



Installing Cisco Unified Presence Server Release 1.0(3)

This document contains information about installing Cisco Unified Presence Server on one server or several servers in a cluster environment.

Contents

This document contains the following topics:

- [Introduction, page 2](#)
- [Related Documentation, page 2](#)
- [Important Considerations, page 2](#)
- [Frequently Asked Questions About the Cisco Unified Presence Server Installation, page 3](#)
- [Browser Requirements, page 4](#)
- [Configuring the Hardware, page 5](#)
- [Installation Overview, page 5](#)
- [Performing Pre-Installation Tasks, page 6](#)
- [Gathering Information for an Installation, page 6](#)
- [Selecting an Installation Option, page 12](#)
- [Installing Cisco Unified Presence Server, page 12](#)
- [Performing Post-Installation Tasks, page 17](#)
- [Obtaining Documentation, page 18](#)
- [Documentation Feedback, page 19](#)
- [Cisco Product Security Overview, page 19](#)
- [Product Alerts and Field Notices, page 20](#)
- [Obtaining Technical Assistance, page 21](#)
- [Obtaining Additional Publications and Information, page 22](#)



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

© 2006 Cisco Systems, Inc. All rights reserved.

Introduction

For Cisco Unified Presence Server 1.0, the installation process allows you to either perform a basic installation or to 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 Presence Server installation, which installs the software from the installation disc and does not use any imported data.
Apply Additional Release	This option allows you to upgrade the software version that the installation disc contains with the latest service release.

Related Documentation

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

- *Cisco Unified Presence Server Administration Guide*
The *Cisco Unified Presence Server Administration Guide* provides step-by-step instructions for configuring, maintaining, and administering the Cisco Unified Presence Server.
- *Cisco Unified Presence Server Deployment Guide*
This document provides an overview of the configuration process for Cisco Unified Presence Server and Cisco Unified CallManager, as well as information about integrating Cisco Unified Presence Server with Microsoft Live Communications Server, Microsoft Active Directory, and Microsoft Office Communicator.
- *Cisco Unified Presence Server Serviceability Administration Guide*
This document provides descriptions of Cisco Unified Presence Server serviceability, as well as 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 Presence Server data, and restore the data.
- *Cisco Unified Communications Operating System Administration Guide*
This document provides information about how to access and use the utilities that are available through the operating system GUI and the command line interface.

Important Considerations

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

- Ensure that the associated Cisco Unified CallManager server is running software Release 5.1(1) or later.

- For LCS integration, ensure that the associated Microsoft LCS Server is running LCS 5.
- Be aware that when you install Cisco Unified Presence Server on an existing server, the hard drive gets formatted, and all existing data on the drive gets overwritten.
- Install the Cisco Unified Presence Server software on the first node, or publisher, server first and then on the second node. You must configure the second node on the first node before you can install the second node.
- Make sure that the second node can connect to the first node server and to the Cisco Unified CallManager first node during the installation.
- Enter the same security password on all servers in the cluster.
- Install the Cisco Unified Presence Server software during off-peak hours or a maintenance window to avoid impact from call-processing interruptions.
- You must have access to a Secure File Transfer Protocol (SFTP) server to back up Cisco Unified Presence Server over a network.
- Carefully read the instructions that follow before you proceed with the installation

**Note**

For Cisco Unified Personal Communicator requirements, refer to the *Release Notes for Cisco Unified Personal Communicator* at the following URL:

http://www.cisco.com/en/US/products/ps6844/tsd_products_support_series_home.html

Frequently Asked Questions About the Cisco Unified Presence Server Installation

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

How long does it take to perform the Cisco Unified Presence Server installation?

The entire installation process, excluding pre- and post-installation tasks, takes 45 to 120 minutes per server, depending on your server type.

What Passwords do I Need to Specify?

During the Cisco Unified Presence Server 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:

- Operating System Administration
- Disaster Recovery System
- Command Line Interface

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

- Application User password

You use the Application User password to log in to the Cisco Unified Presence Server Administration GUI as CCMAAdministrator.

- AXL API user name and password

You use the AXL API user name and password to allow the proprietary SyncAgent mechanism on the Cisco Unified Presence Server first node to access database information on the Cisco Unified CallManager first node.

You must enter the username and password for the application user that has the Standard AXL API Access role assigned to it on the associated Cisco Unified CallManager first node. By default, the Standard AXL API Access role gets assigned to the CCMAAdministrator User ID.

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

For Cisco Unified Presence Server 1.0, you must do all software installations and upgrades by using the Software Upgrades menu options in Cisco Unified Communications Operating System Administration. The system can upload and process only software that Cisco Systems approved. You cannot install or use third-party or Windows-based software applications with Cisco Unified Presence Server 1.0.

Which servers does Cisco support for this installation?

To find which servers support Cisco Unified Presence Server releases, please refer to the *Cisco Unified Presence Server Hardware Compatibility Matrix for Release 1.0(3)* at

http://www.cisco.com/en/US/products/ps6837/products_device_support_tables_list.html

Browser Requirements

You can access Cisco Unified Presence Server Administration, Cisco Unified Presence Server Serviceability, and Cisco IPT Administration by using the following browsers:

- Microsoft Internet Explorer version 6.0 or later
- Netscape Navigator version 7.2 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 Presence Server application. See [Table 2](#) for the BIOS settings and [Table 3](#) for the RAID settings that are set up during installation.

Table 2 *BIOS Configuration Settings for HP and IBM Servers*

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

Table 3 *RAID Settings*

Cisco MCS 7825 (HP and IBM)	Cisco MCS 7835 (HP and IBM)	Cisco MCS 7845 (HP and IBM)
RAID not applicable	Logical drives: 1	Logical drives: 2
RAID not applicable	RAID type: 1(1+0)	RAID type: 1(1+0)
Note For the Cisco 7825H1 and the Cisco 7825I1, SATA RAID is enabled, and the RAID type is 1(1+0), with one logical drive.		



Note

If the hardware configuration process fails during installation, you can use boot-time utilities that are found on both the IBM and HP servers to manually configure the RAID and BIOS settings, as shown in [Table 2](#) and [Table 3](#).

Installation Overview

The following sections contain the procedures for installing the first and second nodes. Review these sections carefully before you perform the installation:

- [Performing Pre-Installation Tasks, page 6](#)
- [Gathering Information for an Installation, page 6](#)
- [Installing Cisco Unified Presence Server, page 12](#)
- [Performing Post-Installation Tasks, page 17](#)

Performing Pre-Installation Tasks

Perform the following tasks before you begin the installation:

	Pre-installation Task	Important Notes
Step 1	Before the installation, obtain the necessary information for configuring the Cisco Unified Presence Server on the first and second nodes (if applicable).	See Gathering Information for an Installation , page 6.
Step 2	Before installing Cisco Unified Presence Server, ensure that you have added the Cisco Unified Presence Server node as an application server on the Cisco Unified CallManager first node.	From the Cisco Unified CallManager Administration window, navigate to System > Application Server . For more information, see the <i>Cisco Unified CallManager Administration Guide</i> .
Step 3	Before installing Cisco Unified Presence Server, ensure that you activate the Cisco AXL Web Service on the associated Cisco Unified CallManager server.	From Cisco Unified CallManager Serviceability window, navigate to Tools > Service Activation . For more information, see the <i>Cisco Unified CallManager Serviceability Administration Guide</i> .
Step 4	Before installing Cisco Unified Presence Server, ensure that the server has network access to the Cisco Unified CallManager first node.	
Step 5	Before installing the Cisco Unified Presence Server second node, ensure that you have added the Cisco Unified Presence Server second node as an application server on the Cisco Unified CallManager first node and that you have also added the second node as a server on the Cisco Unified Presence Server first node.	From the Cisco Unified CallManager Administration window, navigate to System > Application Server . From the Cisco Unified Presence Server Administration window, navigate to System > Server . For more information, see the <i>Cisco Unified CallManager Administration Guide</i> and the <i>Cisco Unified Presence Server Administration Guide</i> .
Step 6	If you use DNS, ensure that you have configured the host name of the new server on the DNS server and that the DNS server can resolve the host name of the Cisco Unified CallManager first node and of the other Cisco Unified Presence Server node (if any).	

Gathering Information for an Installation

Use [Table 5](#) to record the information about your Cisco Unified Presence Server server. Gather this information for each server that you are installing in the cluster. You should make copies of this table and record your entries for each server in a separate table.

See [Table 5 on page 9](#) for definitions of these fields.



Note

Because some fields are optional, they may not be relevant to your configuration. For example, you may choose not to set up an SMTP host.

**Caution**

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

The last column in the table shows whether a field can be changed after installation, and if so, whether you can change it through operating system administration or through the Command Line Interface (CLI).

Table 4 Configuration Data

Configuration Data	Your Entry	Can Entry Be Changed After Installation
Administrator Login		No
Administrator Password		Yes CLI: set password admin
Application User Password		No
AXL User ID Enter the user name for the application user with AXL API access on the Cisco Unified CallManager first node, normally CCMAdministrator .		Yes GUI: Cisco Unified Presence Server > Security > AXL Configuration
AXL User Password Enter the password for the application user with AXL API access on the Cisco Unified CallManager first node.		Yes GUI: Cisco Unified Presence Server > Security > AXL Configuration
Cisco Unified CallManager Publisher Host Name		No
Cisco Unified CallManager Publisher IP Address		No
Cisco Unified CallManager Publisher Security Password Note You must enter the security password that is configured on the Cisco Unified CallManager first node.		No
Country		Yes CLI: set web-security
DHCP		Yes CLI: set network dhcp
DNS Primary		Yes CLI: set network dns

Table 4 Configuration Data (Continued)

Configuration Data	Your Entry	Can Entry Be Changed After Installation
DNS Secondary		Yes CLI: set network dns
Domain		Yes CLI: Set Network Domain
Domain Name Service DNS Enable		No
First Cisco Unified Presence Server Node Host Name Note You require this parameter only for the second node.		No
First Cisco Unified Presence Server Node IP Address Note You require this parameter only for the second node.		No
Gateway Address		Yes. Use Cisco Unified Communications Operating System Administration: Settings > IP or CLI: set network gateway
Host Name		No
IP Address		Yes Use Cisco Unified Communications Operating System Administration: Settings > IP or CLI: set network IP
IP Mask		Yes. Use Cisco Unified Communications Operating System Administration: Settings > IP or CLI: set IP

Table 4 Configuration Data (Continued)

Configuration Data	Your Entry	Can Entry Be Changed After Installation
Location		Yes CLI: set web-security
Master Administrator ID		No
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 5 Field Definitions

Field	Description	Usage
Administrator Login	This field specifies the name that you want to assign to this account.	Ensure the name is unique; it can contain lowercase, alphanumeric characters, hyphens, and underscores. It must start with a lowercase, alphanumeric character. For this mandatory field, you should record it for use when logging in to the CLI on the platform or into the Cisco IPT Platform Administration. Note You cannot change this field after installation.
Administrator Password	This field specifies the password for the Administrator account.	Use this password to log in to Cisco IPT Platform Administration, Disaster Recovery System, and the CLI.
Application User Password	This field specifies the password for Cisco Unified Presence Server administration.	Use this password to log in to the Cisco Unified Presence Server administration GUI.

Table 5 *Field Definitions (Continued)*

Field	Description	Usage
DHCP	Dynamic Host Configuration Protocol	Choose Yes if you want to use DHCP to automatically configure the network settings on your server. If you choose No, you must enter a hostname, IP Address, IP Mask, Gateway, and DNS configuration.
DNS Enabled	A Domain Name System (DNS) server represents a device that resolves a hostname into an IP address or an IP address into a hostname. The DNS fields only display when you are not using DHCP.	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 IP Telephony network. If you have a DNS server, Cisco recommends entering Yes to enable DNS. Disabling DNS limits the systems ability to resolve some domain names.
DNS Primary	Cisco Unified Presence Server contacts this DNS server first when attempting to resolve host names.	Enter the IP address of the DNS server that you want to specify as the primary DNS server. Enter the IP address in dotted decimal format as ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0). Consider this field mandatory if DNS is set to yes .
DNS Secondary	When a primary DNS server fails, Cisco Unified Presence Server will attempt to connect to the secondary DNS server.	In this optional field, enter the IP address of the secondary DNS. Enter the IP address in dotted decimal format as ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0).
Domain	This field represents the name of the domain in which this machine is located.	Consider this field mandatory if DNS is set to yes .
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 being able to communicate with devices only on your subnet.

Table 5 **Field Definitions (Continued)**

Field	Description	Usage
Host Name	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. No other machine in this network should 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)
SMTP Location	This field specifies the name of the SMTP host that is used for outbound e-mail.	Enter the hostname or dotted IP address for the SMTP server. For a host, it can contain alphanumeric characters, hyphens, or periods. For a host name, it must start with an alphanumeric character. You must fill in this field if you plan to use electronic notification. If not, you can leave it blank.
Time zone	This field reflects 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.

Selecting an Installation Option

After the software installation starts, you will get asked to select one of the options that [Table 6](#) lists.

Table 6 *Installation Options*

Installation Options	Description
Basic Install	This option represents the basic installation and does not use any imported data.
Apply Additional Release	This option allows you to upgrade the preinstall software with the latest service release prior to configuring your system. Note Ensure that you have the software image available on DVD or on a remote server prior to choosing this option.

Installing Cisco Unified Presence Server

Use this procedure to begin installing the Cisco Unified Presence Server application.

-
- Step 1** Insert the installation DVD into the tray and restart the server, so it boots from the DVD. After the server completes its boot sequence, the DVD Found window displays.
- Step 2** To perform a media check, choose **Yes**.
The Media Check window displays.
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.
After you choose **OK**, the system installer performs various hardware checks to ensure your system is correctly configured for Cisco Unified Presence Server, including the following checks:
- 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 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 software version, if any, on your hard drive and the version on the DVD. To continue with the installation, choose **Yes**, or choose **No** to cancel.

**Caution**

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

The Platform Installation Wizard window displays.

Step 5 To continue the installation, choose **Proceed**.

The CUPS Node Configuration window displays.

Step 6 To continue with the installation, choose **OK** on the CUPS Node Configuration window.

**Note**

Before proceeding with the installation, be sure that you have configured the Cisco Unified Presence Server on the Cisco Unified CallManager first node and that you have network access to the Cisco Unified CallManager server. See [Performing Pre-Installation Tasks](#) for more information.

The Apply Additional Release window displays.

Step 7 If you want to upgrade to a later release of the software during the installation process, choose **Yes** and continue with the [“Apply Additional Release”](#) section on page 13.

Step 8 If you want to install the software on the DVD without upgrading, choose **No**.

The Basic Install Window displays.

Step 9 Choose **Continue** and skip to the [“Basic Installation”](#) section on page 15.

Apply Additional Release

If you chose Apply Additional Release, 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.

The Install Upgrade Retrieval Mechanism Configuration window displays.

Step 10 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 14.
- **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 14.
- **LOCAL**—Retrieves the upgrade file from a local CD or DVD. Continue with the [“Upgrade from a Local Disc”](#) section on page 13.

Upgrade from a Local Disc**Note**

If you download an upgrade file from Cisco.com using Internet Explorer and have WinZip (or a similar zip utility) installed on your PC, the file extension gets changed from .gz.sgn to .gz.gz. To successfully install the upgrade, you must rename the file and change the extension back to .gz.sgn.

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
```

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



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

- Step 11** 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 12** The window displays the patch file that is available on the CD or DVD. To update the system with this patch, choose **Continue**.

The CUPS Node Configuration window displays. Continue with the [“Basic Installation” section on page 15](#).

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 13** The installation process allows you to automatically set the speed and duplex settings of the Ethernet network interface card (NIC) by using automatic negotiation.
- 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 14** 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 15** For network configuration, you can choose either to 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 15](#).
 - If you want to configure static IP addresses for the node, choose **No**.

The Static Network Configuration window displays.

- Step 16** If you chose not to use DHCP, enter your static network configuration values and choose **OK**. See [Table 5](#) for field descriptions.

The DNS Client Configuration window displays.

- Step 17** To enable DNS, choose **Yes**, enter your DNS client information, and choose **OK**. See [Table 5](#) for field descriptions.

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

Retrieving the Remote Patch

- Step 18** Enter the location and login information for the remote file server. After restarting the network, the system connects to the remote server and retrieves a list of available upgrade patches.

The Install Upgrade Patch Selection window displays.

- Step 19** Choose the upgrade patch that you want to install. The system downloads, unpacks, and installs the patch and then restarts the system.

The CUPS Node Configuration window displays. Basic Installation

To continue with the installation, choose **Yes** on the CUPS Node Configuration window. Continue with the [“Basic Installation” section on page 15](#).

Basic Installation



Tip Before proceeding with the installation, be sure that you have configured the Cisco Unified Presence Server on Cisco Unified CallManager first node and that you have network access to the Cisco Unified CallManager server.

- Step 20** When the Timezone Configuration window displays, choose the appropriate time zone for the server and then choose **OK**.

The Auto Negotiation Configuration window displays.

- Step 21** The installation process allows you to automatically set the speed and duplex settings of the Ethernet network interface card (NIC) by using automatic negotiation.

- 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 22** 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 23** If you want to use DHCP, choose **Yes** and skip to [“Configure the Administrator Login” section on page 16](#).

If you want to set up a static IP address for the server, choose **No**.

The Static Network Configuration window displays.

Configure Static Network Values and DNS

- Step 24** Enter your static network configuration values and choose **OK**. See [Table 5 on page 9](#) for field descriptions.

The DNS Client Configuration window displays.

Step 25 Choose **Yes**, enter your DNS client information, and choose **OK**. See [Table 5 on page 9](#) for field descriptions.

The Administrator Login Configuration window displays.

Configure the Administrator Login

Step 26 Enter your administrator login and password from [Table 4](#).

The CCM Publisher Connectivity window displays.

Step 27 Enter the Cisco Unified CallManager publisher hostname, IP address, and security password from [Table 4](#) and choose **OK** to continue.

After connectivity and version validation, the First CUPS Node Configuration window displays.

Step 28 Choose whether you are installing the first Cisco Unified Presence Server node in the cluster

- If you are installing the first Cisco Unified Presence Server node, choose **Yes**.
The Application User Password Configuration window displays. Continue with the [“Configuring the First Node” section on page 16](#).
- If you are installing the second Cisco Unified Presence Server node, choose **No**.
The CUPS Node Configuration window displays. Continue with the [“Configuring the Second Node” section on page 16](#).

Configuring the First Node

Step 29 Enter the Application User Password from [Table 4](#) and choose **OK**.

The AXL API Access Configuration window displays.

Step 30 Enter the AXL User ID and password from [Table 4](#).

The Certificate Information window displays.

Step 31 Enter your certificate information from [Table 4](#) and choose **OK**.

The SMTP Host Configuration window displays.

Step 32 If you want to configure an SMTP host, choose **Yes** and enter the SMTP location.



Note You must configure an SMTP server to use certain operating system features. However, you can also configure an SMTP server later by using the Cisco Unified Communications Operating System GUI or the command line interface.

The Platform Configuration Confirmation window displays.

Step 33 To start installing the software, choose **OK** or, if you want to change the configuration, choose **Back**.

Step 34 When the installation process completes, you get prompted to log in with the Administrator account and password.

Step 35 Complete the post-upgrade tasks that are listed in the [“Performing Post-Installation Tasks” section on page 17](#).

Configuring the Second Node

Step 36 When the CUPS Node Configuration displays, choose **OK** to continue.

**Caution**

Before proceeding with the installation, be sure that you have configured the second Cisco Unified Presence Server node on both the Cisco Unified Presence Server first node and on the associated Cisco Unified CallManager first node. The new node must also have network access to both the first Cisco Unified Presence Server node and the Cisco Unified CallManager first node.

The First CUPS Node Access Configuration window displays.

Step 37 Enter the host name and IP address for the first Cisco Unified Presence Server node.

The Certificate Information window displays.

Step 38 Enter your certificate information from [Table 5](#) and choose **OK**.

The SMTP Host Configuration window displays.

Step 39 If you want to configure an SMTP host, choose **Yes** and enter the SMTP location.

**Note**

You must configure an SMTP server to use certain operating system features. However, you can also configure an SMTP server later by using the Cisco Unified Communications Operating System GUI or the command line interface.

The Platform Configuration Confirmation window displays.

Step 40 To start installing the software, choose **OK** or, if you want to change the configuration, choose **Back**.

Step 41 When the installation process completes, you get prompted to log in with the Administrator account and password.

Step 42 Complete the post-upgrade tasks that are listed in the [“Performing Post-Installation Tasks”](#) section on [page 17](#).

Performing Post-Installation Tasks

After installing Cisco Unified Presence Server, you must set some configuration parameters and perform other post-installation tasks before you can begin using it. Perform these tasks for the first server that you install before you install the second Cisco Unified Presence Server node.

For post-installation tasks that you must complete after the installation, see [Table 7](#).

Table 7 Post-Installation Tasks

Post-Installation Tasks	Important Notes
Upload the Cisco Unified Presence Server license file.	From the Cisco Unified Presence Server Administration window, navigate to System > Licensing > License File Upload . For more information, see the <i>Cisco Unified Presence Server Administration Guide</i> .
Before installing a second Cisco Unified Presence Server node, ensure that you have added the Cisco Unified Presence Server node as an application server on the Cisco Unified CallManager first node.	From the Cisco Unified CallManager Administration window, navigate to System > Application Server . For more information, see the <i>Cisco Unified CallManager Administration Guide</i> .
Before installing a second Cisco Unified Presence Server node, ensure that you have added the Cisco Unified Presence Server node as a server on the first Cisco Unified Presence Server node.	From the Cisco Unified Presence Server Administration window, navigate to System > Server . For more information, see the <i>Cisco Unified Presence Server Administration Guide</i> .
Activate the required Cisco Unified Presence Server services, including <ul style="list-style-type: none"> • Cisco Enterprise SIP Proxy • Cisco Enterprise Presence Engine 	From the Cisco Unified Presence Server Serviceability window, navigate to Tools > Service Activation . For more information, see the <i>Cisco Unified Presence Server Administration Guide</i> and the <i>Cisco Unified Presence Server Serviceability Administration Guide</i> .
Configure the Cisco Unified CallManager Presence Gateways.	From the Cisco Unified Presence Server Administration window, navigate to Cisco Unified Presence Server > Presence Engine > CallManager Presence Gateways . For more information, see the <i>Cisco Unified Presence Server Administration Guide</i> .
Configure the backup settings. Remember to back up your Cisco Unified Presence Server data daily.	For more information, see the <i>Disaster Recovery System Administration Guide</i> .

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 Support site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

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

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 these announcements 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. Registered users can access the tool at this URL:

<http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

To register as a Cisco.com user, go to this URL:

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

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support 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 Support Website

The Cisco Support 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/en/US/support/index.html>

Access to all tools on the Cisco Support 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

Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get 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. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page 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 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, 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)

