



Upgrading Cisco Unified CallManager Release 5.1(1)

The 5.0(x) release of Cisco Unified CallManager uses a different installation framework than previous releases of Cisco Unified CallManager. Before upgrading to Cisco Unified CallManager 5.1(1), review all installation instructions carefully. This document includes information about upgrading to Cisco Unified CallManager 5.1(1) from a Cisco Unified CallManager 4.x release. This document also provides instructions for installing software patches and upgrade software after you have upgraded to Cisco Unified CallManager 5.1(1).

Contents

This document contains the following topics:

- [Installation Overview](#)
- [Related Documentation](#)
- [Important Considerations](#)
- [Frequently Asked Questions About the Cisco Unified CallManager Installation](#)
- [Browser Requirements](#)
- [Configuring the Hardware](#)
- [Upgrading Cisco Unified CallManager](#)
- [Upgrading the First Cisco Unified CallManager Node](#)
- [Upgrading Subsequent Nodes in the Cluster](#)
- [Post-Upgrade Tasks](#)
- [Installing Upgrade Software After Upgrading to Cisco Unified CallManager 5.1\(1\)](#)
- [Using the Disaster Recovery Disc](#)
- [Examining Log Files](#)
- [Obtaining Documentation](#)
- [Documentation Feedback](#)



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

© 2006 Cisco Systems, Inc. All rights reserved.

- [Cisco Product Security Overview](#)
- [Obtaining Technical Assistance](#)

Installation Overview

Cisco Unified CallManager 5.1(1) uses a different installation framework than previous releases. The installation process allows you to perform a basic installation, upgrade from Cisco Unified CallManager 4.x to Cisco Unified CallManager 5.1(1), and upgrade to a newer service release during the installation.

For a more detailed description of the different installation types, see [Table 1](#).

Table 1 *Installation Options*

Installation Types	Description
Basic Install	This option represents the basic Cisco Unified CallManager 5.1(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 the installation disc contains with the latest service release. You can also choose Upgrade During Install followed by a Windows Upgrade and perform both during the installation process.
Windows Upgrade	This option allows you to import database information from a Cisco Unified CallManager 4.x system by using a file that the Data Migration Assistant (DMA) tool produces.



Note

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

Related Documentation

Cisco strongly recommends that you review the following documents before you perform the Cisco Unified CallManager installation:

- *Cisco Unified CallManager Administration Guide* and *Cisco Unified CallManager System Guide*
The *Cisco Unified CallManager Administration Guide* provides step-by-step instructions for configuring, maintaining, and administering the Cisco Unified CallManager voice over IP network.
The *Cisco Unified CallManager System Guide* provides descriptions of the Cisco Unified CallManager system and its components, configuration checklists, and links to associated *Cisco Unified CallManager Administration Guide* procedures.
- *Cisco Unified CallManager Features and Services Guide*
This document describes how to configure features and services for Cisco Unified CallManager, including Cisco Music On Hold, Cisco Unified CallManager Extension Mobility, and so on.

- The *Cisco Unified CallManager Serviceability System Guide* and *Cisco Unified CallManager Serviceability Administration Guide*
These documents provide descriptions of Cisco Unified CallManager serviceability and remote serviceability and step-by-step instructions for configuring alarms, traces, and other reporting.
- *Disaster Recovery System Administration Guide*
This document describes how to configure the backup settings, back up Cisco Unified CallManager data, and restore the data.
- *Data Migration Assistant User Guide*
This document provides procedures for migrating data from earlier versions of Cisco Unified CallManager.
- *Cisco Unified Communications Operating System Administration Guide*
This document provides information on how to access and use the utilities that are available on the platform. This document also includes instructions for installing new locales.
- *Cisco Unified CallManager Security Guide*
This document provides instructions on how to configure and troubleshoot authentication and encryption for Cisco Unified CallManager, Cisco Unified IP Phones, SRST references, and Cisco MGCP gateways.

Table 2 lists URLs for software and additional documentation.

Table 2 Quick Reference for URLs

Related Information and Software	URL
Cisco MCS data sheets	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/index.html
Software-only servers (IBM, HP, Compaq, Aquarius)	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html
<i>Cisco Unified CallManager Compatibility Matrix</i>	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/cmcomp.htm
Cisco Unified CallManager documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm
<i>Cisco Unified CallManager Security Guide</i>	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/ae/index.htm
Cisco Unified CallManager backup and restore documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm
Cisco Unified CallManager service releases	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml
Related Cisco IP telephony application documentation	http://www.cisco.com/univercd/cc/td/doc/product/voice/index.htm

Important Considerations

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

- Be aware that when you install Cisco Unified CallManager 5.1(1) on an existing server, the hard drive gets formatted, and all existing data on the drive gets overwritten.
- Be aware that all secure phones will remain down during the upgrade process.
- Install the Cisco Unified CallManager software on the first node, or publisher, server first and then on the subsequent nodes. You must configure the subsequent nodes on the first node before you can install the subsequent node.
- Enter the same security password on all servers in the cluster.
- Before you can install subsequent, or subscriber, nodes, you must first configure them on the first, or publisher, node.
- Install the Cisco Unified CallManager software during off-peak hours or a maintenance window to avoid impact from call-processing interruptions.
- Configure the server by using static IP addressing to ensure that the server obtains a fixed IP address and that the Cisco Unified IP Phones can register with the application when you plug the phones into the network.
- You must have access to an SFTP server to back up Cisco Unified CallManager over a network.
- Do not attempt to perform any configuration tasks during the installation.
- Do not install any Cisco-verified applications until you complete installing Cisco Unified CallManager on every server in the cluster.
- Be aware that customer background images, custom TFTP files, custom MoH files, and customer ring tones do not get migrated during the upgrade process. You must reinstall these files after the upgrade completes. See the [“Post-Upgrade Tasks” section on page 32](#) for more information.
- Be aware that end-user settings such as ring tones and background images do not get migrated during the upgrade process. The end user must reconfigure these items after the upgrade completes.
- Carefully read the instructions that follow before you proceed with the installation

Frequently Asked Questions About the Cisco Unified CallManager Installation

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

How long does it take to perform the Cisco Unified CallManager Windows Upgrade?

The entire upgrade process, excluding pre- and post-installation tasks, takes approximately 60 to 100 minutes per server, depending on your server type and the number of database entries that you have configured on the Cisco Unified CallManager server. The following tables provide Windows upgrade performance measurements for three different servers with various database sizes.

MCS-7845H-3000 Typical Windows Upgrade Performance Measurements

Table 3 shows the upgrade performance measurements for an MCS-7845H-3000 server that is configured as follows:

- CPUs: 2, 3.066 GHz
- Memory: 4 GB
- Hard drives: 4, 72 GB, RAID 1+0

Table 3 MCS-7845H-3000 Typical Windows Upgrade Performance Measurements

Performance Measure	Publisher With 500 Database Entries	Publisher With 2500 Database Entries	Publisher With 10,000 Database Entries	Subscriber With 2500 Database Entries
System Boot From DVD	1.5 minutes	1.5 minutes	1.5 minutes	1.5 minutes
DVD Checksum	8 minutes	8 minutes	8 minutes	8 minutes
RIOS/RAID Setting	0.5 minutes	0.5 minutes	0.5 minutes	0.5 minutes
Reboot	2 minutes	2 minutes	2 minutes	2 minutes
DVD Checksum	8 minutes	8 minutes	8 minutes	8 minutes
Start Installing (Skip option)	21 minutes	21 minutes	21 minutes	21 minutes
Reboot	2 minutes	2 minutes	2 minutes	2 minutes
Installation and Configuration	42 minutes	43.5 minutes	50 minutes	23 minutes
Service Start	5 minutes	5 minutes	5 minutes	5 minutes
Total	90 minutes	91.5 minutes	98 minutes	71 minutes

MCS-7835-H1 Typical Windows Upgrade Performance Measurements

Table 4 shows the upgrade performance measurements for an MCS-7835-H1 server that is configured as follows:

- CPUs: 1, 3.4 GHz
- Memory: 2 GB
- Hard drives: 1, 72 GB

Table 4 MCS-7835-H1 Typical Windows Upgrade Performance Measurements

Performance Measure	Publisher With 500 Database Entries	Publisher With 2500 Database Entries	Publisher With 10,000 Database Entries	Subscriber With 2500 Database Entries
System Boot From DVD	1.5 minutes	1.5 minutes	1.5 minutes	1.5 minutes
DVD Checksum	6 minutes	6 minutes	6 minutes	6 minutes
RIOS/RAID Setting	0.5 minutes	0.5 minutes	0.5 minutes	0.5 minutes
Reboot	2 minutes	2 minutes	2 minutes	2 minutes
DVD Checksum	6 minutes	6 minutes	6 minutes	6 minutes
Start Installing (Skip option)	13 minutes	13 minutes	13 minutes	13 minutes

Table 4 MCS-7835-H1 Typical Windows Upgrade Performance Measurements (continued)

Performance Measure	Publisher With 500 Database Entries	Publisher With 2500 Database Entries	Publisher With 10,000 Database Entries	Subscriber With 2500 Database Entries
Reboot	2 minutes	2 minutes	2 minutes	2 minutes
Installation and Configuration	33 minutes	35 minutes	40 minutes	17 minutes
Service Start	5 minutes	5 minutes	5 minutes	5 minutes
Total	69 minutes	71 minutes	76 minutes	53 minutes

MCS-7825-H1 Typical Windows Upgrade Performance Measurements

Table 5 shows the upgrade performance measurements for an MCS-7825-H1 server that is configured as follows:

- CPUs: 1, 3.4 GHz
- Memory: 2 GB
- Hard drives: 1, 72 GB

Table 5 MCS-7825-H1 Typical Windows Upgrade Performance Measurements

Performance Measure	Publisher With 500 Database Entries	Publisher With 1000 Database Entries	Subscriber With 1000 Database Entries
System Boot From DVD	1.5 minutes	1.5 minutes	1.5 minutes
DVD Checksum	10 minutes	10 minutes	10 minutes
RIOS/RAID Setting	0.5 minutes	0.5 minutes	0.5 minutes
Reboot	2 minutes	2 minutes	2 minutes
DVD Checksum	10 minutes	10 minutes	10 minutes
Start Installing (Skip option)	21.5 minutes	21.5 minutes	21.5 minutes
Reboot	2 minutes	2 minutes	2 minutes
Installation and Configuration	40 minutes	42 minutes	20 minutes
Service Start	5 minutes	5 minutes	4 minutes
Total	92.5 minutes	94.5 minutes	71.5 minutes

What Passwords do I Need to Specify?

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

- Administrator account

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

- Platform 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 the following default application user names:

- CCMAAdministrator
- CCMSysUser
- WDSysUser
- CCMQRTSysUser
- IPMASysUser
- WDSecureSysUser
- CCMQRTSecureSysUser
- IPMASecureSysUser

You can change the application user password for each application in Cisco Unified CallManager Administration through **User Management>Application User**. See the *Cisco Unified CallManager Administration Guide* for more information.

- Database Access Security Password

The system uses this password to authorize communications between nodes, and this password must be the same on all nodes in the cluster.

The Database Access Security password must start with an alphanumeric character, be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores.

- End User Password and PIN

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



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

Which servers does Cisco support for this installation?

To find which servers support Cisco CallManager 5.0 releases, refer to the Guide to Cisco CallManager Upgrades and Server Migrations at

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

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

For Cisco Unified CallManager 5.1(1), you must do all software installations and upgrades by using the Software Upgrades menu options in Platform Administration. The system can upload and process only software that Cisco Systems approved. You cannot install or use third-party or Windows-based software applications that you may have been using with a previous version of Cisco Unified CallManager with Cisco Unified CallManager 5.1(1).

Browser Requirements

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

- Microsoft Internet Explorer version 6.0 or later
- Netscape Navigator version 7.1 or later



Note

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

Configuring the Hardware

As a part of software installation, the system installer configures the system BIOS and RAID settings for the new operating system and Cisco Unified CallManager application. See [Table 6](#) for the BIOS settings and [Table 7](#) 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 6](#) and [Table 7](#).

Table 6 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 7 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.		

Upgrading Cisco Unified CallManager

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

- [Performing Pre-Upgrade Tasks, page 9](#)
- [Gathering Information for an Installation, page 11](#)
- [Handling Network Errors During Installation, page 17](#)
- [Upgrading the First Cisco Unified CallManager Node, page 17](#)
- [Navigating Within the Installation Wizard, page 18](#)
- [Selecting an Installation Option, page 18](#)
- [Installing the New Operating System and Application on the First Node, page 19](#)
- [Upgrading Subsequent Nodes in the Cluster, page 26](#)
- [Post-Upgrade Tasks, page 32](#)

Performing Pre-Upgrade Tasks

Perform the following tasks before you begin the upgrade:

	Pre-Upgrade Task	Important Notes
Step 1	Verify that you meet the system requirements for upgrading Cisco Unified CallManager nodes in the cluster.	See the “ Which servers does Cisco support for this installation? ” section on page 8.
Step 2	Run Cisco Unified CallManager Upgrade Utility on the server to verify that the system is ready for upgrade.	Refer to <i>Using Cisco Unified CallManager Upgrade Utility</i> .
Step 3	Perform the recommended backup procedures on the publisher server. Back up every database that is associated with your Cisco Unified CallManager server.	Refer to <i>Cisco IP Telephony Backup and Restore System (BARS) Administration Guide</i> .

Pre-Upgrade Task	Important Notes
<p>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>	<p>For more information on CAR, refer to the <i>CDR Analysis and Reporting Administration Guide</i>.</p>
<p>Step 5 If you do not need to carry over your CDR data to Cisco Unified CallManager 5.1(1), Cisco recommends that you purge the CDR data before you run DMA.</p>	<p>Purging the CDR data speeds up the migration process and decreases the size of the DMA TAR file.</p>
<p>Step 6 Export the data on the current Cisco Unified CallManager 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>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 CallManager 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>Step 7 Before the upgrade, obtain the necessary information for configuring the platform and Cisco Unified CallManager on the first and subsequent nodes.</p>	<p>See the “Gathering Information for an Installation” section on page 11.</p>
<p>Step 8 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 the “Assigning the Host Name/IP Address (Servername) to the 5.1(1) Server” section on page 18</p>
<p>Step 9 Familiarize yourself with the navigation options within the installation wizards.</p>	<p>See “Navigating Within the Installation Wizard” section on page 18.</p>

Gathering Information for an Installation

Use [Table 8 on page 11](#) to record the information about your Cisco Unified CallManager server. Gather this information for each Cisco Unified CallManager server that you are installing in the cluster. You may not need to obtain all the information; gather only the information that is pertinent to your system and network configuration. You 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

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 8 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

Table 8 Configuration Data (continued)

Configuration Data	Your Entry	Can Entry Be Changed After Installation
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
Time Zone		Yes CLI > Set Timezone
Unit		Yes CLI > set web-security

Table 8 Configuration Data (continued)

Configuration Data	Your Entry	Can Entry Be Changed After Installation
End-User Password		Yes See “End User Configuration” in the <i>Cisco Unified CallManager Administration Guide</i> .
End-User PIN		Yes See “End User Configuration” in the <i>Cisco Unified CallManager Administration Guide</i> .

For more detailed descriptions of each installation field, see [Table 9](#).

Table 9 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 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.
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.

Table 9 *Installation Field Definitions (continued)*

Field	Description	Usage
DNS Enabled	<p>A DNS server represents a device that resolves a hostname into an IP address or an IP address into a hostname.</p> <p>Note You cannot change the DNS settings after the installation is complete. To change DNS settings, you must reinstall Cisco Unified CallManager.</p>	<p>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.</p> <p>If you have a DNS server, Cisco recommends entering Yes to enable DNS. Disabling DNS limits the system ability to resolve some domain names.</p>
DNS Primary	<p>Cisco Unified CallManager contacts this DNS server first when it attempts to resolve host names.</p>	<p>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).</p> <p>Consider this field mandatory if DNS is set to yes.</p>
DNS Secondary	<p>When a primary DNS server fails, Cisco Unified CallManager will attempt to connect to the secondary DNS server.</p>	<p>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).</p>
Domain	<p>This field represents the name of the domain in which this machine is located.</p>	<p>Consider this field mandatory if DNS is set to yes.</p>
First Cisco Unified CallManager Node	<p>The first Cisco Unified CallManager node contains the database.</p> <p>Subsequent nodes connect to the 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 CallManager node in the cluster.</p> <p>If you are configuring subsequent nodes, see Table 9 for information on the different fields.</p>

Table 9 *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)
NIC Speed	This field specifies the speed of the server network interface card (NIC) in megabits per second.	The possible speeds comprise 10 or 100.
NIC Duplex	This field specifies the duplex setting of the server NIC.	The possible settings comprise half and full.

Table 9 Installation Field Definitions (continued)


Field	Description	Usage
NTP Server	This field identifies the NTP server with which you want to keep time synchronization.	<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>
Security Password	<p>Cisco Unified CallManager 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	This field specifies the name of the SMTP host that is used for outbound e-mail.	<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>

Table 9 *Installation Field Definitions (continued)*

Field	Description	Usage
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.

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.

Upgrading the First Cisco Unified CallManager Node

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

1. Verify that you have completed all pre-upgrade tasks. See the [“Performing Pre-Upgrade Tasks” section on page 9](#).
2. Familiarize yourself with navigation within the installation wizard. See the [“Navigating Within the Installation Wizard” section on page 18](#).
3. Know which installation options to choose. See [Table 11 on page 18](#).
4. Configure the hardware with the hardware configuration disc. See the [“Configuring the Hardware” section on page 8](#).
5. Install the new operating system on the first node. See the [“Installing the New Operating System and Application on the First Node” section on page 19](#)
6. Perform the appropriate post-upgrade tasks. See the [“Post-Upgrade Tasks” section on page 32](#).

Navigating Within the Installation Wizard

For instructions on how to navigate within the installation wizard, see [Table 10](#).

Table 10 *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)

Selecting an Installation Option

After the platform software installation starts, you will be asked to select one of the options that [Table 11](#) lists.

Table 11 *Installation Options*

Installation Options	Description
Basic Install	This option represents the basic installation and does not use any imported data.
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 CallManager 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/IP Address (Servername) 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.

Installing the New Operating System and Application on the First Node

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


Caution

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

Procedure

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



Note If you have a new server with preinstalled Cisco Unified CallManager, you do not need to install from a DVD. Go directly to the [“If You Choose Skip” procedure on page 20](#).

- 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 21](#).
- 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 20](#).

If You Choose Skip

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

Step 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 21](#).

If You Choose Proceed

- Step 9** Choose the type of installation to perform by doing the following steps. See [Table 11](#) 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 21](#).
 - 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 23](#).



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

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 22](#).
- **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 22](#).
- **LOCAL**—Retrieves the upgrade file from a local CD or DVD. Continue with the [“Upgrade From a Local Disc” section on page 21](#).

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.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 22.
 - 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 9](#) 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 9](#) 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 9](#) 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 23](#).

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 9](#) 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 9](#) for field descriptions.

The Administrator Login Configuration window displays.

Step 34 Enter your administrator login and password from [Table 8 on page 11](#).

The Certificate Signing Request Information window displays.

Step 35 Enter your certificate signing request information from [Table 8 on page 11](#) 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 8](#).



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 8](#) 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/IP Address \(Servername\) to the 5.1\(1\) Server”](#) section on page 18.

- 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.
- Step 51** Complete the post-upgrade tasks that are listed in the “[Post-Upgrade Tasks](#)” section on page 32.
-

Upgrading Subsequent Nodes in the Cluster

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

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

To upgrade a subsequent node in the cluster from Cisco Unified CallManager 4.x to Cisco Unified CallManager 5.1(1), perform the following steps:

1. Upgrade the first node, the Cisco Unified CallManager 4.x publisher server, to Cisco Unified CallManager 5.1(1).
2. Using Cisco Unified CallManager Administration on the first node, configure the subsequent nodes.
3. Ensure that the subsequent nodes have network connectivity to the first node.
4. Install the new operating system and Cisco Unified CallManager application from a DVD.
5. If required, upgrade the software to a later service release.
6. Configure the Platform and Cisco Unified CallManager.

**Note**

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

Install the New Operating System and Application on Subsequent Nodes

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

**Caution**

Before beginning this procedure, ensure you have already upgraded the Cisco Unified CallManager 4.x publisher server, configured the subsequent node on the Cisco Unified CallManager 5.1(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 CallManager preinstalled, you do not need to install from a DVD. Go directly to the [“If You Choose Skip” procedure on page 20](#).

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 28](#).
- 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 27](#).

If You Choose Skip

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

Step 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 28.

If You Choose Proceed

- Step 9** Choose the type of installation to perform by doing the following steps. See [Table 11](#) 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 28.
 - To skip this step, choose **No**.
 - To return to the previous window, choose **Back**.
 - b. In the Windows Upgrade window, choose **No**.
 - c. In the Basic Install window, choose **Continue** to install the software version on the DVD or configure the preinstalled software with the basic installation. Continue with the [“Basic Installation”](#) section on page 30.

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 29.
 - **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 29.
 - **LOCAL**—Retrieves the upgrade file from a local CD or DVD. Continue with the [“Upgrade From a Local Disc”](#) section on page 28.

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 30](#).
- 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 9](#) 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 9](#) 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 9](#) 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 30](#).

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 9](#) 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 9](#) 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 [Table 8](#).



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 [Table 8](#) 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 [Table 8](#).

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 Tasks](#)” section on page 32.
-

Post-Upgrade Tasks

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

Table 12 Post-Upgrade Tasks

Post-Upgrade Tasks	Important Notes
<p>Verify that all appropriate Cisco Unified CallManager services started.</p> <p>Verify that you can make internal calls.</p> <p>Verify that you can place and receive a call across gateways.</p>	<p>Refer to the following documents:</p> <ul style="list-style-type: none"> • <i>Cisco Unified CallManager Serviceability Administration Guide</i> • <i>Cisco Unified CallManager Serviceability System Guide</i> <p>See the “Verifying Cisco Unified CallManager Services” section on page 33.</p>
<p>If security is enabled on the cluster, you must configure CTL.</p>	<p>To configure CTL on the upgraded cluster</p> <ol style="list-style-type: none"> 1. Uninstall the existing CTL client. 2. Install the new CTL client. 3. Run the CTL client by using at least one of the previously used USB keys. 4. Update the new CTL file on all nodes. 5. Restart all nodes. <p>For information about performing these tasks and about Cisco Unified CallManager security, refer to the <i>Cisco Unified CallManager Security Guide</i>.</p>
<p>Configure the backup settings.</p> <p>Remember to back up your Cisco Unified CallManager data daily.</p>	<p>Refer to the <i>Disaster Recovery System Administration Guide</i>.</p>
<p>The locale, English_United_States, installs automatically on the server. If required, you can add new locales to the server.</p>	<p>Refer to the <i>Cisco Unified Communications Operating System Administration Guide</i>.</p>
<p>Cisco recommends that you implement authentication and encryption in your Cisco IP Telephony network.</p>	<p>Refer to the <i>Cisco Unified CallManager Security Guide</i>.</p>
<p>If you are using Microsoft Active Directory or Netscape Directory, enable synchronization with the LDAP server.</p>	<p>For more information on directories, refer to the <i>Cisco Unified CallManager System Guide</i>.</p> <p>For more information on enabling synchronization, refer to the <i>Cisco Unified CallManager Administration Guide</i>.</p>
<p>Upgrade subscriber servers as subsequent Cisco Unified CallManager nodes in the cluster.</p>	<p>Remember to enter the same security password for the first node.</p> <p>See the “Upgrading Subsequent Nodes in the Cluster” section on page 26</p>

Table 12 Post-Upgrade Tasks (continued)

Post-Upgrade Tasks	Important Notes
Install and configure subsequent Cisco Unified CallManager nodes in the cluster.	Subscriber servers automatically get defined as subsequent nodes in the database. Remember to enter the same security password that you used for the first node. See the “Upgrading Subsequent Nodes in the Cluster” section on page 26
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 CallManager nodes to Cisco Unified CallManager Administration. For more information, refer to <i>Cisco Unified CallManager Administration Guide</i>. 2. Install the new application and configure subsequent Cisco Unified CallManager nodes in the cluster. See the “Upgrading Subsequent Nodes in the Cluster” section on page 26. Remember to enter the same security password that you used for the first node.
Reinstall customer background images, custom TFTP files, custom MoH files, and customer ring tones.	To upload these files, log in to Cisco Unified Communications Operating System Administration and navigate to the Software Upgrades>Upload TFTP Server File menu. See the <i>Cisco Unified Communications Operating System Administration Guide</i> for more information.
Install the required client-side plug-ins, such as Cisco Unified CallManager Real-Time Monitoring Tool and Cisco CallManager Attendant Console.	From Cisco Unified CallManager Administration, choose Application>Plugins . For more information, see the <i>Cisco Unified CallManager Administration Guide</i> .
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 CallManager Services

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

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

Procedure

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

Installing Upgrade Software After Upgrading to Cisco Unified CallManager 5.1(1)

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

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

**Note**

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

Upgrading the System

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

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

From Local Source

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


Note

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

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

Procedure

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


Note

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

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

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


Note

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

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

`http://server-name/iptplatform`

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

Step 5 Enter your Administrator username and password.

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

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

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

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

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

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

When the download completes, the Checksum window displays.

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


Caution

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

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

A Warning window displays the current and upgrade software versions.

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

The Post Installation Options window displays.

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

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

Step 16 Click **Upgrade**.

The Upgrade Status windows displays and displays the Upgrade log.

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

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

The Switch Software Version window displays.

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

The Switch Software Version window displays.

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

From Remote Source

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



Note

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

Procedure

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

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

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

If the upgrade file is located on a Linux or Unix server, you must enter a forward slash at the beginning of the directory path. For example, if the upgrade file is in the patches directory, you must enter **/patches**. If the upgrade file is located on a Windows server, check with your system administrator for the correct directory path.

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

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

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

Step 5 Click **Next**.

The system checks for available upgrades.

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

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

When the download completes, the Checksum window displays.

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



Caution

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

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

A Warning window displays the current and upgrade software versions.

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

The Post Installation Options window displays.

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

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

Step 12 Click **Upgrade**.

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

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

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

The Switch Software Version window displays.

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

Reverting to a Previous Version

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

Procedure

-
- Step 1** Open Cisco Unified Communications Operating System Administration directly by entering the following URL:
- http://server-name/iptplatform**
- where *server-name* is the host name or IP address of the Cisco Unified CallManager server.
- Step 2** Enter your Administrator username and password.
- Step 3** Choose **Restart>Switch Versions**.
- The Switch Software Version window displays.
- When you verify that you want to restart the system, the system restarts running the upgraded software.
-

Using the Disaster Recovery Disc

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

Reverting to a Previous Version of Cisco Unified CallManager

If the upgrade from Cisco Unified CallManager 4.x to Cisco Unified CallManager 5.1(1) is unsuccessful, you can use the Disaster Recovery Disc to revert to a Windows-based version of Cisco Unified CallManager.



Caution

If you revert to a previous version of Cisco Unified CallManager, you will lose any configuration changes that you made by using Cisco Unified CallManager 5.1(1).

To use the Disaster Recovery Disk, use this procedure:

Procedure

-
- Step 1** Insert the Disaster Recovery disc and restart the system, so it boots from the CD. After the server completes the boot sequence, the Disaster Recovery menu displays.
- Step 2** For Windows preinstallation setup, enter **W**.
- Step 3** To continue, enter **Yes**.



Caution

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

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

- Step 4** Following the instructions in the installation guide for your Windows-based version of Cisco Unified CallManager, install Cisco Unified CallManager on the publisher server first and then on the subscriber nodes.
- Step 5** Using the Cisco Unified Communications Backup and Restore System (BARS), restore the previously backed-up data to the servers. For more information, see the *Cisco Unified Communications Backup and Restore System Administration Guide* for your version of BARS.
-

Switching Partitions

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



Caution

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

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

Procedure

- Step 1** Insert the Disaster Recovery disc and restart the system, so it boots from the CD. After the server completes the boot sequence, the Disaster Recovery menu displays.
- Step 2** To restart the server, so it is running the software on the currently inactive partition, enter **S**.
- Step 3** Press **Enter**.
- The server restarts.
-

Examining Log Files

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

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

```
CLI>file list install
```

To view the log file from the command line, enter

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

where *log_file* is the log file name.

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

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

<http://www.cisco.com/univercd/home/home.htm>

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

If you do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: <http://tools.cisco.com/RPF/register/register.do>) Registered users can access the tool at this URL: <http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the **Cisco Product Identification Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

**Tip**

Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411

Australia: 1 800 805 227

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:
<http://www.cisco.com/offer/subscribe>
- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:
<http://www.cisco.com/go/guide>
- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:
<http://www.cisco.com/univercd/cc/td/doc/abtnicd/136957.htm>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

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, 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. (0609R)

Copyright © 2006. Cisco Systems, Inc. All rights reserved.

