6.

If You Choose Skip

Start here if you have a server that has Cisco Unified Communication Manager pre installed or if you chose **Skip** on Platform Installation Wizard window.

- Step 6** 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 you have a file that the Data Migration Assistant created, see the *Data Migration Assistant User Guide* for more information.

- Step 7** To continue, choose **OK**.

The Platform Installation Wizard window displays.

- Step 8** To continue with the installation, choose **Proceed**.

The Upgrade During Install window displays. Continue with the “If You Choose Proceed” section on page 3-6.

If You Choose Proceed

- Step 9** Choose the type of installation to perform by doing the following steps. See Table 3-2 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 “Upgrade During Install” section on page 3-6.
 - To skip this step, choose **No**.
 - To return to the previous window, choose **Back**.
- b. In the Windows Upgrade window, choose **Yes**. Continue with the “Windows Upgrade” section on page 3-8.



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

Upgrade During Install

If you chose Upgrade During Install, the installation wizard installs the software version on the DVD first and then restarts the system. You then get prompted to enter certain network configuration parameter values and the location of the upgrade file.

- Step 10** After the system restarts, the Platform Installation Wizard window displays. To continue the installation, choose **Proceed**.

The Upgrade During Install window displays.

- Step 11** Choose **Yes**.

The Install Upgrade Retrieval Mechanism Configuration window displays.

- Step 12** 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 “Upgrade From a Remote Server” section on page 3-7.
- **FTP**—Retrieves the upgrade file from a remote server by using File Transfer Protocol (FTP). Skip to the “Upgrade From a Remote Server” section on page 3-7.

- **LOCAL**—Retrieves the upgrade file from a local CD or DVD. Continue with the “Upgrade From a Local Disc” section on page 3-7.

Upgrade From a Local Disc

Before you can upgrade from a local drive, 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.

The patch-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.

- Step 13** 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.

The Install Upgrade Patch Selection Validation window displays.

- Step 14** The window displays the patch file that is available on the CD or DVD. To update the system with this patch, choose **Continue**.

Upgrade 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.

The Auto Negotiation Configuration window displays.

- Step 15** 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 16** 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 17** 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 the “Retrieving the Remote Patch” section on page 3-8.
- If you want to configure static IP addresses for the node, choose **No**. The Static Network Configuration window displays.

Step 18 If you chose not to use DHCP, enter your static network configuration values and choose **OK**. See Table 2-2 for field descriptions.

The DNS Client Configuration window displays.

Step 19 To enable DNS, choose **Yes**, enter your DNS client information, and choose **OK**. See Table 2-2 for field descriptions.

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

Retrieving the Remote Patch

Step 20 Enter the location and login information for the remote file server. See Table 2-2 for field descriptions. After restarting the network, 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 21 Choose the upgrade patch to install. The system downloads, unpacks, and installs the patch and then restarts the system so it is running the upgraded software version.

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

Using Preexisting Configuration Information

Step 22 If you have preexisting configuration information 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.

The Platform Installation Wizard window displays.

Step 23 To continue with the Platform Installation Wizard, choose **Proceed**.

Step 24 To configure the platform now, choose **Proceed**.

Step 25 In the Upgrade During Install window, choose **No**.

Step 26 In the Windows Upgrade window, choose **Yes**. Continue with the “Windows Upgrade” section on page 3-8.

Windows Upgrade

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

Step 27 In the Windows Upgrade window, choose **Yes**.

The Timezone Configuration window displays.

Step 28 Choose the appropriate time zone for the server and then choose **OK**.

The Auto Negotiation Configuration window displays.

- Step 29** 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 30** 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 31** 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. The Administrator Login Configuration window displays.
 - If you want to configure static IP addresses for the node, choose **No**. The Static Network Configuration window displays.
- Step 32** If you chose not to use DHCP, enter your static network configuration values and choose **OK**. See Table 2-2 for field descriptions.
- The DNS Client Configuration window displays.
- Step 33** To enable DNS, choose **Yes**, enter your DNS client information, and choose **OK**. See Table 2-2 for field descriptions.
- The Administrator Login Configuration window displays.
- Step 34** Enter your administrator login and password from Table 2-1 on page 2-4.
- The Certificate Signing Request Information window displays.
- Step 35** Enter your certificate signing request information from Table 2-1 on page 2-4 and choose **OK**.
- The First Node Configuration window displays.
- Step 36** 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. The external NTP server must be stratum 9 or higher (meaning stratum 1-9). Subsequent nodes in the cluster will get their time from the first node.
-
- Step 37** 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. To continue with the installation, choose **Proceed**.

Note If the Test button displays, you can choose **Test** to check whether the NTP servers that you entered are accessible.

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

- 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 38 Enter the Database Access Security password from Table 2-1 on page 2-4.

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 this password must be the same on all nodes in the cluster.

The SMTP Host Configuration window displays.

Step 39 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 DMA Retrieval Mechanism Configuration window displays.

Step 40 Choose the mechanism that will be used to retrieve the DMA file:

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

Note To support retrieval of the DMA file, an FTP server should support the CD, BIN, DIR, and GET commands., and an SFTP server should support CD, LS, 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 41 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 42** 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 43** Enter the Application User Password from Table 2-1 and confirm the password by entering it again.
- Step 44** Choose **OK**.
The End User Password/PIN Configuration window displays.
- Step 45** 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 46** 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(1) server by comparing the value in the DMA file to the value that is configured on the 5.1(1) system. For more information, refer to the “Assigning the Host Name or IP Address to the Server” section on page 3-3.
- Step 47** 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 48** If no mismatch exists, or you select **Proceed**, the Platform Configuration Confirmation window displays.
- Step 49** To continue, choose **OK**.
- Step 50** When the installation process completes, you get prompted to log in by using the Administrator account and password.
-

What To Do Next

Complete the Checklist for Upgrading Subsequent Nodes in the Cluster. When that is done, complete the post-upgrade tasks listed in the Post-Upgrade Checklist.

Checklist for 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 Communication Manager application on the first node (Checklist for Upgrading the First Cisco Unified CM Node) and then configure the subsequent node on the first node by using Cisco Unified Communication Manager 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 Communication Manager 4.x to Cisco Unified Communication Manager 5.1(1), perform the following steps:

	Task	Task Details (Links) and Notes
<input type="checkbox"/>	Step 1 Using Cisco Unified Communication Manager Administration on the first node, configure the subsequent nodes.	
<input type="checkbox"/>	Step 2 Ensure that the subsequent nodes have network connectivity to the first node.	
<input type="checkbox"/>	Step 3 Install the new operating system and Cisco Unified Communication Manager application from a DVD.	Install the New Operating System and Application on Subsequent Nodes
<input type="checkbox"/>	Step 4 If required, upgrade the software to a later service release.	
<input type="checkbox"/>	Step 5 Configure the platform and Cisco Unified Communication Manager.	



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 Communication Manager application on a subsequent node.



Caution Before beginning this procedure, ensure you have already upgraded the Cisco Unified Communication Manager 4.x publisher server, configured the subsequent node on the Cisco Unified Communication Manager 5.1(1) 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 Media Check window displays.



Note If you have a new server that has Cisco Unified Communication Manager pre installed, you do not need to install from a DVD. Go directly to the “If You Choose Skip” procedure on page 3-6.

Step 2 Verify that the checksum that displays on the Media Check matches the checksum for the release on Cisco.com.

When the media check completes, the Media Check Result window displays.

Step 3 If the Media Check Result displays Pass, choose **OK** to continue the installation.

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



Note The installation process performs various hardware checks on your server and verifies RAID configuration and BIOS settings. If the installation process makes any changes to your hardware configuration settings, you will get prompted to restart your system.

The Overwrite Hard Drive window displays.

Step 4 The **Overwrite Hard Drive** window indicates the current software version on your hard drive, if any, 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 5 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 3-13.
- 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 3-13.

If You Choose Skip

Start here if you have a server that has Cisco Unified Communication Manager pre installed or if you chose **Skip** on Platform Installation Wizard window.

Step 6 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 7 To continue, choose **OK**.

The Platform Installation Wizard window displays.

Step 8 To continue with the installation, choose **Proceed**.

The Install During Upgrade window displays. Continue with the “If You Choose Proceed” section on page 3-13.

If You Choose Proceed

Step 9 Choose the type of installation to perform by doing the following steps. See Table 3-2 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 “Upgrade During Install” section on page 3-14.
 - 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 pre installed software with the basic installation. Continue with the “Basic Installation” section on page 3-16.

Upgrade During Install

If you chose Upgrade During Install, the installation wizard installs the software version on the DVD first and then restarts the system. You then get prompted to enter certain network configuration parameter values and the location of the upgrade file.

- Step 10** After the system restarts, the Platform Installation Wizard window displays. To continue the installation, choose **Proceed**.



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.

The Upgrade During Install window displays.

- Step 11** Choose **Yes**.

The Install Upgrade Retrieval Mechanism Configuration window displays.

- Step 12** Choose the upgrade retrieval mechanism that you want 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 “Upgrade From a Remote Server” section on page 3-15.
- **FTP**—Retrieves the upgrade file from a remote server by using File Transfer Protocol (FTP). Skip to the “Upgrade From a Remote Server” section on page 3-15.
- **LOCAL**—Retrieves the upgrade file from a local CD or DVD. Continue with the “Upgrade From a Local Disc” section on page 3-14.

Upgrade From a Local Disc

Before you can upgrade from a local drive, 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.

The patch-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.

- Step 13** 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.

The Install Upgrade Patch Selection Validation window displays.

- Step 14** The window displays the patch file that is available on the CD or DVD. To update the system with this patch, choose **Continue**.

Upgrade 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.

The Auto Negotiation Configuration window displays.

- Step 15** 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 16** 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 17** 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 the “Retrieving the Remote Patch” section on page 3-15.
 - If you want to configure static IP addresses for the node, choose **No**. The Static Network Configuration window displays.

- Step 18** If you chose not to use DHCP, enter your static network configuration values and choose **OK**. See Table 2-2 for field descriptions.

The DNS Client Configuration window displays.

- Step 19** To enable DNS, choose **Yes**, enter your DNS client information, and choose **OK**. See Table 2-2 for field descriptions.

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

Retrieving the Remote Patch

- Step 20** Enter the location and login information for the remote file server. See Table 2-2 for field descriptions. After restarting the network, the system connects to the remote server and retrieves a list of available upgrade patches.

To support retrieval of the patch file, an FTP server should support the CD, BIN, DIR, and GET commands., and an SFTP server should support CD, LS, GET commands.

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 21** Choose the upgrade patch that you want to install. The system downloads, unpacks, and installs the patch and then restarts the system, so it is running on the upgraded software version.

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

Using Preexisting Configuration Information

- Step 22** If you have preexisting configuration information 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.

The Platform Installation Wizard window displays.

- Step 23** To continue with the Platform Installation Wizard, choose **Proceed**.

The Product Installation Configuration window displays.

- Step 24** To configure the platform now, choose **Proceed**.

The Upgrade During Installation window displays.

- Step 25** In the Upgrade During Install window, choose **No**.

- Step 26** In the Windows Upgrade window, choose **No**.

- Step 27** In the Basic Install window, choose **Continue**. Continue with the “Basic Installation” section on page 3-16.

Basic Installation

- Step 28** When the Timezone Configuration displays, choose the appropriate time zone for the server and then choose **OK**.

The Auto Negotiation Configuration window displays.

- Step 29** 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 30** 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 31** 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 32** If you chose not to use DHCP, enter your static network configuration values and choose **OK**. See Table 2-2 for field descriptions.

The DNS Client Configuration window displays.

Step 33 To enable DNS, choose **Yes**, enter your DNS client information, and choose **OK**. See Table 2-2 for field descriptions.

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

Step 34 Enter your Administrator login and password from the Installation Information Worksheet.



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

The Certificate Signing Request Information window displays.

Step 35 Enter your certificate signing request information from the Installation Information Worksheet and choose **OK**.

The First Node Configuration window displays.

Step 36 To configure this server as a subsequent node in the cluster, choose **No**.

The First Node Access Configuration window displays.

Step 37 Enter the First Node Access Configuration information from the Installation Information Worksheet.

The SMTP Host Configuration window displays.

Step 38 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 39 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 40 To log in, enter the account name **CCMAdministrator** and the password that you entered during installation.

Step 41 Complete the post-upgrade tasks that are listed in the Post-Upgrade Checklist.

Related Training

Please check back for updated training links.



Post-Install

Introduction

In this section you will use the Post-Upgrade Checklist to complete all the tasks necessary after upgrading the system components.

Before You Begin

You should have completed the two installation tasks, Checklist for Upgrading the First Cisco Unified CM Node and Checklist for Upgrading Subsequent Nodes in the Cluster.

When You Are Done

You will have completed the Post-Upgrade Checklist and be ready to deploy your system.

Post-Upgrade Checklist

When you complete your upgrade of Cisco Unified Communication Manager, you must perform all appropriate tasks as described in the checklist below. Clicking a link in the “Task Details” column opens the referenced procedure in a popup window. Notes indicate where there are other sections of the referenced document important for background information or context.

Table 4-1 Post-Upgrade Checklist

		Post-Upgrade Task	Task Details (Links and Notes)
<input type="checkbox"/>	Step 1	If you previously had NIC teaming configured: Configure NIC teaming on each server.	On each Cisco Unified CM server, use the CLI to execute this command: set network failover enable This command is described in “Command Line Interface” in the <i>Cisco Unified CallManager Operating System Administration Guide, Release 5.1(1)</i> .
<input type="checkbox"/>	Step 2	Verify that all appropriate Cisco Unified Communication Manager services started. Verify that you can make internal calls. Verify that you can place and receive a call across gateways.	See Verifying Cisco Unified Communication Manager Services. For more information, refer to the following documents: <ul style="list-style-type: none"> Managing Services in the <i>Cisco Unified Communication Manager Serviceability Administration Guide</i> Service Management in the <i>Cisco Unified Communication Manager Serviceability System Guide</i> <p>Note The information in the 5.0(4) Guides applies to 5.1(1) as well.</p>
<input type="checkbox"/>	Step 3	If security is enabled on the cluster, you must configure CTL.	To configure CTL on the upgraded cluster <ol style="list-style-type: none"> Uninstall the existing CTL client. Install the new CTL client. Run the CTL client by using at least one of the previously used USB keys. Update the new CTL file on all nodes. Restart all nodes. For information about performing these tasks and about Cisco Unified Communication Manager security, refer to the <i>Cisco Unified Communication Manager Security Guide</i> .
<input type="checkbox"/>	Step 4	Configure the backup settings. Remember to back up your Cisco Unified Communication Manager data daily.	Refer to the <i>Disaster Recovery System Administration Guide</i> .
<input type="checkbox"/>	Step 5	The locale, English_United_States, installs automatically on the server. If required, you can add new locales to the server.	Refer to the <i>Cisco Unified Communications Operating System Administration Guide</i> .

Table 4-1 Post-Upgrade Checklist

		Post-Upgrade Task	Task Details (Links and Notes)
<input type="checkbox"/>	Step 6	If you are using Microsoft Active Directory or Netscape Directory, enable synchronization with the LDAP server.	For more information on directories, refer to the <i>Cisco Unified Communication Manager System Guide</i> (PDF). In the PDF, see the “Understanding the Directory” chapter. For more information on enabling synchronization, refer to the <i>Cisco Unified Communication Manager Administration Guide</i> .
<input type="checkbox"/>	Step 7	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: <ol style="list-style-type: none"> 1. Define all subsequent nodes in the cluster by adding the host name or IP address of subsequent Cisco Unified Communication Manager nodes to Cisco Unified Communication Manager Administration. For more information, refer to <i>Cisco Unified Communication Manager Administration Guide</i>. In the PDF, see the “Configuring a Server” chapter. 2. Install the new application and configure subsequent Cisco Unified Communication Manager nodes in the cluster. See the “Checklist for Upgrading Subsequent Nodes in the Cluster” section on page 3-11. Remember to enter the same security password that you used for the first node.
<input type="checkbox"/>	Step 8	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 <i>Cisco Unified Communications Operating System Administration Guide</i> for more information.
<input type="checkbox"/>	Step 9	Install the required client-side plug-ins, such as Cisco Unified Communication Manager Real-Time Monitoring Tool and Cisco Communication Manager Attendant Console.	From Cisco Unified Communication Manager Administration, choose Application>Plug-ins . For more information, see the <i>Cisco Unified Communication Manager Administration Guide</i> . In the PDF, see the “Installing Plug-ins” chapter.
<input type="checkbox"/>	Step 10	Inform end users that they must reconfigure their ring tones and background images after the upgrade.	These settings do not get migrated.

Verifying Cisco Unified Communication Manager Services

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

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

Procedure

- Step 1** Open a web browser on a computer with network access to the Cisco Unified Communication Manager server.
- Step 2** Enter the following url:
`http://ccm_server:8080/ccadmin`
where *ccm_server* specifies the IP address or hostname of the Cisco Unified Communication Manager server.
- Step 3** Enter the Cisco Unified Communication Manager Administrator user name and password.
- Step 4** From the Navigation menu, choose Cisco Unified Communication Manager Serviceability and click **Go**.
- Step 5** Navigate to **Tools > Service Activation**.
- Step 6** Verify that all migrated services are running.
-

Related Training

Please check back for updated training links.



Resources

Overview of Resources

This section provides links to documentation and training resources for additional Cisco Unified Communications Manager information.

Documentation Resources

[Cisco Unified Communications Manager documentation home page](#)

[Cisco Unified Communications System for IP Telephony Technical Information Site Release 5.1\(1\)](#)

[Cisco Unified Communications System for Contact Center Technical Information Site Release 5.1\(1\)](#)

Training Resources

[Training Available to Partners](#)



Help

This information system, the Cisco Information Access Manager (IAM), is designed to give you an easily-navigable portal to all documentation for your system, solution, or product. The following sections describe using the IAM:

- About the IAM Window
- Types of Topics
- Comprehensive Index (in some IAMs)
- Graphics with Hotspots and Popup Text (Image Maps)
- Where Information Is Located
- About the Secondary Browser Window
- Tips on Using The IAM



Note

Please make sure your browser does not block popup windows for this site. If a popup link fails to open, check your browser settings. Alternatively, press **Ctrl** when you click the link to override your browser's settings.

About the IAM Window

The IAM window is laid out so that you can navigate easily between topic areas, drill down to get detailed information, and directly access product and platform documentation, without ever losing your place or having to cope with a complex hierarchy of windows.

Figure 5-1 shows an example of an IAM window. View descriptions of numbered screen elements in Table 5-1.



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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

Figure 5-1 Example of Information Access Manager Window

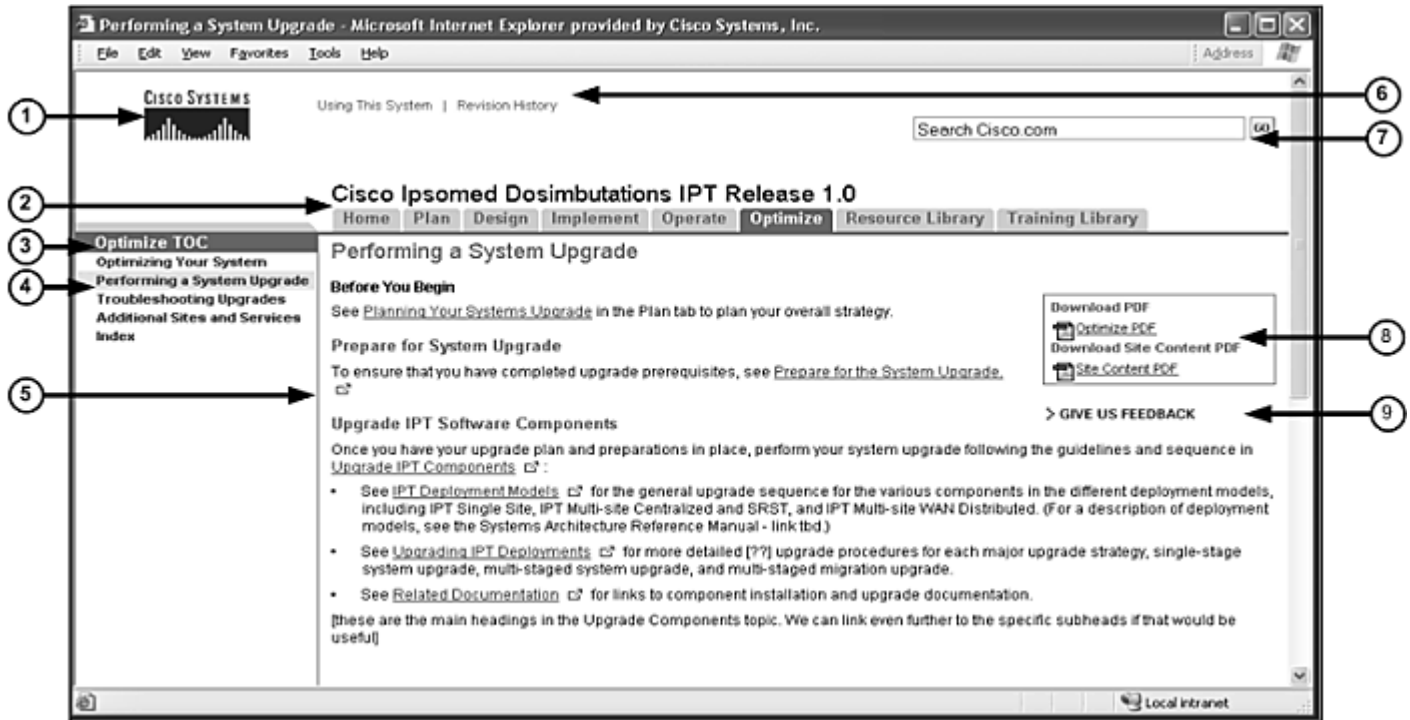



Table 5-1 Key to Screen Illustration

- | | |
|--|---|
| <p>1 Cisco logo. Click to go to Cisco Systems home page, replacing the IAM in the browser (the Back button takes you back to the IAM window).</p> <p>2 Tabs for global navigation between processes or other major categories. Click a tab to go to the home page for that tab. The table of contents (TOC) changes, showing topics specific to that tab. In the first content pane for a tab, you are shown an overview of what's in the tab and the tasks and concepts covered.</p> <p>3 TOC for navigation within a tab. The TOC changes when you click a different tab.</p> <p>Some IAMs have an Index link at the bottom of every tab. Click for an index for the entire IAM. Use this if you aren't sure where to find a topic.</p> | <p>4</p> <p>5</p> <p>6 Access-from-anywhere links to Using This System and Revision History. (These may have different titles.)</p> <p>7 Search box: Use to search all of Cisco.com, not specifically this IAM. Search list appears in a new window so you don't lose your place here.</p> <p>8 Download Adobe Acrobat PDF of content of this tab or entire site content</p> <p>Note Like any PDF, the PDF does not include linked content.</p> <p>9</p> |
|--|---|

Table 5-1 Key to Screen Illustration

4	Main heading in a TOC, such as "Performing a System Upgrade". If the heading is blue, it is a link that goes to a topic in the content area. If it is black, it is unlinked and simply a title for linked subtopics below. A highlight in the TOC indicates the current topic displayed in the content pane.	9	GIVE US FEEDBACK: Click to go the Feedback form at the bottom of the page. [do not use for alpha feedback, please use the Livelink discussion mailer columbusdocfeedback@elink.cisco.com.]
5	Content pane, where the information resides. Note two kinds of links in the content pane: <ul style="list-style-type: none">• A link to another topic in the content pane looks like an ordinary link. Clicking the link switches the contents of this pane.• A link to a secondary topic has a popup icon . Clicking the link opens a new browser window, offset from the current window. If the window is already open, the topic replaces the current contents.		

Types of Topics

When you see a reference to a topic, you can tell what type of topic it is by its name:

- “Doing” topics, such as “Installing the Cisco CallManager”, are *task topics*, and provide instructions for doing something.
- “Overview” or “About” topics are *concepts* to help you understand and plan your deployment and carry out tasks knowledgeably.

Some tabs may group topics under headings such as “Planning Concepts” and “Planning Tasks.”

Comprehensive Index (in some IAMs)



If you see an Index link at the bottom of the TOC, you can click it to view a hyperlinked index to all the topics in the IAM. Use this if you aren’t sure where to find a topic you are interested in.

Graphics with Hotspots and Popup Text (Image Maps)



Some graphics in the IAM may be image maps. An image map may have hotspots you can run your pointer over to view a popup description or click to open a linked topic in a secondary window.

Where Information Is Located

Cisco systems and solutions encompass a range of products and technologies, and their documentation encompasses information that may reside in several locations:

-
- Overviews and high-level process and procedure information specific to your solution or system are included directly in the IAM.
 - Product and technology overviews, detailed requirements, task details, and other more generic topics are located outside the IAM. These topics have the appearance of standard Cisco documentation with which you may already be familiar. Links to these topics appear with the popup icon , for example, [Installing the Cisco Unified CallManager](#) . This means that clicking the link opens the topic in a new, secondary browser window offset from the current window, rather than replacing the current topic in the content area of the current window. You can click to view the information when you need it, and then return to your place in the main IAM flow.

About the Secondary Browser Window

When a topic like [Installing the Cisco Unified CallManager](#)  opens in a new, secondary browser window, that window stays open until you close it. (Click the **Close** button or choose **File > Close**.) If the window is open when you click another  link, the new topic replaces the current one. You can use the browser **Back** button if you want to retrace your steps in the secondary window.

Tips on Using The IAM

- Use tabs to navigate between major process areas.
- Use the left navigation menu to navigate to major topics on a tab.
- In a secondary popup window:
 - When you are done with the window, click the **Close** button to close it. (It does not close automatically.)
 - You can go back to a previous topic by right-clicking and choosing **Back**.
 - You can view normal browser toolbars, the address bar, and any other browser items you don't see by using commands on the **View** menu.
- (In some IAMs) Use the **Index** (click the link at the bottom of any tab) if you aren't sure where to find a topic you are interested in.



History

This technical information site for the Cisco Unified Communications Manager upgrade is updated periodically. Check here for to find out the latest documentation release.

10/8/2007: Moved licensing step from Pre-Upgrade to Install Checklist; added step on NIC speed and duplex settings to Pre-Upgrade Checklist; corrected minor errata.

8/28/2007: Corrections of minor errata.

8/14/2007: First customer release. Adds information on NIC teaming and licensing

Draft releases:

8/10/2007: Incorporates changes from UC Upgrade Checklist Core Team Meeting Minutes 8/6/07 and test review through 8/10/2007.

8/2/2007: Incorporates information from review comments summarized in UC Upgrade Checklist Core Team Meeting Minutes 7/30/07.

July 19, 2007 release: Initial review



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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

