



Installation Guide for Cisco Unity Connection

Release 2.x
Revised March 7, 2008

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-13434-05

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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. (0501R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Installation Guide for Cisco Unity Connection Release 2.x
© 2008 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface v

- Audience and Use v
- Documentation Conventions v
- Cisco Unity Connection Documentation vi
- Obtaining Documentation, Obtaining Support, and Security Guidelines vi
- Cisco Product Security Overview vi

CHAPTER 1

Overview of Mandatory Tasks for Installing a Cisco Unity Connection 2.x System 1-1

- Part 1: Installing and Configuring the Cisco Unity Connection Server 1-1
- Part 2: Setting Up Administrator Workstations 1-2
- Part 3: Setting Up the Phone System Integration 1-2
- Part 4: Populating the System with User and Call Management Data 1-2
- Part 5: Configuring the System for Features 1-5
- Part 6: Setting Up VPIM Networking 1-5
- Part 7: Setting Up User Workstations 1-6
- Part 8: Backing Up Cisco Unity Connection Data 1-6
- Part 9: Training 1-6

CHAPTER 2

Installing the Operating System and Cisco Unity Connection 2-1

- Pre-Installation Tasks 2-2
- Important Considerations 2-2
- Frequently Asked Questions About the Installation 2-3
 - How Much Time Does the Installation Require? 2-3
 - What User Names and Passwords do I Need to Specify? 2-3
 - What is a Strong Password? 2-4
 - Which Servers Does Cisco Support for this Installation? 2-5
 - May I Install Other Software on the Server? 2-5
- Browser Requirements 2-5
- Installing a Memory Upgrade (Selected Servers Only) 2-5
- Configuring the Hardware 2-8
- Verifying DNS Registration 2-8
- Gathering Information for an Installation 2-9

- Using the Cisco Unified Communications Answer File Generator **2-13**
- Handling Network Errors During Installation **2-13**
- Installing the New Operating System and Application **2-14**
 - Navigating Within the Installation Wizard **2-14**
 - Starting the Installation **2-14**
 - Entering Preexisting Configuration Information **2-16**
 - Performing the Basic Installation **2-16**
 - Configuring the Server **2-18**
- Post-Installation Tasks **2-19**
 - Changing the Default Application User Passwords **2-20**
 - Activating Services **2-20**
 - Examining Log Files **2-20**



Preface

This preface contains the following sections:

- [Audience and Use](#), page v
- [Documentation Conventions](#), page v
- [Cisco Unity Connection Documentation](#), page vi
- [Obtaining Documentation, Obtaining Support, and Security Guidelines](#), page vi
- [Cisco Product Security Overview](#), page vi

Audience and Use

The *Installation Guide for Cisco Unity Connection* is intended for installers of a Cisco Unity Connection system. If you are configuring access to Microsoft Exchange e-mail messages through text to speech or configuring access to Exchange calendars and contacts for use with personal call transfer rules, you need a working knowledge of Microsoft Exchange.

Documentation Conventions

Table 1 Conventions in the Installation Guide for Cisco Unity Connection

Convention	Description
boldfaced text	Boldfaced text is used for: <ul style="list-style-type: none">• Key and button names. (Example: Click OK.)• Information that you enter. (Example: Enter Administrator in the User Name box.)
< > (angle brackets)	Angle brackets are used around parameters for which you supply a value. (Example: In your browser, go to https://<Cisco Unity Connection server IP address>/cuadmin.)
- (hyphen)	Hyphens separate keys that must be pressed simultaneously. (Example: Press Ctrl-Alt-Delete .)
> (right angle bracket)	A right angle bracket is used to separate selections that you make in the navigation bar of Cisco Unity Connection Administration. (Example: In Cisco Unity Connection Administration, go to Contacts > System Contacts .)

The *Installation Guide for Cisco Unity Connection* also uses the following conventions:

**Note**

Means reader take note. Notes contain helpful suggestions or references to material not covered in the document.

**Caution**

Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Cisco Unity Connection Documentation

For descriptions and URLs of Cisco Unity Connection documentation on Cisco.com, see the *Documentation Guide for Cisco Unity Connection*. The document is shipped with Cisco Unity Connection and is available at

http://www.cisco.com/en/US/products/ps6509/products_documentation_roadmaps_list.html.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Cisco Product Security Overview

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

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



CHAPTER 1

Overview of Mandatory Tasks for Installing a Cisco Unity Connection 2.x System

Use the following high-level task list to install the Cisco Unity Connection 2.x system correctly. The tasks reference detailed instructions in the *Installation Guide for Cisco Unity Connection* and in other Cisco Unity Connection documentation as noted. Follow the documentation for a successful installation.

The task list leads you through the complete installation of the Cisco Unity Connection system—from installing and configuring the Connection server; to populating the Connection system with user and call management data; to setting up optional features, such as using IMAP clients to access voice messages; to backing up Connection data.

The list is divided into nine parts:

- [Part 1: Installing and Configuring the Cisco Unity Connection Server, page 1-1](#)
- [Part 2: Setting Up Administrator Workstations, page 1-2](#)
- [Part 3: Setting Up the Phone System Integration, page 1-2](#)
- [Part 4: Populating the System with User and Call Management Data, page 1-2](#)
- [Part 5: Configuring the System for Features, page 1-5](#)
- [Part 6: Setting Up VPIM Networking, page 1-5](#)
- [Part 7: Setting Up User Workstations, page 1-6](#)
- [Part 8: Backing Up Cisco Unity Connection Data, page 1-6](#)
- [Part 9: Training, page 1-6](#)

Some of the tasks apply only to specific situations, and are noted as such. If a task does not apply to your situation, skip it.

Part 1: Installing and Configuring the Cisco Unity Connection Server

Revised March 7, 2008

1. Verify the following requirements:
 - a. System requirements for the Cisco Unity Connection 2.x system. Refer to *System Requirements for Cisco Unity Connection Release 2.x* at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html.

- b. Requirements for integrating the phone system(s). See the “Requirements” section of the applicable Cisco Unity Connection integration guide(s) at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.
2. Download Connection languages (locales), if applicable, for the installation. Refer to *Release Notes for Cisco Unity Connection* at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.
3. Set up and configure the Cisco Unity Connection server. Refer to the “Installing the Operating System and Cisco Unity Connection” chapter of this guide.
4. Install Connection languages, if applicable. Refer to the “Software Upgrades” chapter of *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Part 2: Setting Up Administrator Workstations

5. Configure the browser(s) on administrator workstations to access Cisco Unity Connection web applications. Refer to the “Configuring the Browser on an Administrator Workstation” chapter of the *System Administration Guide for Cisco Unity Connection* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.
6. Download and install the Real-Time Monitoring Tool software. Refer to the “Installing and Configuring Real-Time Monitoring Tool” chapter of the *Real-Time Monitoring Tool Administration Guide for Cisco Unity Connection* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Part 3: Setting Up the Phone System Integration

7. Set up the integration between Cisco Unity Connection and the phone system(s). See the applicable Cisco Unity Connection integration guide(s) at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.
8. Store all of the software that was shipped with Cisco Unity Connection together in a location that is safe and can be readily accessed.

Part 4: Populating the System with User and Call Management Data

You do many of the tasks in Part 4 by using Cisco Unity Connection Administration. (For information on logging on to Connection Administration and on using it, refer to the “Accessing and Using Cisco Unity Connection Administration” chapter of the *System Administration Guide for Cisco Unity Connection*.)

The tasks in Part 4 reference chapters in the following guides, as noted:

- *System Administration Guide for Cisco Unity Connection*
- *User Moves, Adds, and Changes Guide for Cisco Unity Connection*

Both guides are available at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

9. Obtain and install Connection licenses. See the “Managing Licenses” chapter of the *System Administration Guide*.
10. Familiarize yourself with the following Cisco Unity Connection concepts:
 - a. Call management. See the “Call Management Overview” and “Creating a Call Management Plan” chapters of the *System Administration Guide*.
 - b. User, administrator accounts, templates, class of service, and roles. See the “Introduction to Cisco Unity Connection Users and Contacts” and “Preparing to Add User Accounts” chapters of the *User Moves, Adds, and Changes Guide*.
11. Develop a system plan:
 - a. Identify business and nonbusiness hours, and holidays. See the “Managing Schedules and Holidays” chapter of the *System Administration Guide*.
 - b. Map out a call management plan. See the “Creating a Call Management Plan” chapter of the *System Administration Guide*.
 - c. Review the default restriction tables, and determine whether changes or new tables are needed. See the “Overview: Default Restriction Tables” section in the “Managing Restriction Tables” chapter of the *System Administration Guide*.
 - d. Determine password and account lockout policies for phone and web-tool access, and the logon policy for web-tool access. See the “Specifying Password, Logon, and Lockout Policies” chapter of the *System Administration Guide*.
 - e. Determine the number and types of administrator accounts that you need, and the roles to assign to the accounts. See the “Preparing to Add User Accounts” chapter of the *User Moves, Adds, and Changes Guide*.
 - f. Determine the features that you will enable for users, and whether changes or new templates and COSes are needed. See the “Preparing to Add User Accounts” chapter of the *User Moves, Adds, and Changes Guide*.
 - g. Review the default message store quotas, and determine whether changes are needed. See the “Specifying Mailbox Size Quotas” chapter of the *System Administration Guide*.
 - h. Review the default message aging policy, and determine whether changes are needed. See the “Changing the Message Aging Policy” chapter of the *System Administration Guide*.
 - i. Review the default system distribution lists, and determine whether changes or new distribution lists are needed. See the “Managing System Distribution Lists” chapter of the *System Administration Guide*.
12. For the following defaults that you reviewed in Task 11., make changes or create new ones, as applicable:
 - a. Schedules. See the “Managing Schedules and Holidays” chapter of the *System Administration Guide*.
 - b. Restriction tables. See the “Managing Restriction Tables” chapter of the *System Administration Guide*.
 - c. Password, lockout, and logon policies. See the “Specifying Password, Logon, and Lockout Policies” chapter of the *System Administration Guide*.
 - d. Classes of service. See the “Adding, Modifying, or Deleting a Class of Service” chapter of the *User Moves, Adds, and Changes Guide*.

- e. User templates. See the “Adding, Modifying, or Deleting a User Template” chapter of the *User Moves, Adds, and Changes Guide*.
 - f. Message aging policy. See the “Changing the Message Aging Policy” chapter of the *System Administration Guide*.
 - g. System distribution lists. See the “Managing System Distribution Lists” chapter of the *System Administration Guide*.
13. Test the system configuration:
 - a. Add a Connection user account to use as a test account. See the “Adding Cisco Unity Connection User Accounts Individually” chapter of the *User Moves, Adds, and Changes Guide*.
 - b. Use the phone to log on to Cisco Unity Connection as the test user, record a name, and set a phone password. Hang up.
 - c. Call Cisco Unity Connection and log on as the test user again to confirm that the password, greeting, and conversation version specified for the user are working properly. Confirm that the user inherited the correct class of service by testing any applicable features by phone.
 - d. Log on to the Cisco Personal Communications Assistant (PCA) as the test user. If you gave the test user the required COS rights, confirm that you can browse from the Cisco PCA Home page to the applicable web tools.
 - e. Make corrections to the system configuration as necessary.
 14. Create administrator accounts. See the “Adding Cisco Unity Connection User Accounts Individually” chapter of the *User Moves, Adds, and Changes Guide*.
 15. Create user accounts. See the “Adding Cisco Unity Connection User Accounts Individually,” “Managing User Accounts in Bulk,” or “Creating Multiple User Accounts from Cisco Unified Communications Manager Users” chapter of the *User Moves, Adds, and Changes Guide*, as applicable.
 16. Customize individual user account settings to offer additional features and functionality, as needed. See the “Setting Up Features and Functionality That Are Controlled by User Account Settings” and “Setting Up Features and Functionality That Are Controlled by Class of Service” chapters of the *User Moves, Adds, and Changes Guide*.
 17. Add individual users to system distribution lists, as needed. See the “Managing System Distribution List Members” section in the “Managing System Distribution Lists” chapter of the *System Administration Guide*.
 18. Implement, then test the call management plan you created in Task 11.b.:
 - a. Create call handlers. See the “Managing Call Handlers” chapter of the *System Administration Guide*.
 - b. Specify directory handler settings. See the “Managing Directory Handlers” chapter of the *System Administration Guide*.
 - c. Create interview handlers. See the “Managing Interview Handlers” chapter of the *System Administration Guide*.
 - d. Set up call routing. See the “Managing Call Routing Tables” chapter of the *System Administration Guide*.

Part 5: Configuring the System for Features

19. *If any users will have access to the Cisco Unity web tools or will use an IMAP e-mail client to access Connection voice messages:* Secure Cisco Personal Communications Assistant (PCA) and IMAP access to Connection. See the “Securing Cisco PCA and IMAP E-Mail Client Access to Cisco Unity Connection” chapter of the *System Administration Guide*.
20. *If any users will have access to Cisco Unified MeetingPlace Express:* Confirm that you have configured the integration with Cisco Unified MeetingPlace Express. See the “Integrating with Cisco Unified MeetingPlace Express” chapter of the *System Administration Guide*.
21. *If users will have access to their Exchange e-mail by using text to speech (TTS):* Confirm that you have configured access to Exchange e-mail for use with TTS. See the “Configuring Access to Exchange E-Mails Through TTS” chapter of the *System Administration Guide*.
22. *If users will be allowed to base Personal Call Transfer Rules on Exchange calendar and contact information:* Confirm that you have configured access to Exchange calendars and contacts. See the “Configuring Access to Exchange Calendars and Contacts for Personal Call Transfer Rules” chapter of the *System Administration Guide*.
23. *If users will be using SMTP message notification devices:* Confirm that you have set up and enabled message notification for users. See the “Setting Up SMTP Message Notifications” chapter of the *System Administration Guide*.
24. *If any users will have access to Cisco Unity Connection Phone View:* Confirm that you have configured Cisco Unified Communications Manager for Phone View and that you have enabled Phone View for the phone system in Cisco Unity Connection Administration. See the “Setting Up Phone View” chapter of the *System Administration Guide*.
25. *If any users will have access to Cisco Unified Personal Communicator:* Confirm that you have configured the applicable servers, and set up the client applications. See the “Access to Voice Messages from the Cisco Unified Personal Communicator” section in the “Setting Up Features and Functionality That Are Controlled by Class of Service” chapter of the *User Moves, Adds, and Changes Guide*.
26. *If any administrators and/or users will have access to Cisco Unity Connection Broadcast Administrator:* Confirm that you have set it up. See the “Setting Up Broadcast Messaging” chapter of the *System Administration Guide*.
27. *If any administrators and/or users will need access to Cisco Unity Connection Greetings Administrator to manage greetings over the phone:* Set it up. See the “Setting Up the Cisco Unity Greetings Administrator” section in the “Managing Recorded Greetings and Recorded Names” chapter of the *System Administration Guide*.

Part 6: Setting Up VPIM Networking

28. *If users will be sending messages to remote voice messaging systems by VPIM Networking:* Set up VPIM Networking. See the “Using VPIM Networking” chapter of the *System Administration Guide*.

Part 7: Setting Up User Workstations

The tasks in Part 7 reference chapters in the *User Workstation Setup Guide for Cisco Unity Connection* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

29. Set up access to the Cisco PCA. See the “Setting Up Access to the Cisco Personal Communications Assistant” chapter.
30. Set up Media Master playback and recording devices. See the “Setting Up Playback and Recording Devices for the Media Master” chapter.
31. Configure IMAP e-mail accounts to access Connection voice messages. See the “Configuring an E-Mail Account to Access Cisco Unity Connection Voice Messages” chapter.
32. Confirm that users are able to access and use the Connection features that have been enabled for them.

Part 8: Backing Up Cisco Unity Connection Data

33. Refer to the *Disaster Recovery System Administration Guide for Cisco Unity Connection* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.



Note Third-party backup applications are not supported.

Part 9: Training

34. Train users, operators, and support desk personnel to use the Cisco Unity Connection system. See the “User Orientation” and “Operator and Support Desk Orientation” chapters of the *User Workstation User Setup Guide*.



CHAPTER 2

Installing the Operating System and Cisco Unity Connection

This document contains the following topics:

- [Pre-Installation Tasks, page 2-2](#)
- [Important Considerations, page 2-2](#)
- [Frequently Asked Questions About the Installation, page 2-3](#)
 - [How Much Time Does the Installation Require?, page 2-3](#)
 - [What User Names and Passwords do I Need to Specify?, page 2-3](#)
 - [What is a Strong Password?, page 2-4](#)
 - [Which Servers Does Cisco Support for this Installation?, page 2-5](#)
 - [May I Install Other Software on the Server?, page 2-5](#)
- [Browser Requirements, page 2-5](#)
- [Installing a Memory Upgrade \(Selected Servers Only\), page 2-5](#)
- [Configuring the Hardware, page 2-8](#)
- [Verifying DNS Registration, page 2-8](#)
- [Gathering Information for an Installation, page 2-9](#)
- [Using the Cisco Unified Communications Answer File Generator, page 2-13](#)
- [Handling Network Errors During Installation, page 2-13](#)
- [Installing the New Operating System and Application, page 2-14](#)
 - [Navigating Within the Installation Wizard, page 2-14](#)
 - [Starting the Installation, page 2-14](#)
 - [Entering Preexisting Configuration Information, page 2-16](#)
 - [Performing the Basic Installation, page 2-16](#)
 - [Configuring the Server, page 2-18](#)
- [Post-Installation Tasks, page 2-19](#)
 - [Changing the Default Application User Passwords, page 2-20](#)
 - [Activating Services, page 2-20](#)
 - [Examining Log Files, page 2-20](#)

Pre-Installation Tasks

Revised January 7, 2008

Table 2-1 contains a list of pre-installation tasks that you need to perform to ensure that you can successfully install Cisco Unity Connection.

Table 2-1 Pre-Installation Tasks

	Task	Important Notes
Step 1	Read this entire document to familiarize yourself with the installation procedure.	
Step 2	Verify the integrity of any new server hardware (such as hard drives and memory) by running any manufacturer-provided utilities.	
Step 3	Ensure that your servers are listed as supported hardware and sized appropriately to support the load of the cluster.	For information about the capacity of server models, see <i>Cisco Unity Connection Supported Platforms List</i> at http://www.cisco.com/en/US/products/ps6509/products_data_sheets_list.html . Make sure to account for any growth that has occurred since initial system configuration.
Step 4	Record the network interface card (NIC) speed and duplex settings of the switch port to which you will connect the new server. You should configure the same NIC settings on the server and on the switch port. For GigE (1000/FULL), you should set NIC and switch port settings to Auto/Auto; do not set hard values.	If you are using Network Fault Tolerance, the Network Fault Tolerance configuration gets lost during the replacement. You will need to configure it on each server after the upgrade. Enable PortFast on all switch ports that are connected to Cisco servers. With Portfast enabled, the switch immediately brings a port from the blocking state into the forwarding state by eliminating the forwarding delay [the amount of time that a port waits before changing from its Spanning-Tree Protocol (STP) learning and listening states to the forwarding state].
Step 5	If you use DNS, verify that all servers on which you plan to install Cisco Unity Connection are properly registered in DNS.	For more information, see the “ Verifying DNS Registration ” section on page 2-8.
Step 6	Record the configurations settings for each server that you plan to install.	To record your configuration settings, see Table 4 .

Important Considerations

Revised January 7, 2008

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

- Be aware that when you install on an existing server, the hard drive gets formatted, and all existing data on the drive gets overwritten.
- Ensure that you connect the server to an uninterruptible power supply (UPS) to provide backup power and protect your system. Failure to do so may result in damage to physical media and require a new installation.

- Install the Cisco Unified Communications Manager software on the first node or publisher server first and then on the subsequent nodes.
- Make sure that the subsequent node servers that you are installing can connect to the first node server during the installation.
- When you enter the Security password on the first node, be sure that you write it down and save it. You must enter the same password on each subsequent node that you install in the cluster. Install the software during off-peak hours or a maintenance window to avoid impact from interruptions.
- Configure the server by using static IP addressing to ensure that the server obtains a fixed IP address.
- Do not attempt to perform any configuration tasks during the installation.
- Do not install any Cisco-verified applications until you complete the installation.
- Be aware that directory names and filenames that you enter while you are running the installation program are case-sensitive.
- Carefully read the information that follows before you proceed with the installation.

Frequently Asked Questions About the Installation

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

How Much Time Does the Installation Require?

Added January 7, 2008

The entire installation process, excluding pre- and post-installation tasks, takes 45 to 90 minutes, depending on your server type.

What User Names and Passwords do I Need to Specify?

Revised January 7, 2008



Note

The system checks your passwords for strength. For guidelines on creating a strong passwords, see the [“What is a Strong Password?”](#) section on page 2-4.

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

- Administrator Account user name and password
- Application User name and password
- Security password

Administrator Account User Name and Password

You use the Administrator Account user name and password to log in to the following areas:

- Cisco Unified Communications Operating System Administration
- Disaster Recovery System
- Command Line Interface

To specify the Administrator Account user name and password, follow these guidelines:

- Administrator Account user name—The Administrator Account user name must start with an alphabetic character and can contain alphanumeric characters, hyphens and underscores.
- Administrator Account password—The Administrator Account password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

You can change the Administrator Account 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 Name and Password

You use the Application User name and password to access applications that are installed on the system, including the following areas:

- Cisco Unified Serviceability
- Real-Time Monitoring Tool

To specify the Application User name and password, follow these guidelines:

- Application User name—The Application User name must start with an alphabetic character and can contain alphanumeric characters, hyphens and underscores.
- Application User password—The Application User password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

You can change the Application User name and password by using the command line interface. For more information, see the *Cisco Unified Communications Operating System Administration Guide*.

Security Password

The Security password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

What is a Strong Password?

Added January 7, 2008

The installation wizard checks to ensure that you enter a strong password. To create a strong password, follow these recommendations:

- Mix uppercase and lowercase letters.
- Mix letters and numbers.
- Include hyphens and underscores.
- Remember that longer passwords are stronger and more secure than shorter ones.

Avoid the following types of passwords:

- Do not use recognizable words, such as proper names and dictionary words, even when combined with numbers.
- Do not invert recognizable words.
- Do not use word or number patterns, like aaabbb, qwerty, zyxwvuts, 123321, and so on.
- Do not use recognizable words from other languages.
- Do not use personal information of any kind, including birthdays, postal codes, names of children or pets, and so on.

Which Servers Does Cisco Support for this Installation?

For information about supported servers, see *Cisco Unity Connection Supported Platforms List* at http://www.cisco.com/en/US/products/ps6509/products_data_sheets_list.html.

May I Install Other Software on the Server?

You must do all software installations and upgrades by using Cisco Unified Communications Operating System Administration. The system can upload and process only software that Cisco Systems approved. You cannot install or use unapproved third-party or Windows-based software applications.

Browser Requirements

You can access Cisco Unified Serviceability, Cisco Unified Communications Operating System Administration, and Disaster Recovery System by using the following browsers:

- Microsoft Internet Explorer version 6.x or version 7.x
- Netscape Navigator version 7.1 or later

You can access Cisco Unity Connection Administration and Cisco Unity Connection Serviceability by using the following browsers:

Operating System on the Remote Workstation	Supported Browsers
Windows XP, Windows 2003, or Windows 2000	<ul style="list-style-type: none"> • Internet Explorer 6.0 and 7.0 • Firefox 1.5 and Firefox 2.0
RedHat Linux Enterprise	<ul style="list-style-type: none"> • Firefox 1.5 and Firefox 2.0

Cisco does not support or test other browsers.

Installing a Memory Upgrade (Selected Servers Only)

Added January 7, 2008



Note

If you are installing a server that does not require a memory upgrade, skip this section.

Some servers that are qualified for use with Cisco Unity Connection require a memory upgrade. Refer to the applicable table in the *Cisco Unity Connection Support Platforms List* at http://www.cisco.com/en/US/products/ps6509/products_data_sheets_list.html for memory information:

- Platform Overlays: Current Cisco, IBM, and HP Servers Without the Cisco Unity Connection 2.x Operating System
- Supported Traditional Cisco, IBM, and HP Servers



Warning

Before working on a system that has an on/off switch, turn OFF the power and unplug the power cord.
Statement 1

**Warning**

Before opening the chassis, disconnect the telephone-network cables to avoid contact with telephone-network voltages. Statement 2

**Warning**

This equipment is to be installed and maintained by service personnel only as defined by AS/NZS 3260 Clause 1.2.14.3 Service Personnel. Statement 88

**Warning**

During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself. Statement 94

**Warning**

The safety cover is an integral part of the product. Do not operate the unit without the safety cover installed. Operating the unit without the cover in place will invalidate the safety approvals and pose a risk of fire and electrical hazards. Statement 117

**Warning**

Do not work on the system or connect or disconnect cables during periods of lightning activity. Statement 1001

**Warning**

Read the installation instructions before connecting the system to the power source. Statement 1004

**Warning**

To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

- **This unit should be mounted at the bottom of the rack if it is the only unit in the rack.**
- **When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.**
- **If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.** Statement 1006

**Warning**

There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions. Statement 1015

**Warning**

This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security. Statement 1017

**Warning**

To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables. Statement 1021


Warning

To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord. Statement 1023


Warning

This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available. Statement 1024


Warning

Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.
Statement 1029


Warning

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.
Statement 1030


Warning

Ultimate disposal of this product should be handled according to all national laws and regulations.
Statement 1040

To Install a Memory Upgrade (Selected Servers Only)

Step 1 Remove the cover.

Step 2 Install the memory modules in the applicable slots or locations, depending on the server model:

Server	Number and type of DIMMs to install	DIMM slots occupied by memory modules after you have installed the additional modules
MCS 7835-H1 and equivalents	2 PC2-3200	DIMM slots 1A, 2A, 3B, and 4B
MCS 7835-I1 and equivalents	2 PC2-3200	DIMM slots 1, 2, 3, and 4
MCS 7835-H2 and equivalents	2 PC2-5300	DIMM slots 1, 4, 7, and 10
MCS 7835-I2 and equivalents	2 PC2-5300	DIMM slots 1A, 3A, 5B, and 7B


Caution

If you install new memory modules in the wrong slots, the server and operating system may not recognize that they have been installed, and Cisco Unity Connection performance may suffer.

Step 3 Reattach the cover.

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 for Cisco Unity Connection. See [Table 2](#) for the BIOS settings and [Table 3](#) for the RAID settings that are set up during installation.



Note

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

Table 2 BIOS Configuration Settings for HP and IBM Servers

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

Table 3 RAID Settings

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

Verifying DNS Registration

Added January 7, 2008

If you use DNS, verify that all servers to be added are registered in DNS properly by performing the following actions:

Procedure

-
- Step 1** Open a command prompt.
 - Step 2** To ping each server by its DNS name, enter **ping** *DNS_name*.
 - Step 3** To look up each server by IP address, enter **nslookup** *IP_address*.
-

Gathering Information for an Installation

Revised January 7, 2008

Use [Table 4](#) to record the information about your server. You may not need to obtain all the information; gather only the information that is pertinent to your system and network configuration.



Note

Because some of the fields are optional, they may not apply to your configuration. For example, if you choose not to set up an SMTP host during installation, the parameter still displays, but you do not need to enter a value.



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 you can change a field after installation, and if you can, it provides the appropriate Command Line Interface (CLI) command.

Table 4 Configuration Data

Parameter	Description	Can Entry Be Changed After Installation?
Administrator ID Your entry:	This field specifies the administrator account user ID that you use for secure shell access to the CLI, for logging into Cisco Unified Communications Operating System Administration and for logging into the Disaster Recovery System.	No, you cannot change the entry after installation. Note After installation, you can create additional administrator accounts, but you cannot change the original administrator account user ID.
Administrator Password Your entry:	This field specifies the password for the Administrator account, which you use for secure shell access to the CLI, for logging into Cisco Unified Communications Operating System Administration and for logging into the Disaster Recovery System. Ensure the password is at least six characters long; it can contain alphanumeric characters, hyphens, and underscore.	Yes, you can change the entry after installation by using the following CLI command: CLI > set password admin
Application User Name Your entry:	You use the Application User name as the default password for applications that are installed on the system, for example, Cisco Unity Connection Administration and Cisco Unity Connection Serviceability.	Yes, you can change the entry after installation by using the following CLI command: CLI > utils reset_ui_administrator_name
Application User Password Your entry:	You use the Application User password as the default password for applications that are installed on the system, for example, Cisco Unity Connection Administration and Cisco Unity Connection Serviceability.	Yes, you can change the entry after installation by using the following CLI command: CLI > utils reset_ui_administrator_password

Table 4 Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
Country Your entry:	From the list, choose the appropriate country for your installation. Note The value you enter gets used to generate a Certificate Signing Request (CSR).	Yes, you can change the entry after installation by using the following CLI command: CLI > set web-security
DHCP Your entry:	If you want to use DHCP to automatically configure the network settings on your server, choose Yes . If you choose Yes , you do not get prompted for DNS or static configuration settings. If you choose No , you must enter a hostname, IP Address, IP Mask, and Gateway.	Yes, you can change the entry after installation by using the following CLI command: CLI > set network dhcp
DNS Enable Your entry:	A DNS server resolves a hostname into an IP address or an IP address into a hostname. If you do not have a DNS server, enter No . If you have a DNS server, Cisco recommends that you enter Yes to enable DNS. Note When DNS is not enabled, you should only enter IP addresses (not host names) for all network devices.	Yes, you can change the entry after installation by using the following CLI command: CLI > set network dns
DNS Primary Your entry:	Enter the IP address of the DNS server that you want to specify as the primary DNS server. Enter the IP address in dotted decimal format as ddd.ddd.ddd.ddd. Consider this field mandatory if DNS is set to yes (DNS enabled).	Yes, you can change the entry after installation by using the following CLI command: CLI > set network dns
DNS Secondary (optional) Your entry:	Enter the IP address of the DNS server that you want to specify as the optional secondary DNS server.	Yes, you can change the entry after installation by using the following CLI command: CLI > set network dns
Domain Your entry:	This field represents the name of the domain in which this machine is located. Consider this field mandatory if DNS is set to yes .	Yes, you can change the entry after installation by using the following CLI command: CLI > set network domain

Table 4 Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
Gateway Address Your entry:	Enter the IP address of the network gateway. If you do not have a gateway, you must still set this field to 255.255.255.255. Not having a gateway may limit you to only being able to communicate with devices on your subnet. If DHCP is set to No , consider this field mandatory.	Yes, you can change the entry after installation by using the following CLI command: CLI > set network gateway
Hostname Your entry:	Enter a host name that is unique to your server. The host name can comprise up to 64 characters and can contain alphanumeric characters and hyphens. If DHCP is set to No , consider this field mandatory.	No, you cannot change the entry after installation.
IP Address Your entry:	Enter the IP address of your server. If DHCP is set to No , consider this field mandatory.	Yes, you can change the entry after installation by using the following CLI command: CLI > set network IP
IP Mask Your entry:	Enter the IP subnet mask of this machine. If DHCP is set to No , consider this field mandatory.	Yes, you can change the entry after installation by using the following CLI command: CLI > set network ip eth0
Location Your entry:	Choose the appropriate location for the server. Note The value you enter gets used to generate a Certificate Signing Request (CSR).	Yes, you can change the entry after installation by using the following CLI command: CLI > set web-security
MTU Size Your entry:	The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host will transmit on the network. Enter the MTU size in bytes for your network. If you are unsure of the MTU setting for your network, use the default value. Default: 1500 bytes	Yes, you can change the entry after installation by using the following CLI command: CLI > set network mtu
NIC Duplex Your entry:	Choose the duplex mode for the network interface card (NIC), either Full or Half. Note This parameter only displays when you choose not to use Automatic Negotiation.	Yes, you can change the entry after installation by using the following CLI command: CLI > set network nic

Table 4 Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
NIC Speed Your entry:	Choose the speed for the NIC, either 10 megabits per second or 100 megabits per second. Note This parameter only displays when you choose not to use Automatic Negotiation.	Yes, you can change the entry after installation by using the following CLI command: CLI > set network nic
NTP Server Your entry:	Enter the hostname or IP address of one or more network time protocol (NTP) servers with which you want to synchronize. Note You can enter up to five NTP servers.	Yes, you can change the entry after installation by using the following CLI command: CLI > utils ntp config
Organization Your entry:	Enter the name of your organization. Note The value you enter gets used to generate a Certificate Signing Request (CSR).	Yes, you can change the entry after installation by using the following CLI command: CLI > set web-security
Security Password Your entry:	The password must contain at least six alphanumeric characters. It can contain hyphens and underscores, but it must start with an alphanumeric character. Note Save this password.	Yes, you can change the entry after installation by using the following CLI command: CLI > set password security
SMTP Location Your entry:	Enter the hostname or IP address for the SMTP server that is used for outbound e-mail. The hostname can contain alphanumeric characters, hyphens, or periods, but it must start with an alphanumeric character. Note You must fill in this field if you plan to use electronic notification.	Yes, you can change the entry after installation by using the following CLI command: CLI > set smtp
State Your entry:	Enter the state where the server is located. Note The value you enter gets used to generate a Certificate Signing Request (CSR).	Yes, you can change the entry after installation by using the following CLI command: CLI > set web-security
Time Zone Your entry:	This field specifies the local time zone and offset from Greenwich Mean Time (GMT). Choose the time zone that most closely matches the location of your machine.	Yes, you can change the entry after installation by using the following CLI command: CLI > set timezone
Unit Your entry:	Enter your unit. Note The value you enter gets used to generate a Certificate Signing Request (CSR).	Yes, you can change the entry after installation by using the following CLI command: CLI > set password admin

Using the Cisco Unified Communications Answer File Generator

Revised January 7, 2008

Cisco Unified Communications Answer File Generator, a web application, generates answer files for unattended installations of Cisco Unity Connection. Individual answer files get copied to a USB key or a floppy diskette and are used in addition to the Cisco Unity Connection DVD during the installation process.

The web application supports the following features:

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

The following usage requirements apply:

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

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

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

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



Note

If you are using a USB key to perform an unattended installation, Cisco recommends that you use USB keys that are preformatted to be compatible with Linux 2.4. These keys will have a W95 FAT32 format.

Handling Network Errors During Installation

Revised January 7, 2008

During the installation process, the installation program verifies that the server can successfully connect to the network by using the network configuration that you enter. If it cannot connect, a message displays, and you get prompted to select one of the following options:

- **RETRY**—The installation program tries to validate networking again. If validation fails again, the error dialog box displays again.
- **REVIEW (Check Install)**—This option allows you to review and modify the networking configuration. When detected, the installation program returns to the network configuration windows.

Networking gets validated after you complete each networking window, so the message might display multiple times.

- **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. If you choose to ignore network errors, the installation may fail.

Installing the New Operating System and Application

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

- [Navigating Within the Installation Wizard, page 2-14](#)
- [Starting the Installation, page 2-14](#)
- [Entering Preexisting Configuration Information, page 2-16](#)
- [Performing the Basic Installation, page 2-16](#)
- [Configuring the Server, page 2-18](#)

Navigating Within the Installation Wizard

For instructions on how to navigate within the installation wizard, see [Table 5](#).

Table 5 *Installation Wizard Navigation*

To Do This	Press This
Move to the next field	Tab
Move to the previous field	Alt-Tab
Choose an option	Space bar or Enter
Scroll up or down in a list	Up or down arrow
Go to the previous window	Space bar or Enter to choose Back (when available)
Get help information on a window	Space bar or Enter to choose Help (when available)

Starting the Installation

Revised January 7, 2008

To start the installation, follow this procedure.



Note

If you have a new server with the Cisco Unity Connection software preinstalled, you do not need to install from a DVD, unless you want to reimage the server with a later product release. You can go directly to the [“Entering Preexisting Configuration Information” procedure on page 2-16](#).

Procedure

- Step 1** If you have a USB key with configuration information that the Answer File Generator generated, insert it now.
- Step 2** Insert the installation DVD into the tray and restart the server, so it boots from the DVD. After the server completes the boot sequence, the DVD Found window displays.
- Step 3** To perform the media check, choose **Yes** or, to skip the media check, choose **No**.

The media check checks the integrity of the DVD. If your DVD passed the media check previously, you might choose to skip the media check.

- Step 4** If you choose **Yes** to perform the media check, the Media Check Result window displays. Perform these tasks:
- 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 DVD directly from Cisco.

- Step 5** The system installer performs the following hardware checks to ensure that your system is correctly configured. If the installer makes any changes to your hardware configuration settings, you will get prompted to restart your system. Leave the DVD in the drive during the reboot:

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

No hard drives have been found. You probably need to manually choose device drivers for install to succeed. Would you like to select drivers now?

To continue the installation, choose **Yes**.

- The installation next checks to see whether you have a supported hardware platform. If your server does not meet the exact hardware requirements, the installation process fails with a critical error. If you think this is not correct, capture the error and report it Cisco support.
- The installation process next verifies RAID configuration and BIOS settings.



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

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

- Step 6** In the Product Deployment Selection window, select the product to install; then, choose **OK**.



Note If one or more products are not supported on your server, that information also appears. If Cisco Unity Connection is listed as not supported on your server, confirm that the server meets Connection 2.x specifications, particularly regarding memory and processor speed. Refer to the applicable table for your server model in the “Cisco Unity Connection Supported Servers” section of the *Cisco Unity Connection Supported Platforms List* at http://www.cisco.com/en/US/products/ps6509/products_data_sheets_list.html. (If a memory upgrade is required, see the “Installing a Memory Upgrade (Selected Servers Only)” section on page 2-5 before you start the installation again.)

- Step 7** If software is currently installed on the server, the Overwrite Hard Drive window opens and displays the current software version on your hard drive and the version on the DVD. Choose **Yes** to continue with the installation or **No** to cancel.



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

The Platform Installation Wizard window displays.

- Step 8** Choose the applicable option:
- If Cisco Unity Connection software is already installed on the server, click **Skip**, and continue with the “Entering Preexisting Configuration Information” section on page 2-16.

- If you want to perform a standard installation, click **Proceed**, and continue with this procedure.
- If you want to perform an unattended installation, click **Skip**, and continue with the [“Entering Preexisting Configuration Information”](#) section on page 2-16. For an unattended installation, you provide preexisting configuration information on a USB key or floppy disk.
- If you want to install the software now and configure it later, click **Skip**, and continue with the [“Entering Preexisting Configuration Information”](#) section on page 2-16. This installation method may take more time than other methods.

Step 9 In the Basic Install window, choose **Continue** to install the software version on the DVD or configure the preinstalled software. Continue with the [“Performing the Basic Installation”](#) section on page 2-16.

Entering Preexisting Configuration Information

Revised January 7, 2008

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

Procedure

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



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

The Platform Installation Wizard window displays.

- Step 3** To continue with the Platform Installation Wizard, choose **Proceed**.
- Step 4** In the Basic Install window, choose **Continue**. Continue with the [“Performing the Basic Installation”](#) section on page 2-16.
-

Performing the Basic Installation

Revised January 7, 2008

Procedure

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

The Auto Negotiation Configuration window displays.

Step 2 The installation process allows you to automatically set the speed and duplex settings of the Ethernet network interface card (NIC) by using automatic negotiation. You can change this setting after installation.

- To enable automatic negotiation, choose **Yes** and continue with [Step 5](#).

The MTU Configuration window displays.



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

- To disable automatic negotiation, choose **No** and continue with [Step 3](#).

The NIC Speed and Duplex Configuration window displays.

Step 3 If you chose to disable automatic negotiation, manually choose the appropriate NIC speed and duplex settings now and choose **OK** to continue.

The MTU Configuration window displays.

Step 4 In the MTU Configuration window, you can change the MTU size from the operating system default. The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host will transmit on the network. If you are unsure of the MTU setting for your network, use the default value, which is 1500 bytes.



Caution If you configure the MTU size incorrectly, your network performance can be affected.

- To accept the default value (1500 bytes), choose **No**.
- To change the MTU size from the operating system default, choose **Yes**, enter the new MTU size, and choose **OK**.

The DHCP Configuration window displays.

Step 5 For network configuration, you can choose to either set up a static network IP address for the server 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. Skip to [Step 8](#).
- If you want to configure a static IP address for the server, choose **No**. The Static Network Configuration window displays.

Step 6 If you chose not to use DHCP, enter your static network configuration values and choose **OK**. See [Table 4](#) for field descriptions.

The DNS Client Configuration window displays.

Step 7 To enable DNS, choose **Yes**, enter your DNS client information, and choose **OK**. See [Table 4](#) for field descriptions.

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

Step 8 Enter your Administrator login and password from [Table 4](#).



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

The Certificate Information window displays.

- Step 9** Enter your certificate signing request information and choose **OK**.
Continue with the [“Configuring the Server”](#) section on page 2-18.

Configuring the Server

Revised January 7, 2008

After you finish the basic installation, follow this procedure to configure the server.

Procedure

- Step 1** The Network Time Protocol Client Configuration window displays.
Cisco recommends that you use an external NTP server to ensure accurate system time. Ensure the external NTP server is stratum 9 or higher (meaning stratum 1-9).
- Step 2** Choose whether you want to configure an external NTP server or manually configure the system time.
- To set up an external NTP server, choose **Yes** and enter the IP address, NTP server name, or NTP server pool name for at least one NTP server. You can configure up to five NTP servers, and Cisco recommends that you use at least three. Choose **Proceed** to continue with the installation.
The system contacts an NTP server and automatically sets the time on the hardware clock.



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

- To manually configure the system time, choose **No** and enter the appropriate date and time to set the hardware clock. Choose **OK** to continue with the installation.

The Database Access Security Configuration window displays.

- Step 3** Enter the Security password from [Table 4](#).



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

The SMTP Host Configuration window displays.

- Step 4** If you want to configure an SMTP server, choose **Yes** and enter the SMTP server name.



Note You must configure an SMTP server to use certain platform features; however, you can also configure an SMTP server later by using the platform GUI or the command line interface.

- Step 5** Choose **OK**. The Application User Configuration window displays.
- Step 6** Enter the Application User name and password from [Table 4](#) and confirm the password by entering it again.
- Step 7** Choose **OK**. The Platform Configuration Confirmation window displays.
- Step 8** To continue with the installation, choose **OK**; or to modify the platform configuration, choose **Back**.
The system installs and configures the software. The DVD drive ejects, and the server reboots. Do not reinsert the DVD.
- Step 9** When the installation process completes, you get prompted to log in by using the Administrator account and password.
- Step 10** Complete the post-installation tasks that are listed in the “[Post-Installation Tasks](#)” section on page 2-19.

Post-Installation Tasks

Revised January 7, 2008

After installing Cisco Unity Connection on your server, you must perform some post-installation tasks before you can begin using it. For a list of tasks, see [Table 6](#).



Note

To access web applications, you must use a web browser from a computer that has network access to the Cisco Unity Connection server.

Table 6 *Post-Installation Tasks*

Post-Installation Tasks	Important Notes
Log in as the Cisco Unity Connection Application User and change the Application User passwords.	See the “ Changing the Default Application User Passwords ” section on page 2-20.
Activate Cisco Unity Connection feature services that you want to run. Before you activate feature services, you must perform required preactivation tasks. For service activation requirements, refer to the <i>Cisco Unified Serviceability Administration Guide</i> .	Refer to <i>Cisco Unified Serviceability Administration Guide</i> . See the “ Activating Services ” section on page 2-20.
Configure the backup settings. Remember to back up your Cisco Unity Connection data daily.	Refer to <i>Disaster Recovery System Administration Guide</i> .
If applicable, configure any network management systems in use at your site.	Refer to the <i>Cisco Unified Serviceability Administration Guide</i> .

Changing the Default Application User Passwords

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

Activating Services

Even though all services are installed on the server, you may need to use Cisco Unified Serviceability to manually activate services that you want to run. For service recommendations and more information, refer to *Cisco Unified Serviceability Administration Guide*.

Examining Log Files

If you encounter problems with the installation, you may be able to examine the install log files by entering the following commands in Command Line Interface.

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

```
CLI>file list install *
```

To view the log file from the command line, enter

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

where *log_file* is the log file name.

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