



Cisco Unity Connection Reconfiguration and Upgrade Guide

Release 1.x
Revised March 27, 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-8448-04

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.

CCDE, CCENT, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0803R)

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.

Cisco Unity Connection 1.x Reconfiguration and Upgrade Guide
© 2008 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface v

- Audience and Use v
- Documentation Conventions v
- Cisco Unity Connection Documentation vi
- Obtaining Documentation and Submitting a Service Request vi

CHAPTER 1

Upgrading Cisco Unity Connection or Voice-Recognition Software to the Shipping Version 1-1

- Task List for Upgrading Cisco Unity Connection Software to the Shipping Version on the Connection Server 1-2
- Task List for Upgrading Voice-Recognition Software to the Shipping Version on a Separate Voice-Recognition Server 1-3
- Downloading Software for the Upgrade 1-4
- Uninstalling Cisco Security Agent for Cisco Unity 1-6
- Installing the Latest Microsoft Service Packs and Updates, and Cisco Security Agent for Cisco Unity 1-6
- Upgrading Cisco Unity Connection or Voice-Recognition Software 1-7
- Reinstalling Cisco Unity Connection Languages 1-8

CHAPTER 2

Migrating from Cisco Unity 4.0(5) or Later to the Shipping Version of Cisco Unity Connection 2-1

- Task List for Migrating from Cisco Unity with Exchange to Cisco Unity Connection 2-1
- Task List for Migrating from Cisco Unity with Domino to Cisco Unity Connection 2-4
- Verifying System Requirements 2-5
- Obtaining Cisco Unity Connection License Files 2-5
- Duration of the Migration (With Exchange Only) 2-7
- Gathering Telephony Settings from the Cisco Unity System 2-7
- Backing Up Cisco Unity Data and Messages 2-8
- Exporting Cisco Unity Subscriber Data and Voice Messages from Cisco Unity (With Exchange Only) 2-8
 - Stopping Virus-Scanning and Cisco Security Agent Services 2-8
 - Determining the Account That the AvCsMgr Service Logs On As 2-9
 - Installing the Unity to Connection Migration Export Tool on the Cisco Unity Server 2-9
 - Exporting Cisco Unity Subscriber Data and Voice Messages 2-10
 - Restarting Virus-Scanning and Cisco Security Agent Services 2-10
- Removing Cisco Unity (With Exchange Only) 2-10
- Importing Data and Messages into Cisco Unity Connection (With Exchange Only) 2-11

Installing the Unity to Connection Migration Import Tool on the Cisco Unity Connection Server	2-11
Updating the Export File to Accommodate Limited Licenses for User Features	2-11
Importing Cisco Unity Subscriber Data and Voice Messages into Cisco Unity Connection	2-12
Reassigning Cisco Personal Assistant Phones to Cisco Unity Connection	2-12
Deleting Unassigned Directory Numbers	2-13

CHAPTER 3

Adding Licensed Features to Cisco Unity Connection 3-1

Task List for Adding Licensed Features to Cisco Unity Connection	3-1
Obtaining and Installing a License File That Has Additional Features	3-2
Adding Voice Messaging Ports	3-3

CHAPTER 4

Changing Access to Exchange Data for Additional Servers or for Relocated Exchange Mailboxes 4-1

Moving Exchange Mailboxes Between Servers to Which Connection Access to Exchange Data Is Configured	4-1
Task List for Configuring Connection Access to Exchange Data on Additional Servers	4-2
Creating the AD Service Account that Connection Uses to Access Exchange Data	4-3
Granting Exchange Permissions to the AD Service Account	4-4
Creating and Installing SSL Certificates	4-6
Creating Connection External Services to Specify the Exchange Servers That Users Can Access	4-11
Configuring the Connection Server to Trust Exchange Certificates	4-12
Requiring Secure Communication Between Connection and Exchange (Optional But Recommended)	4-13
Updating or Creating Connection User External Service Accounts to Access the Additional Exchange Servers	4-14

APPENDIX A

Removing Software A-1

Removing Cisco Unity Connection and Voice-Recognition Software from the Connection Server	A-1
Removing Voice-Recognition Software from a Separate Voice-Recognition Server	A-2

INDEX



Preface

This preface contains the following sections:

- [Audience and Use, page v](#)
- [Documentation Conventions, page v](#)
- [Cisco Unity Connection Documentation, page vi](#)
- [Obtaining Documentation and Submitting a Service Request, page vi](#)

Audience and Use

The *Cisco Unity Connection Reconfiguration and Upgrade Guide* is intended for system administrators and technicians who handle upgrades and changes to the Cisco Unity Connection system configuration.

The *Cisco Unity Connection Reconfiguration and Upgrade Guide* focuses on information and procedures necessary for changing the current configuration of the system. The guide does not include information on changing Cisco Unity Connection data (for example, user templates and call handlers).

Documentation Conventions

Table 1 *Cisco Unity Connection Reconfiguration and Upgrade Guide Conventions*

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 the Command Prompt window, enter ping <IP address> .)

Table 1 *Cisco Unity Connection Reconfiguration and Upgrade Guide Conventions (continued)*

Convention	Description
- (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 on menus. (Example: On the Windows Start menu, click Settings > Control Panel > Phone and Modem Options .)

The *Cisco Unity Connection Reconfiguration and Upgrade Guide* 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 *Cisco Unity Connection Documentation Guide*. 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 and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



CHAPTER 1

Upgrading Cisco Unity Connection or Voice-Recognition Software to the Shipping Version

The task list and procedures in this chapter apply only to upgrading the Cisco Unity Connection or voice-recognition software to the currently shipping version. Note that the list contains some tasks that reference instructions in other Connection documentation.

For information on adding Cisco Unity Connection features, see the [“Adding Licensed Features to Cisco Unity Connection”](#) chapter after you have finished upgrading the software.

This chapter contains the following sections:

- [Task List for Upgrading Cisco Unity Connection Software to the Shipping Version on the Connection Server, page 1-2](#)
- [Task List for Upgrading Voice-Recognition Software to the Shipping Version on a Separate Voice-Recognition Server, page 1-3](#)
- [Downloading Software for the Upgrade, page 1-4](#)
- [Uninstalling Cisco Security Agent for Cisco Unity, page 1-6](#)
- [Installing the Latest Microsoft Service Packs and Updates, and Cisco Security Agent for Cisco Unity, page 1-6](#)
- [Upgrading Cisco Unity Connection or Voice-Recognition Software, page 1-7](#)
- [Reinstalling Cisco Unity Connection Languages, page 1-8](#)

Task List for Upgrading Cisco Unity Connection Software to the Shipping Version on the Connection Server

1. Determine whether the version of Cisco Security Agent for Cisco Unity installed on the Cisco Unity Connection server, if any, is earlier than the latest version available on the Cisco Software Center website:
 - a. For instructions on determining the version of Cisco Security Agent for Cisco Unity installed on the Connection server, refer to the “Determining the Software Version” section in any *Release Notes for Cisco Security Agent for Cisco Unity* at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.
 - b. For the version of Cisco Security Agent for Cisco Unity that is included in the latest Cisco Unity Server Updates wizard, refer to *Software Installed by the Cisco Unity Server Updates Wizard* at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html.
2. Download software for the upgrade. See “Downloading Software for the Upgrade” section on page 1-4.
3. If the version of Cisco Security Agent for Cisco Unity installed on the Connection server is earlier than the version installed by the latest Cisco Unity Server Updates wizard, stop and uninstall the version that is installed on the server. See the “Uninstalling Cisco Security Agent for Cisco Unity” section on page 1-6.
4. Install the latest Microsoft service packs and updates, and the latest version of Cisco Security Agent for Cisco Unity, as applicable. See the “Installing the Latest Microsoft Service Packs and Updates, and Cisco Security Agent for Cisco Unity” section on page 1-6.
5. If you downloaded the latest version of the Cisco Unity Connection Disaster Recovery tools (DiRT) in Task 2., install the Disaster Recovery Backup tool on the Cisco Unity Connection server.
6. Back up Cisco Unity Connection data and voice messages by using the Connection Disaster Recovery Backup tool. (If you did not download and install the latest version, use the version in Tools Depot.) For instructions, refer to Disaster Recovery Backup tool Help. (The Help file, UnityDisasterRecovery.htm, is in the same directory as UnityDisasterRecoveryBackup.exe.)
7. *If Connection languages other than English-United States are installed:* Uninstall all Connection languages other than English-United States (you downloaded new versions of language files in Task 2.) You will reinstall language files after you have upgraded Cisco Unity Connection software to the shipping version.



Caution The version of languages that you install must match the version of Cisco Unity Connection installed, or language installation will fail.

8. Upgrade Cisco Unity Connection software. See the “Upgrading Cisco Unity Connection or Voice-Recognition Software” section on page 1-7.
9. *If you uninstalled Connection languages in Task 7.:* Reinstall Connection languages. For installation instructions, see the following documentation, depending on the Connection version:
 - For Connection 1.2(1) and later, see the “Reinstalling Cisco Unity Connection Languages” section on page 1-8.
 - For Connection 1.1(1), refer to *Installing Cisco Unity Connection Version 1.1(1) Languages* at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html.

10. Install the service release for the shipping version of Cisco Unity Connection, if available. Instructions for installing the service release are available in the following documentation, depending on the Connection version:
 - For Connection 1.2(1) and later, refer to *Release Notes for Cisco Unity Connection <Version> Service Release <Number>* at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.
 - For Connection 1.1(1), refer to the “Cisco Unity Connection 1.1(1) Service Release 1” section under “New Support—Release 1.1(1)” in *Release Notes for Cisco Unity Connection Release 1.1(1)* at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.
11. *If the system is using a separate voice-recognition server:* Continue with the “Task List for Upgrading Voice-Recognition Software to the Shipping Version on a Separate Voice-Recognition Server” section on page 1-3.

Task List for Upgrading Voice-Recognition Software to the Shipping Version on a Separate Voice-Recognition Server

1. Determine whether the version of Cisco Security Agent for Cisco Unity installed on the voice-recognition server, if any, is earlier than the latest version available on the Cisco Software Center website:
 - a. For instructions on determining the version of Cisco Security Agent for Cisco Unity installed on the voice-recognition server, refer to the “Determining the Software Version” section in any *Release Notes for Cisco Security Agent for Cisco Unity* at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.
 - b. For the version of Cisco Security Agent for Cisco Unity that is included in the latest Cisco Unity Server Updates wizard, refer to *Software Installed by the Cisco Unity Server Updates Wizard* at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html.
2. *If you have not already downloaded software for the Connection upgrade:* Download software. See the “Downloading Software for the Upgrade” section on page 1-4. You do not need to download the Disaster Recovery tools or Connection languages.
3. If the version of Cisco Security Agent for Cisco Unity installed on the voice-recognition server is earlier than the version installed by the latest Cisco Unity Server Updates wizard, stop and uninstall the version that is installed on the server. See the “Uninstalling Cisco Security Agent for Cisco Unity” section on page 1-6.
4. Install the latest Microsoft service packs and updates, and the latest version of Cisco Security Agent for Cisco Unity, as applicable. See the “Installing the Latest Microsoft Service Packs and Updates, and Cisco Security Agent for Cisco Unity” section on page 1-6.
5. Upgrade voice-recognition software. See the “Upgrading Cisco Unity Connection or Voice-Recognition Software” section on page 1-7.

6. Install the service release for the shipping version of Cisco Unity Connection, if available. Instructions for installing the service release are available in the following documentation, depending on the Connection version:
 - For Connection 1.2(1) and later, refer to *Release Notes for Cisco Unity Connection <Version> Service Release <Number>* at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.
 - For Connection 1.1(1), refer to the “Cisco Unity Connection 1.1(1) Service Release 1” section under “New Support—Release 1.1(1)” in *Release Notes for Cisco Unity Connection Release 1.1(1)* at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.

Downloading Software for the Upgrade

This section lists the software needed to upgrade Cisco Unity Connection to the shipping version. The *Cisco Unity Connection Reconfiguration and Upgrade Guide* instructs you when to install the software you download.



Note

To access software download pages, you must be logged on to Cisco.com as a registered user.

Download the following software for all upgrades:

Cisco Unity Connection Server Updates Wizard

The latest version of the Cisco Unity Server Updates wizard, which installs the latest Microsoft updates that are required with Connection, and the latest version of Cisco Security Agent for Cisco Unity. The wizard is available from the Cisco Unity Connection Software Download page.

Even if you have the Connection DVD for the currently shipping version, we recommend that you download the Server Updates wizard, which may have been updated after the disc was produced.

Instructions for downloading and burning a disc of the Server Updates wizard are available in the release notes for the applicable Connection version at

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



Note

Because of export controls on the strong encryption in the Server Updates wizard, the first time you download the wizard, you need to fill out a brief questionnaire. Follow the on-screen prompts.

(For a list of the updates that are installed, refer to *Software Installed by the Cisco Unity Server Updates Wizard* at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html. For information on Cisco Security Agent for Cisco Unity, see *Release Notes for Cisco Security Agent for Cisco Unity* at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.)

Cisco Unity Connection Service Release

The Cisco Unity Connection service release (a rollup of Cisco Unity Connection engineering specials) for the shipping version, if available. Instructions for downloading the service release are available in the following locations, depending on the Connection version:

- For Connection 1.2(1) and later, in the applicable version of *Release Notes for Cisco Unity Connection <Version> Service Release <Number>* at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.



Note If there are no release notes available, a service release for the shipping version has not been released yet.

- For Connection 1.1(1), in *Release Notes for Cisco Unity Connection Release 1.1(1)* at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.

Cisco Unity Connection DVD Image

If you do not have the Cisco Unity Connection DVD or if the version on the DVD is earlier than the currently shipping version, download the DVD image for the currently shipping Connection version from the Cisco Unity Connection Software Download page.

Instructions for downloading and burning a disc of the DVD image are available in the release notes for the applicable Connection version at

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

Cisco Unity Connection Languages

If Connection languages other than English-United States are installed, versions of the language files that match the version of Cisco Unity Connection to which you are upgrading. With a Connection software upgrade, you must also reinstall Connection languages.



Caution

The version of languages that you install must match the version of Cisco Unity Connection installed, or language installation will fail.

Languages other than English-United States are not included on the Cisco Unity Connection DVD. You must download language files from the Cisco Unity Connection Software Download page. (Depending on your license settings, English-United States may not be available.)

Instructions for downloading and burning a disc of the languages that you want to upgrade are available in the following locations, depending on the Connection version:

- For Connection 1.2(1) and later, in the release notes for the applicable Connection version at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.
- For Connection 1.1(1), in *Installing Cisco Unity Connection Version 1.1(1) Languages* at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html.

Cisco Unity Connection Disaster Recovery Tools

The latest version of the Cisco Unity Connection Disaster Recovery tools (DiRT). DiRT is used to back up Cisco Unity Connection data and voice messages before the upgrade and to restore Cisco Unity Connection data and messages, if necessary. (The tools are included on the Cisco Unity Connection DVD, but updates are posted regularly to the Cisco Unity Tools website.)

DiRT is available at http://ciscounitytools.com/App_CUC_DisasterRecoveryTool.htm.

Microsoft Service Packs

The latest service packs recommended for use with Cisco Unity Connection, if any were qualified after the shipping version of Connection was released. Available on the Microsoft website. Also download or print the installation instructions.

For information on recommended service packs, refer to the “Recommended Service Packs—Cisco Unity Connection Server” and “Recommended Service Packs—Optional Voice Recognition Server” sections of *Cisco Unity Connection System Requirements, and Supported Hardware and Software* at

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

Uninstalling Cisco Security Agent for Cisco Unity

To upgrade to the latest version of Cisco Security Agent for Cisco Unity, you need to stop the Cisco Security Agent service and uninstall Cisco Security Agent for Cisco Unity. You will reinstall Cisco Security Agent for Cisco Unity later in the upgrade process.

To Uninstall Cisco Security Agent for Cisco Unity

-
- Step 1** Log on to Windows by using an account that is a member of the local Administrators group.
- Step 2** Stop the Cisco Security Agent service:
- On the Windows Start menu, click **Programs > Administrative Tools > Services**.
 - In the right pane, double-click **Cisco Security Agent**.
 - On the General tab, click **Stop** to stop the service immediately.
 - Click **OK** to close the Cisco Security Agent Properties dialog box.
- Step 3** On the Windows Start menu, click **Programs > Cisco Systems > Uninstall Cisco Security Agent**.
- Step 4** Click **Yes** to confirm that you want to uninstall Cisco Security Agent for Cisco Unity.
- Step 5** Click **Yes** again to restart the server.
-

Installing the Latest Microsoft Service Packs and Updates, and Cisco Security Agent for Cisco Unity

To Install the Latest Microsoft Service Packs and Updates, and Cisco Security Agent for Cisco Unity

-
- Step 1** If you downloaded any Microsoft service packs when you downloaded software in the “[Downloading Software for the Upgrade](#)” section on page 1-4, install them now. Follow the instructions that you printed when you downloaded the service packs.
- Step 2** Insert the “Cisco Unity Server Updates wizard <date>” CD that you burned in the “[Downloading Software for the Upgrade](#)” section on page 1-4 into the DVD drive on the server.

Step 3 Run `ServerUpdatesWizard.exe`.

Step 4 Follow the on-screen prompts.

Upgrading Cisco Unity Connection or Voice-Recognition Software

You run the Cisco Unity Connection Setup program to upgrade Connection software on the Connection server or to upgrade voice-recognition software on a separate server. The Setup program checks the system, prompts you to specify the software to install and where, then upgrades the software you select.

To Upgrade Cisco Unity Connection or Voice-Recognition Software

Step 1 On the Connection or voice-recognition server, log on to Windows by using an account that is a member of the local Administrators group.

Step 2 If you are upgrading software on a separate voice-recognition server, skip to [Step 3](#).

If you are upgrading software on the Connection server, stop Connection:

- a. In the system tray, right-click the **Cisco Unity Connection Server Status** icon, and click **Stop > Cisco Unity Connection**.
- b. On the Windows Start menu, click **Programs > Cisco Unity > Cisco Unity Connection Server Status**.
- c. In the Cisco Unity Connection Server Status utility, confirm that the Server Status tab displays “Cisco Unity Connection is stopped” before you continue with [Step 3](#).

Step 3 Insert the applicable Cisco Unity Connection disc in the DVD drive:

- The DVD you burned after downloading the software image from the Cisco Unity Connection Software Download page (in the “[Downloading Software for the Upgrade](#)” section on page 1-4).
- The applicable DVD shipped with Connection. Note that one disc is for installing Connection on a system with 24 or fewer voice ports, and the other is for installing Connection on a system with 25 or more voice ports.

Step 4 On the Connection DVD, browse to the root directory, and run **Setup.exe**.

Step 5 Follow the on-screen prompts.

Step 6 When the upgrade is complete, restart the server when prompted.

Step 7 If you are upgrading software on a separate voice-recognition server, skip to [Step 8](#).

If you are upgrading software on the Connection server, in the Server Status utility (which starts automatically when you restart the server), confirm that the Server Status tab displays “Cisco Unity Connection is currently running” before you continue with [Step 8](#).

Step 8 Test the upgrade:

- a. Call Connection, and confirm that it answers.
- b. Confirm that you can log on to the Cisco Personal Communications Assistant (PCA) as a subscriber.

- c. For a system using voice recognition, either on the Connection server or on a separate voice-recognition server, log into a voice-recognition-enabled voice mailbox, and confirm that Connection plays the voice-recognition conversation.
-

Reinstalling Cisco Unity Connection Languages

**Caution**

The version of the languages that you reinstall must match the version of Cisco Unity Connection installed, or reinstalling languages will fail.

To Reinstall a Cisco Unity Connection Language

- Step 1** If you are not already logged on to the Cisco Unity Connection server, log on by using an account that is a member of the local Administrators group.
 - Step 2** On the CD or DVD that you burned for language software (in the [“Downloading Software for the Upgrade”](#) section on page 1-4), browse to the root directory.
 - Step 3** Double-click **CiscoUnityConnection<version><language>.exe**, where <language> is the three-letter language abbreviation.
 - Step 4** Follow the on-screen prompts to complete the language installation.
 - Step 5** Repeat [Step 2](#) through [Step 4](#) for each language that you are installing.
-



CHAPTER 2

Migrating from Cisco Unity 4.0(5) or Later to the Shipping Version of Cisco Unity Connection

The sections in this chapter apply only to a migration from a Cisco Unity system that is running version 4.0(5) or later, is integrated with Cisco Unified CallManager version 4.0(x) or later, and uses Cisco Personal Assistant.

This chapter contains the following sections:

- [Task List for Migrating from Cisco Unity with Exchange to Cisco Unity Connection, page 2-1](#)
- [Task List for Migrating from Cisco Unity with Domino to Cisco Unity Connection, page 2-4](#)
- [Verifying System Requirements, page 2-5](#)
- [Obtaining Cisco Unity Connection License Files, page 2-5](#)
- [Duration of the Migration \(With Exchange Only\), page 2-7](#)
- [Gathering Telephony Settings from the Cisco Unity System, page 2-7](#)
- [Backing Up Cisco Unity Data and Messages, page 2-8](#)
- [Exporting Cisco Unity Subscriber Data and Voice Messages from Cisco Unity \(With Exchange Only\), page 2-8](#)
- [Removing Cisco Unity \(With Exchange Only\), page 2-10](#)
- [Importing Data and Messages into Cisco Unity Connection \(With Exchange Only\), page 2-11](#)
- [Reassigning Cisco Personal Assistant Phones to Cisco Unity Connection, page 2-12](#)
- [Deleting Unassigned Directory Numbers, page 2-13](#)

Task List for Migrating from Cisco Unity with Exchange to Cisco Unity Connection

Do the following tasks in the order listed.

1. If Cisco Unity is at version 4.0(4) or earlier and you want to export data and messages from Cisco Unity for importing into Cisco Unity Connection, upgrade to Cisco Unity 4.0(5). The Unity to Connection Migration Export tool, which exports Cisco Unity data for import into Cisco Unity Connection, runs only on Cisco Unity 4.0(5) or later systems.

2. Verify the following requirements:
 - a. Requirements for the Cisco Unity Connection system and for the migration. See the “[Verifying System Requirements](#)” section on page 2-5.
 - 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.
3. Confirm that Cisco Unity Connection license file(s) are available. If the Information Services manager has not already registered Cisco Unity Connection, do so now. See the “[Obtaining Cisco Unity Connection License Files](#)” section on page 2-5.
4. Review the information on the amount of time required for the migration. See the “[Duration of the Migration \(With Exchange Only\)](#)” section on page 2-7.
5. Download the latest versions of the following utilities from the Cisco Unity Tools website:
 - Gather Unity System Info at http://www.ciscounitytools.com/App_GatherUnitySystemInfo.htm.
 - Unity to Connection Migration Export at http://ciscounitytools.com/App_CUCMigrationExport.htm.
 - Unity to Connection Migration Import at http://ciscounitytools.com/App_CUCMigrationImport.htm.
6. Generate and print reports on data for the Cisco Unity system, if applicable. Refer to the “Reports” chapter of the *Cisco Unity Maintenance Guide, Release 4.0(5)* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

**Caution**

The Unity to Connection Migration Export tool, which exports data from the Cisco Unity 4.0(5) or later system, does not export data that Cisco Unity uses to generate reports. In addition, if you are reusing the Cisco Unity server as the Cisco Unity Connection server, all the existing Cisco Unity software and data—including data that Cisco Unity uses to generate reports—is deleted during the migration. If you want any reports from the existing Cisco Unity system, generate them now.

7. Generate and print the telephony report from the Gather Unity System Info utility. See the “[Gathering Telephony Settings from the Cisco Unity System](#)” section on page 2-7.
8. Back up the Cisco Unity server. See the “[Backing Up Cisco Unity Data and Messages](#)” section on page 2-8.
9. Export Cisco Unity data and voice messages. See the “[Exporting Cisco Unity Subscriber Data and Voice Messages from Cisco Unity \(With Exchange Only\)](#)” section on page 2-8.
10. *If Cisco Unity is installed in a Unified Messaging configuration:* Remove Cisco Unity to remove Cisco Unity data from Active Directory. See the “[Removing Cisco Unity \(With Exchange Only\)](#)” section on page 2-10.

11. Do the tasks in the following parts of the “Overview of Mandatory Tasks for Installing a Cisco Unity Connection 1.x System” chapter of the *Cisco Unity Connection Installation Guide* at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html:
 - Task 2 through Task 11 in “Part 1: Installing and Configuring the Cisco Unity Connection Server.” Note the following:

In Task 4, skip the section “Obtaining Cisco Unity Connection License Files (Connection Server Only)”;

you obtained the license files in Task 3. of this list.

When you configure Connection for the integration with the phone system in Task 6., refer to the settings in the Telephony section of the Gather Unity System Info report, which you generated and printed in Task 7. of this task list.
 - All of “Part 2: Installing and Configuring a Separate Voice-Recognition Server (Optional),” if applicable.
 - If you exported Cisco Unity data and voice messages in Task 9. of this list, do Task 17. through Task 20. in “Part 3: Populating the Cisco Unity Connection System with User and Call Management Data.”

If you did not export Cisco Unity data and voice messages, in Task 9. of this list, do Task 17 through Task 22 in “Part 3: Populating the Cisco Unity Connection System with User and Call Management Data.”

**Caution**

Although classes of service and templates in Cisco Unity Connection are generally comparable to those in Cisco Unity, there are some significant differences, so we encourage you to read the documentation before you create classes of service and user templates.

12. If you did not export Cisco Unity data and voice messages, skip to Task 13. in this list.

If you exported data and voice messages, import data and voice messages into Cisco Unity Connection. See the “[Importing Data and Messages into Cisco Unity Connection \(With Exchange Only\)](#)” section on page 2-11.
13. Do the tasks in the following parts of the “Overview of Mandatory Tasks for Installing a Cisco Unity Connection 1.x System” chapter of the *Cisco Unity Connection Installation Guide* at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html:
 - Task 23 through Task 29 in “Part 3: Populating the Cisco Unity Connection System with User and Call Management Data.”
 - All of “Part 4: Setting Up Administrator and User Workstations.”
 - All of “Part 5: Customizing the Cisco Unity Connection Conversation.”
 - All of “Part 6: Backing Up Cisco Unity Connection Data.”
 - All of “Part 7: Training.”
14. Reassign the phones that were used by Cisco Personal Assistant to Cisco Unity Connection. See the “[Reassigning Cisco Personal Assistant Phones to Cisco Unity Connection](#)” section on page 2-12.
15. On the Cisco Unified CallManager server, delete the unassigned directory numbers that were used by Cisco Personal Assistant. See the “[Deleting Unassigned Directory Numbers](#)” section on page 2-13.

Task List for Migrating from Cisco Unity with Domino to Cisco Unity Connection

The Cisco Unity utilities used for exporting and importing data and voice messages are not supported when IBM Lotus Domino is the message store. As a result, when you migrate from a Cisco Unity with Domino system, you must create Connection users with one of the methods documented in the *Cisco Unity Connection User Moves, Adds, and Changes Guide*. In addition, you cannot transfer Cisco Unity voice messages to Connection.

Note that if you do not have any Connection users who will use Microsoft Exchange for e-mail, calendaring, or contacts, skip any Exchange-specific tasks.

Do the following tasks in the order listed.

1. Verify the following requirements:
 - a. Requirements for the Cisco Unity Connection system and for the migration. See the “[Verifying System Requirements](#)” section on page 2-5.
 - 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. Confirm that Cisco Unity Connection license file(s) are available. If the Information Services manager has not already registered Cisco Unity Connection, do so now. See the “[Obtaining Cisco Unity Connection License Files](#)” section on page 2-5.
3. Download the latest version of the Gather Unity System Info utility from the Cisco Unity Tools website at http://www.ciscounitytools.com/App_GatherUnitySystemInfo.htm.
4. Generate and print reports on data for the Cisco Unity system, if applicable. Refer to the “Reports” chapter of the *Cisco Unity Maintenance Guide, Release 4.0(5)* at http://www.cisco.com/en/US/products/sw/voicew/ps2237/prod_maintenance_guides_list.html.



Caution

If you are reusing the Cisco Unity server as the Cisco Unity Connection server, all the existing Cisco Unity software and data—including data that Cisco Unity uses to generate reports—is deleted during the migration. If you want any reports from the existing Cisco Unity system, generate them now.

5. Generate and print the telephony report from the Gather Unity System Info utility. See the “[Gathering Telephony Settings from the Cisco Unity System](#)” section on page 2-7.
6. Back up the Cisco Unity server. See the “[Backing Up Cisco Unity Data and Messages](#)” section on page 2-8.
7. Do the tasks in the following parts of the “Overview of Mandatory Tasks for Installing a Cisco Unity Connection 1.x System” chapter of the *Cisco Unity Connection Installation Guide* at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html:
 - Task 2 through Task 11 in “Part 1: Installing and Configuring the Cisco Unity Connection Server.” Note the following:

In Task 4, skip the section “Obtaining Cisco Unity Connection License Files (Connection Server Only)”; you obtained the license files in Task 2. of this list.

When you configure Connection for the integration with the phone system in Task 6, refer to the settings in the Telephony section of the Gather Unity System Info report, which you generated and printed in Task 5. of this task list.

- All of “Part 2: Installing and Configuring a Separate Voice-Recognition Server (Optional),” if applicable.
- All of “Part 3: Populating the Cisco Unity Connection System with User and Call Management Data.”

**Caution**

Although classes of service and templates in Cisco Unity Connection are generally comparable to those in Cisco Unity, there are some significant differences, so we encourage you to read the documentation before you create classes of service and user templates.

- All of “Part 4: Setting Up Administrator and User Workstations.”
 - All of “Part 5: Customizing the Cisco Unity Connection Conversation.”
 - All of “Part 6: Backing Up Cisco Unity Connection Data.”
 - All of “Part 7: Training.”
8. Reassign the phones that were used by Cisco Personal Assistant to Cisco Unity Connection. See the “[Reassigning Cisco Personal Assistant Phones to Cisco Unity Connection](#)” section on page 2-12.
 9. On the Cisco Unified CallManager server, delete the unassigned directory numbers that were used by Cisco Personal Assistant. See the “[Deleting Unassigned Directory Numbers](#)” section on page 2-13.

Verifying System Requirements

Refer to *Cisco Unity Connection System Requirements, and Supported Hardware and Software* at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html to confirm that the hardware and software that you intend to use for the Cisco Unity Connection system is supported.

Some hardware, software, and configurations that are supported with Cisco Unity are not supported with Cisco Unity Connection. In particular, note the following:

- Some servers that were supported for Cisco Unity 4.0(5) and later are not supported with Cisco Unity Connection. If the Cisco Unity server is not supported with Connection, Cisco Unity Connection Setup will fail.
- Windows Server 2003 must be installed by using the Cisco Platform Configuration disc. If you install Windows Server 2003 by using any other method, Cisco Unity Connection Setup will fail.
- Phone system integrations that require voice cards are not supported.

Obtaining Cisco Unity Connection License Files

For the migration to Cisco Unity Connection, you obtain license files by sending an e-mail request. Cisco e-mails the license files. The e-mail from Cisco contains instructions on how to save and store the files. Later in the migration process, the *Cisco Unity Connection Reconfiguration and Upgrade Guide* refers you to the *Cisco Unity Connection Installation Guide*, which provides instructions on installing the license files.

The following information is required during registration:

- The MAC address (physical address) for the network interface card (NIC) in the Cisco Unity server.
- The MAC address for the NIC in the Cisco Unity Connection server.

- The product authorization key (PAK), which appears on the back of the Cisco Unity Connection Application Software Media kit.

This section contains two procedures. Do them in the order listed.

To Get the MAC Address of the Cisco Unity and Cisco Unity Connection Servers

-
- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Accessories > Command Prompt**.
- Step 2** In the Command Prompt window, enter **ipconfig /all**, and press **Enter**.
- Step 3** Write down the value of Physical Address, excluding the hyphens, or save it to a file that you can access during online registration. (For example, if the physical address is 00-A1-B2-C3-D4-E5, record 00A1B2C3D4E5.)
- If the server contains more than one NIC, one value will appear for each NIC. Write down the value for the first NIC. This is the MAC address that will be assigned to both NICs when you configure fault tolerance.
- Step 4** Close the Command Prompt window.
- Step 5** If you are using a different server for the Cisco Unity Connection server, repeat [Step 1](#) through [Step 4](#) on the Cisco Unity Connection server.
-

To Register and Obtain the License Files

-
- Step 1** Send an e-mail requesting a license file for the migration to:
connectionmigration@external.cisco.com
- Include the following information:
- The MAC address for the NIC in the Cisco Unity server.
 - The MAC address for the NIC in the Cisco Unity Connection server.
 - The PAK from the Cisco Unity Connection Application Software Media kit.
- Step 2** When you receive a reply from licensing@cisco.com, follow the instructions in the e-mail.
- If there are questions on your request or if we need to confirm that you accept that you will lose features, we will send a query before we send the license files.
- If the license files are lost, it can take up to one business day to get another copy.
-

If you do not get the licensing files within a day or if you need another copy of the licensing file, forward to licensing@cisco.com the e-mail that you sent to connectionmigration@external.cisco.com.



Note

Cisco Unity Connection software comes with a default license file that has a minimal number of settings. The license file allows installation of a Cisco Unity Connection demonstration system. For information and instructions on installing a demonstration system, refer to the “Cisco Unity Connection Demonstration System” appendix of the *Cisco Unity Connection Installation Guide* at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html.

Duration of the Migration (With Exchange Only)

**Note**

If you are migrating a Cisco Unity with Domino system to Cisco Unity Connection, skip this section.

If you plan to export data and messages from Cisco Unity and import them into Cisco Unity Connection, note the following considerations:

- Exporting data takes only a few minutes.
- Messages are exported at the rate of about 240 per minute.
- Data is imported at the rate of about 40 users per minute.
- Messages are imported at the rate of about 150 per minute.

The duration of these tasks will vary depending on the following criteria:

- The speed of the processor in the Cisco Unity server.
- The amount of RAM in the Cisco Unity server.
- The amount of call traffic when you are exporting data.
- When Cisco Unity subscriber mailboxes are homed on a separate Exchange server and you are exporting voice messages, the speed of the network.

Gathering Telephony Settings from the Cisco Unity System

**Note**

If you are not integrating Cisco Unity Connection with the same phone system with which Cisco Unity is integrated, skip this section.

To integrate Cisco Unity Connection with the same phone system with which Cisco Unity is integrated, you need telephony settings from Cisco Unity to facilitate creating the integration. Do the following procedure to install the latest version of the Gather Unity System Info utility, and to display and print the telephony settings.

To Gather Telephony Settings from the Cisco Unity System

- Step 1** Install the Gather Unity System Info utility that you downloaded from the Cisco Unity Tools website:
 - a. Run **Gather Unity System Info.msi**.
 - b. Follow the on-screen prompts.
- Step 2** On the Cisco Unity server, double-click the **Cisco Unity Tools Depot** icon on the Windows desktop.
- Step 3** In the left pane, expand **Reporting Tools**.
- Step 4** Double-click **Gather Unity System Info**.
- Step 5** In the Gather Unity System Info window, select all text.
- Step 6** Press **Ctrl-C** to copy the text to the Windows clipboard.
- Step 7** Open Notepad.
- Step 8** Press **Ctrl-V** to paste the text from the Windows clipboard into Notepad.

- Step 9** Print the text or save it in a file that you can access while you are creating a phone system integration with Cisco Unity Connection.
- Step 10** Exit Notepad.
- Step 11** Exit the Gather Unity System Info utility.
-

Backing Up Cisco Unity Data and Messages

If you are reusing the Cisco Unity server as the Cisco Unity Connection server, back up Cisco Unity data by using the Cisco Unity Disaster Recovery Backup tool in case you need to revert to Cisco Unity 4.0(5).

If Cisco Unity voice messages are stored in an Exchange mailbox store on the Cisco Unity server, back up Exchange messages by using an Exchange-aware backup utility.



Caution

We recommend against using the Cisco Unity Disaster Recovery Backup tool to back up voice messages. The Disaster Recovery Backup tool uses ExMerge to back up Exchange messages, and an ExMerge backup and restore of the message database may be much larger than the message database itself because ExMerge backs up each Exchange mailbox separately. If you use ExMerge and then need to restore Exchange messages, there may not be enough room on the hard disk to restore all mailboxes.

Exporting Cisco Unity Subscriber Data and Voice Messages from Cisco Unity (With Exchange Only)



Note

If you are migrating a Cisco Unity with Domino system to Cisco Unity Connection, skip this section.

Do the procedures in the following five sections in the order listed:

- [Stopping Virus-Scanning and Cisco Security Agent Services, page 2-8](#)
- [Determining the Account That the AvCsMgr Service Logs On As, page 2-9](#)
- [Installing the Unity to Connection Migration Export Tool on the Cisco Unity Server, page 2-9](#)
- [Exporting Cisco Unity Subscriber Data and Voice Messages, page 2-10](#)
- [Restarting Virus-Scanning and Cisco Security Agent Services, page 2-10](#)

Stopping Virus-Scanning and Cisco Security Agent Services



Note

If the system is not using antivirus software or Cisco Security Agent for Cisco Unity, skip this section.

You stop virus-scanning and Cisco Security Agent services on the server so that they do not slow down the installation of software or cause the installations to fail, and so they do not interfere with exporting Cisco Unity data.

**Caution**

Do not stop the Cisco Security Agent service by using the net stop command or the Cisco Security Agent icon in the task bar. These methods are not supported.

To Stop Virus-Scanning and Cisco Security Agent Services

-
- Step 1** Refer to the antivirus software documentation to determine the names of the virus-scanning services.
 - Step 2** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
 - Step 3** For each virus-scanning service and the Cisco Security Agent service, right-click the name of each service, and click **Stop**.
 - Step 4** When all services have stopped, close the Services MMC.
-

Determining the Account That the AvCsMgr Service Logs On As

To install and run the Unity to Connection Migration Export tool, you must log on to Windows by using the account that the Cisco Unity AvCsMgr service logs on as. Do the following procedure to determine that account.

To Determine the Account That the AvCsMgr Service Logs On As

-
- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Services**.
 - Step 2** In the right pane, double-click **AvCsMgr**.
 - Step 3** Click the **Log On** tab.
 - Step 4** Write down the name of the account that the service logs on as.
 - Step 5** Click **Cancel**.
 - Step 6** Close the Services MMC.
 - Step 7** Log out of Windows.
-

Installing the Unity to Connection Migration Export Tool on the Cisco Unity Server

In this section, you install the Unity to Connection Migration Export tool that you downloaded from the Cisco Unity Tools website in the [“Task List for Migrating from Cisco Unity with Exchange to Cisco Unity Connection”](#) section on page 2-1.

To Install the Unity to Connection Migration Export Tool on the Cisco Unity Connection Server

-
- Step 1** Log on to the Cisco Unity server by using the account that you identified in the [“To Determine the Account That the AvCsMgr Service Logs On As”](#) procedure on page 2-9.

- Step 2** Run `CUMigrationExport.msi`.
 - Step 3** Follow the on-screen prompts.
-

Exporting Cisco Unity Subscriber Data and Voice Messages

We recommend that you run the Unity to Connection Migration Export tool during nonbusiness hours so the report runs faster and so it does not interfere with Cisco Unity performance.

To Export Cisco Unity Subscriber Data and Voice Messages

- Step 1** Browse to the directory **CUC Migration Export**.
 - Step 2** Run `UnityToConnectionMigrationExport.exe`.
For information on exporting data and voice messages, including which data can be exported, refer to the Help file `UnityToConnectionMigrationExport.htm`.
-

Restarting Virus-Scanning and Cisco Security Agent Services



Note

If the system is not using antivirus software or Cisco Security Agent for Cisco Unity, or if you are reusing the Cisco Unity server as the Cisco Unity Connection server and will be installing Cisco Unity Connection immediately, skip this section.

To Restart Virus-Scanning and Cisco Security Agent Services

- Step 1** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
 - Step 2** For each virus-scanning service and the Cisco Security Agent service, right-click the name of each service, and click **Start**.
 - Step 3** When the services have restarted, close the Services MMC.
-

Removing Cisco Unity (With Exchange Only)

If Cisco Unity is installed in a Unified Messaging configuration, some Cisco Unity-specific data is stored in the Active Directory database. Removing Cisco Unity removes this data from Active Directory.

To Remove Cisco Unity

- Step 1** On the Cisco Unity server, browse to the directory `CommServer\Utilities\UninstallUnity3xand4x`.

- Step 2** Remove Cisco Unity by following the instructions in the Help file UninstallUnity3xand4x.htm.
-

Importing Data and Messages into Cisco Unity Connection (With Exchange Only)

**Note**

If you are migrating a Cisco Unity with Domino system to Cisco Unity Connection, skip this section.

Do the procedures in the following three sections in the order listed:

- [Installing the Unity to Connection Migration Import Tool on the Cisco Unity Connection Server, page 2-11](#)
- [Updating the Export File to Accommodate Limited Licenses for User Features, page 2-11](#)
- [Importing Cisco Unity Subscriber Data and Voice Messages into Cisco Unity Connection, page 2-12](#)

Installing the Unity to Connection Migration Import Tool on the Cisco Unity Connection Server

In this section you install the Unity to Connection Migration Import tool that you downloaded from the Cisco Unity Tools website in the [“Task List for Migrating from Cisco Unity with Exchange to Cisco Unity Connection”](#) section on page 2-1.

To Install the Unity to Connection Migration Import Tool on the Cisco Unity Connection Server

- Step 1** Log on to the Cisco Unity Connection server.
- Step 2** Run `CUMigrationImport.msi`.
- Step 3** Follow the on-screen prompts.
-

Updating the Export File to Accommodate Limited Licenses for User Features

**Note**

When you import user data, you are prompted to choose the template with which you want users to be created. If the Cisco Unity Connection license includes enough licenses for all users to have the same features (for example, 500 Advanced User licenses when you have 500 users), and if you want to create all users with one template (and the associated class of service), skip this section.

When the Cisco Unity Connection license includes a limited number of licenses for some user features (for example, 50 Advanced User licenses when you have 500 users), you must use different templates and classes of service for the users who should have access to these features and for the users who should not.

If you use one template and class of service for all users and the features are enabled, then importing users will fail after the last license is used. In the example of 50 Advanced User licenses for 500 users, the import will fail while importing the 51st user.

If you use one template and class of service for all users and the features are disabled, then importing users will succeed, but no one will have access to the features for which you have limited licenses. You will then have to manually change the settings for the users who will use those features.

To use two or more templates, you can update the CSV file that was created when you did the procedures in the “Exporting Cisco Unity Subscriber Data and Voice Messages from Cisco Unity (With Exchange Only)” section on page 2-8. For each user, you add the name of the template with which you want each user to be created. For information on editing the CSV file, see the Help for the Bulk Administration Manager tool, which is available in the Administration Tools section of Tools Depot.

Importing Cisco Unity Subscriber Data and Voice Messages into Cisco Unity Connection

To Import Cisco Unity Subscriber Data and Voice Messages into Cisco Unity Connection

-
- Step 1** On the drive where Cisco Unity Connection is installed, browse to the **Connection\Utilities\CUMigrationImport** directory.
- Step 2** Run **UnityToConnectionMigrationImport.exe**. For information on using the import utility, refer to the Help file **UnityToConnectionMigrationImport.htm**.

If you encounter any errors during the import, review the *Migration Tool for Going from Cisco Unity to Connection* training video at http://ciscounitytools.com/TOL_CUC1.1.htm. (Note that although the page is labeled “Connection 1.1 Training Videos,” the video applies to Connection 1.x.)

Reassigning Cisco Personal Assistant Phones to Cisco Unity Connection



Caution

If the phones used by Cisco Personal Assistant are not reassigned to Cisco Unity Connection, calls may be routed to the wrong extension.

You can use the Bulk Administration Tool to change the partition on phones in much less time than it takes to make the changes to each phone individually. For instructions on using the tool, refer to the Cisco Unified CallManager documentation, available at http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_installation_and_configuration_guides_list.html.

If you prefer to make the changes individually on each phone, do the following procedure.

To Individually Reassign Cisco Personal Assistant Phones to Cisco Unity Connection

-
- Step 1** In Cisco Unified CallManager Administration, on the Device menu, click **Phone**.

-
- Step 2** On the Find and List Phones page, click **Find**.
 - Step 3** Click the first phone that you want to assign to the Cisco Unity Connection partition.
 - Step 4** On the Directory Number Configuration page, in the Partition field, click the partition that gives the Cisco Unity Connection voice messaging ports access to the phone.
 - Step 5** In the Calling Search Space field, click the calling search space that provides access to the Cisco Unity Connection pilot number and to other extensions that the phone must be able to call.
 - Step 6** In the Voice Mail Profile field, select the voice mail profile that you created for Cisco Unity Connection when you programmed Cisco Unified CallManager for the integration.
 - Step 7** Click **Update**.
 - Step 8** Repeat [Step 3](#) through [Step 7](#) for all remaining phones that must be reassigned to Cisco Unity Connection.
-

Deleting Unassigned Directory Numbers

Even after you reassign Cisco Personal Assistant subscriber phones to Cisco Unity Connection, the directory numbers that were used by Cisco Personal Assistant remain in the Cisco Unified CallManager database. To prevent calls to these extensions from being misrouted, delete unassigned directory numbers in the Cisco Unified CallManager database.

To Delete Unassigned Directory Numbers

- Step 1** In Cisco Unified CallManager Administration, on the Route Plan menu, click **Route Plan Report**.
 - Step 2** On the Route Plan Report page, in the first Search Options list, click **Unassigned DN** and click **Find**.
 - Step 3** Under Search Results, check the check box next to the directory numbers that were used by Cisco Personal Assistant and click **Delete Selected**.
 - Step 4** When prompted that the directory number will be deleted, click **OK**.
-

■ Deleting Unassigned Directory Numbers



CHAPTER 3

Adding Licensed Features to Cisco Unity Connection

This chapter contains the following sections:

- [Task List for Adding Licensed Features to Cisco Unity Connection](#), page 3-1
- [Obtaining and Installing a License File That Has Additional Features](#), page 3-2
- [Adding Voice Messaging Ports](#), page 3-3

Task List for Adding Licensed Features to Cisco Unity Connection

1. Order the additional feature(s) by using the same source you normally use to purchase Cisco products. The high-level product ID is UNITYCNx-LIC-UPG where x is the Cisco Unity Connection major version number.
2. If you do not already have a license that includes the feature(s) that you want to add, obtain and install the license file. See the [“Obtaining and Installing a License File That Has Additional Features”](#) section on page 3-2.
3. Refer to the applicable documentation listed in [Table 3-1](#) for information on adding or configuring the new feature(s).

Table 3-1 Information on Adding or Configuring New Licensed Features

Feature	Documentation
Adding users	In the <i>Cisco Unity Connection User Moves, Adds, and Changes Guide</i> at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html , see the following chapters: <ul style="list-style-type: none">• “Adding an Individual User Account by Using Cisco Unity Connection Administration.”• “Managing Multiple User Accounts with the Cisco Unity Connection Bulk Administration Manager.”
Adding voice messaging ports	The “Adding Voice Messaging Ports” section on page 3-3 of this guide.

Table 3-1 Information on Adding or Configuring New Licensed Features (continued)

Feature	Documentation
Adding voice recognition	<ul style="list-style-type: none"> The tasks in “Part 2: Installing and Configuring a Separate Voice-Recognition Server (Optional)” in the “Overview of Mandatory Tasks for Installing a Cisco Unity Connection 1.x System” chapter of the <i>Cisco Unity Connection Installation Guide</i> at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html. The “Changing the Conversation Version” section in the “Setting Up Features and Functionality That Are Controlled by User Account Settings” chapter of the <i>Cisco Unity Connection User Moves, Adds, and Changes Guide</i> at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.
Configuring access to Exchange e-mails through TTS	<ul style="list-style-type: none"> The “Configuring Access to Exchange E-Mails Through TTS” chapter of the <i>Cisco Unity Connection Installation Guide</i> at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html. The “Text to Speech Access to Exchange E-Mail” section in the “Setting Up Features and Functionality That Are Controlled by Class of Service” chapter of the <i>Cisco Unity Connection User Moves, Adds, and Changes Guide</i> at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.
Configuring access to the Cisco Unity Inbox web tool	The “Setting Up Access to the Cisco Personal Communications Assistant” chapter of the <i>Cisco Unity Connection User Setup Guide</i> at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html .
Configuring IMAP client access to Cisco Unity Connection voice messages	<ul style="list-style-type: none"> The “Securing Cisco PCA and IMAP E-Mail Client Access to Cisco Unity Connection” chapter of the <i>Cisco Unity Connection Installation Guide</i> at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html. The “IMAP Client Access to Voice Messages” section in the “Setting Up Features and Functionality That Are Controlled by Class of Service” chapter of the <i>Cisco Unity Connection User Moves, Adds, and Changes Guide</i> at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Obtaining and Installing a License File That Has Additional Features

License files, which enable the features purchased by the customer, are required for configuring Cisco Unity Connection software and for adding or changing licensed features. You obtain the license files by completing registration information on Cisco.com.

Shortly after registration, Cisco e-mails the license files. The e-mail from Cisco contains instructions on how to save and store the files.

The following information is required during registration:

- The MAC address (physical address) for the network interface card (NIC) in the Cisco Unity Connection server.
- The product authorization key (PAK), which appears on the sticker located on the back of the Cisco Unity Connection Application Software Media kit.

This section contains three procedures. Do them in the order listed.

To Get the MAC Address of the Cisco Unity Connection Server

- Step 1** On the Windows Start menu, click **Programs > Accessories > Command Prompt**.
- Step 2** In the Command Prompt window, enter **ipconfig /all**, and press **Enter**.
- Step 3** Write down the value for Physical Address, excluding the hyphens (for example, if the physical address is 00-A1-B2-C3-D4-E5, record 00A1B2C3D4E5), or save it to a file that you can access during online registration.
- If the server contains more than one NIC, one value will appear for each NIC. Use the value for the primary NIC.
- Step 4** Close the command prompt window.
-

To Register and Obtain the License Files

- Step 1** Go to the software registration site at <http://www.cisco.com/go/license> (URLs are case sensitive).
- Step 2** Enter the PAK and click **Submit**.
- Step 3** Follow the on-screen prompts.
- Step 4** You will receive an e-mail with the Cisco Unity Connection license file.
-

To Install the License Files

- Step 1** Log on to Windows by using an account that is a member of the local Administrators group.
- Step 2** On the Windows desktop, double-click the **Connection Administration** icon.
- Step 3** In Cisco Unity Connection Administration, expand **System Settings**, then click **Licenses**.
- Step 4** On the Search License page, click **Add New**.
- Step 5** On the Add New License page, click **Browse**, and browse to the location of the new license file.
- Step 6** In the Choose File dialog box, double-click the name of the file.
- Step 7** On the Add New License page, click **Submit**.
- Step 8** If you have more than one new license file, repeat **Step 4** through **Step 7** until you have added all of the new license files.
- Step 9** On the Search License page, check the check box(es) for the license file(s) that you added in **Step 4** through **Step 7**.
- Step 10** Click **Install Selected**.
- Step 11** In the Windows system tray, right-click the **Cisco Unity Connection** icon, and click **Restart > Cisco Unity Connection**.
-

Adding Voice Messaging Ports

Revised March 27, 2008

Voice messaging ports provide the connections for calls between Cisco Unity Connection and the phone system. You can add voice messaging ports after the phone system integration has been created.

**Caution**

The number of voice messaging ports that you add cannot bring the total number of voice messaging ports for all port groups to more than the maximum number of voice messaging ports that are enabled by the Cisco Unity Connection license files. If the license files do not enable the total number of ports, you will not be able to add the new ports.

Do the first procedure below only if the number of ports is changing from 24 or fewer to more than 24. Do the other two procedures for all systems.

To Upgrade from MSDE 2000 to SQL Server 2000 (Only If the Number of Ports Is Changing from 24 or Fewer to More Than 24)

- Step 1** Log on to Windows.
- Step 2** Right-click the Cisco Unity Connection icon in the Windows taskbar, and click **Stop > Cisco Unity Connection**.
- Step 3** Insert the Cisco Unity Connection disc in the CD-ROM drive.
- Step 4** Browse to the directory `SQLServer2000\ENT`, and run **Autorun.exe**.
- Step 5** Click **SQL Server 2000 Components**.
- Step 6** Click **Install Database Server**.
- Step 7** In the Welcome dialog box, click **Next**.
- Step 8** In the Computer Name dialog box, click **Next** to accept the default setting Local Computer.
- Step 9** In the Installation Selection dialog box, click **Upgrade, Remove, or Add Components to an Existing Instance of SQL Server**, and click **Next**.
- Step 10** In the Instance Name dialog box, uncheck the **Default** check box.
- Step 11** In the Instance Name list, click **CISCO UNITY**, and click **Next**.
- Step 12** In the Existing Installation dialog box, click **Next**.
- Step 13** In the Upgrade dialog box, check the **Yes, Upgrade My Programs** check box, and click **Next**.
- Step 14** In the Choose Licensing Mode dialog box, click **Processor License For**, and enter the number of processors in the Connection server.
- Step 15** Click **Continue**.
- Step 16** Click **Yes** to install additional components.
- Step 17** In the Select Components dialog box, check the check boxes for the following components:
 - **Server Components**, and all subcomponents.
 - **Management Tools**, and all subcomponents.
 - **Client Connectivity**.
- Step 18** Click **Next**.
- Step 19** In the Start Copying Files dialog box, click **Next**.
- Step 20** Click **Finish**.
- Step 21** Browse to the directory `SQL Server 2000\SP`, and run **Setup.bat**.

- Step 22** Follow the on-screen prompts to install SQL Server 2000 service pack 4.
- Step 23** At the end of the installation, choose the option to restart the server.
-

To Program the Phone System for the Additional Voice Messaging Ports

- Step 1** See the documentation for the phone system.
-

To Configure Cisco Unity Connection to Use the New Voice Messaging Ports

- Step 1** Log on to Cisco Unity Connection Administration.
- Step 2** In Cisco Unity Connection Administration, expand **Telephony Integrations**, then click **Port**.
- Step 3** On the Search Ports page, under Port Search Results, click **Add New**.
- Step 4** On the New Port page, enter the applicable settings and click **Save**.



Caution Make sure that there are an appropriate number of ports set to answer calls and an appropriate number of ports set to dial out. Otherwise, the integration may not function correctly. See the “Planning How the Voice Messaging Ports Will Be Used by Cisco Unity Connection” section of the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

- Step 5** In the Windows system tray, right-click the **Cisco Unity Connection** icon and click **Restart > Voice Processing Server Role**.
- Step 6** When prompted to confirm stopping the Voice Processing server role, click **Yes**.
- Step 7** In Cisco Unity Connection Administration, in the Related Links list (in page title bar), click **Check Telephony Configuration** and click **Go** to confirm the phone system integration settings.
- If the test is not successful, the Task Results list displays one or more messages with troubleshooting steps. After correcting the problems, check the configuration again.
- Step 8** Log off Cisco Unity Connection Administration.
-



CHAPTER 4

Changing Access to Exchange Data for Additional Servers or for Relocated Exchange Mailboxes

The sections in this chapter apply only when the Cisco Unity Connection system is already configured to access calendar and contact data on Exchange servers, as documented in the *Cisco Unity Connection Installation Guide* (in the “Configuring Access to Exchange Calendars and Contacts for Personal Call Transfer Rules” chapter).

This chapter contains the following sections:

- [Moving Exchange Mailboxes Between Servers to Which Connection Access to Exchange Data Is Configured, page 4-1](#)
- [Task List for Configuring Connection Access to Exchange Data on Additional Servers, page 4-2](#)
- [Creating the AD Service Account that Connection Uses to Access Exchange Data, page 4-3](#)
- [Granting Exchange Permissions to the AD Service Account, page 4-4](#)
- [Creating and Installing SSL Certificates, page 4-6](#)
- [Creating Connection External Services to Specify the Exchange Servers That Users Can Access, page 4-11](#)
- [Configuring the Connection Server to Trust Exchange Certificates, page 4-12](#)
- [Requiring Secure Communication Between Connection and Exchange \(Optional But Recommended\), page 4-13](#)
- [Updating or Creating Connection User External Service Accounts to Access the Additional Exchange Servers, page 4-14](#)

Moving Exchange Mailboxes Between Servers to Which Connection Access to Exchange Data Is Configured

In this section, you move mailboxes between two Exchange servers to which access to Exchange calendar and contact data is already configured, and update existing external service accounts for each Cisco Unity Connection user whose mailbox you moved. It assumes the following conditions have been met:

- The Connection user accounts to which you want to give access to calendar and contact data exist.
- The accounts are assigned to a class of service in which the option Allow Users to Use Personal Call Transfer Rules is enabled.

To Move Exchange Mailboxes Between Servers to Which Connection Access to Exchange Data Is Configured

-
- Step 1** Move the Exchange mailboxes to the other server to which Connection access to Exchange data is configured. Refer to Exchange Help for instructions.
- Step 2** On the Connection server, log on to Cisco Unity Connection Administration.
- Step 3** In Cisco Unity Connection Administration, expand **Users**.
- Step 4** On the Search Users page, in the Search Results table, click the alias of the applicable user.
If the user does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and click **Find**.
- Step 5** On the Edit User Basics page, on the Edit menu, click **External Service Accounts**.
- Step 6** On the External Service Accounts page, click the name of the external service account that was originally created for Connection access to Exchange calendar and contact data.
If there is more than one external service account, use the account for which the value in the Service Type list is **WebDav**.
- Step 7** Confirm that the value of the Account Login field is the Active Directory user logon name for the user.
- Step 8** Change the value of the Server URL Suffix field to the new Exchange account logon name for the user.
- Step 9** Click **Save**.
- Step 10** Repeat [Step 3](#) through [Step 9](#) for any other users whose Exchange mailboxes you moved to the other Exchange server.
-

Task List for Configuring Connection Access to Exchange Data on Additional Servers

To allow Connection access to calendar and contact data on one or more Exchange servers to which access is not already configured, do the following tasks.

1. If the additional Exchange servers are in the same Active Directory domain as any of the Exchange servers to which Connection access to calendar and contact data is already configured, skip to [Task 3](#).

If the additional Exchange servers are in a different Active Directory domain from any of the Exchange servers to which Connection access to calendar and contact data is already configured, create a new Active Directory service account in the same Active Directory domain as the additional Exchange servers. See the [“Creating the AD Service Account that Connection Uses to Access Exchange Data”](#) section on page 4-3.

2. Grant the required Exchange permissions to the Active Directory account that you created in [Task 1](#). See the [“Granting Exchange Permissions to the AD Service Account”](#) section on page 4-4.
3. Create and install an SSL certificate on each additional Exchange server. See the [“Creating and Installing SSL Certificates”](#) section on page 4-6.

4. Create a Connection external service for each additional Exchange server. See the [“Creating Connection External Services to Specify the Exchange Servers That Users Can Access”](#) section on page 4-11.
5. Configure the Connection server to trust the SSL certificates from the additional Exchange servers. See the [“Configuring the Connection Server to Trust Exchange Certificates”](#) section on page 4-12.
6. Configure the additional Exchange servers to require secure (encrypted) communication with the Connection server. See the [“Requiring Secure Communication Between Connection and Exchange \(Optional But Recommended\)”](#) section on page 4-13.
7. Update or create user external service accounts to allow access to calendar and contact data on the additional Exchange servers. See the [“Updating or Creating Connection User External Service Accounts to Access the Additional Exchange Servers”](#) section on page 4-14.

Creating the AD Service Account that Connection Uses to Access Exchange Data



Note

If the additional Exchange servers are in the same Active Directory domain as any of the Exchange servers to which Connection access to calendar and contact data is already configured, skip this section.

Cisco Unity Connection accesses Exchange calendar and contact data by using an Active Directory service account that acts as a proxy for Connection. When you are configuring access to additional Exchange servers that are in a different Active Directory domain from any of the Exchange servers to which Connection access to Exchange data is already configured, you must create a new service account for the additional servers.

To Create the AD Service Account that Cisco Unity Connection Uses to Access Exchange Data

- Step 1** On a server on which Active Directory Users and Computers is installed, log on to Windows by using an account that has the right to create new users.
- Step 2** On the Windows Start menu, click **Programs > Microsoft Exchange > Active Directory Users and Computers** or click **Programs > Administrative Tools > Active Directory Users and Computers**.
- Step 3** In the left pane, expand the domain in which you want to create the account, right-click **Users** or the organizational unit where you want to create the account, and click **New > User**.
- Step 4** Follow the on-screen prompts to create the service account, choosing the following options:
 - When you choose password options, choose the option that prevents the password from expiring. If the password expires, Connection will stop working the next time the server is restarted.
 - Do not create an Exchange mailbox.
- Step 5** Close Active Directory Users and Computers.

Granting Exchange Permissions to the AD Service Account



Note

If the additional Exchange server is in the same Active Directory domain as any of the Exchange servers to which Connection access to calendar and contact data is already configured, skip this section.

To enable the Active Directory service account to access Exchange data, you delegate Exchange View Only Administrator control to the account, and you grant the account Administer Information Store, Send As, and Receive As permissions.

You can delegate control either at the organization level or at the administrative group level. If you delegate control at the administrative group level, you must delegate control in every administrative group that contains the following mailstores:

- An Exchange mailstore from which you want Connection users to be able to import contact data.
- An Exchange mailstore in which you want Connection to be able to access Exchange calendar data.

To Grant Exchange Permissions to the AD Service Account

- Step 1** On a server on which Exchange System Manager is installed, log on to Windows by using an account that is an Exchange Full Administrator.
- Step 2** On the Windows Start menu, click **Programs > Microsoft Exchange > System Manager**.
- Step 3** In the left pane of Exchange System Manager, right-click either the organization name at the top of the tree control or an administrative group that contains mailstores in which you want to access calendar and contact data, and click **Delegate Control**.
- Step 4** On the Welcome to the Exchange Administration Delegation Wizard page, click **Next**.
- Step 5** In the Users or Groups dialog box, click **Add**.
- Step 6** In the Delegate Control dialog box, click **Browse**.
- Step 7** Specify the service account name, depending on the Exchange version:

Exchange 2003	<p>a. In the Select Users, Computers, or Groups dialog box, in the Enter the Object Name to Select field, enter the user logon name for the account created in “To Create the AD Service Account that Cisco Unity Connection Uses to Access Exchange Data” procedure on page 4-3.</p> <p>b. Click Check Names.</p> <p>c. Click OK to close the Select Users, Computers, or Groups dialog box. The account you selected appears in the Group (Recommended) or User box.</p>
Exchange 2000	<p>a. In the Select Users, Computers, or Groups dialog box, in the Look In list, click the name of the domain in which you created the account in the “To Create the AD Service Account that Cisco Unity Connection Uses to Access Exchange Data” procedure on page 4-3.</p> <p>b. In the list of users, computers, and groups, double-click the name of the service account.</p> <p>The Delegate Control dialog box reappears. The account you selected appears in the Group (Recommended) or User box.</p>

- Step 8** In the Role list, click **Exchange View Only Administrator**.
- Step 9** Click **OK** to close the Delegate Control dialog box.
- Step 10** Click **Next**.
- Step 11** Click **Finish**.
- Step 12** If you selected the organization name at the top of the tree control in [Step 3](#), skip to [Step 13](#).
If you selected an administrative group in [Step 3](#) and you want to access calendar and contact data in mailstores in other administrative groups, repeat [Step 3](#) through [Step 11](#) for each administrative group.
- Step 13** In the left pane of Exchange System Manager, right-click the name of a mailbox store that contains mailboxes in which you want to access calendar and contact data, and click **Properties**.
- Step 14** In the <Server name> Properties dialog box, click the **Security** tab.
- Step 15** Click **Add**.
- Step 16** Specify the service account name, depending on the Exchange version:

Exchange 2003	<p>a. In the Select Users, Computers, or Groups dialog box, in the Enter the Object Names to Select field, enter the name of the service account.</p> <p>b. Click Check Names.</p>
Exchange 2000	<p>a. In the Select Users, Computers, or Groups dialog box, in the Look In list, click the name of the domain in which you created the service account.</p> <p>b. In the list of users, computers, and groups, double-click the name of the service account.</p> <p>The Delegate Control dialog box reappears. The account you selected appears in the Group (Recommended) or User box.</p>

- Step 17** Click **OK** to close the dialog box.
- Step 18** In the Mailbox Store <Server name> Properties dialog box, in the Group or User Names list, click the name of the service account.
- Step 19** In the Permissions For <Account name> list, in the Allow column, check the following three check boxes:
- Administer Information Store
 - Receive As
 - Send As
- Do not change any other permissions.
- Step 20** Click **OK** to close the Mailbox Store <Server name> Properties dialog box.
- Step 21** Repeat [Step 13](#) through [Step 20](#) for each additional Exchange server on which you want to access Exchange data.
- Step 22** Close Exchange System Manager.

Creating and Installing SSL Certificates

In this section, you create and install an SSL certificate on each additional Exchange server on which you want to access calendar and contact data. This prevents Cisco Unity Connection from sending the credentials of the service account that you created in the [“Creating the AD Service Account that Connection Uses to Access Exchange Data”](#) section on page 4-3 over the network as unencrypted text. It also prevents Exchange from sending calendar and contact data over the network in unencrypted text.

If you do not create and install SSL certificates, Cisco Unity Connection may still send service account credentials in an encrypted format, depending on whether you have configured one or more authentication schemes in Exchange. However, the available Exchange authentication schemes encrypt only the user name and password, not calendar and contact data, and Exchange documentation indicates that the available schemes provide varying degrees of security. We recommend that you create and install SSL certificates.



Caution

Cisco Unity Connection does not support Passport authentication.

If you use another method to create and install certificates, use the applicable documentation.

This section contains four procedures. Do them in the order listed.

Do the following procedure on any server in the same domain as the Exchange servers that contain calendar and contact data that you want Connection users to be able to access.

To Install the Microsoft Certificate Services Component

-
- Step 1** Locate either a Windows Server 2003 disc or the Cisco Unity Connection disc, which you may be prompted to insert into the DVD drive to complete the installation of the Microsoft Certificate Services component.
 - Step 2** Log on to Windows by using an account that is a member of the local Administrators group.
 - Step 3** On the Windows Start menu, click **Settings > Control Panel > Add or Remove Programs**.
 - Step 4** In the left pane of the Add or Remove Programs control panel, click **Add/Remove Windows Components**.
 - Step 5** In the Windows Components dialog box, check the **Certificate Services** check box. Do not change any other items.
 - Step 6** When the warning appears about not being able to rename the computer or to change domain membership, click **Yes**.
 - Step 7** Click **Next**.
 - Step 8** On the CA Type page, click **Stand-alone Root CA**, and click **Next**. (A stand-alone certification authority (CA) is a CA that does not require Active Directory.)
 - Step 9** On the CA Identifying Information page, in the Common Name for This CA field, enter a name for the certification authority.
 - Step 10** Accept the default value in the Distinguished Name Suffix field.
 - Step 11** For Validity Period, accept the default value of **5 years**.
 - Step 12** Click **Next**.

- Step 13** On the Certificate Database Settings page, click **Next** to accept the default values.
- If a message appears indicating that Internet Information Services is running on the computer and must be stopped before proceeding, click **Yes** to stop the services.
- Step 14** If you are prompted to insert the Windows Server 2003 disc into the drive, insert either the Windows Server 2003 disc or the Cisco Unity Connection disc, which contains the same required software.
- Step 15** In the Completing the Windows Components Wizard dialog box, click **Finish**.
- Step 16** Close the Add or Remove Programs control panel.
-

Do the following procedure on each additional Exchange server that contains calendar and contact data that you want Connection users to be able to access.

To Create a Certificate Signing Request

- Step 1** Log on to Windows by using an account that is a member of the Domain Admins group.
- Step 2** On the Windows Start menu, click **Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
- Step 3** If the server is running Exchange Server 2003, on the Windows Start menu, click **Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
- If the server is running Exchange 2000 Server, on the Windows Start menu, click **Programs > Administrative Tools > Internet Services Manager**.
- Step 4** In the left pane of Internet Information Services, expand the name of this Exchange server.
- Step 5** If the server is running Exchange 2000 Server, skip to [Step 6](#).
- If the server is running Exchange Server 2003, expand **Web Sites**.
- Step 6** Right-click **Default Web Site**, and click **Properties**.
- Step 7** In the Default Web Site Properties dialog box, click the **Directory Security** tab.
- Step 8** Under Secure Communications, click **Server Certificate**.
- Step 9** On the Welcome to the Web Server Certificate Wizard page, click **Next**.
- Step 10** Click **Create a New Certificate**.
- Step 11** Click **Next**.
- Step 12** Click **Prepare the Request Now, But Send It Later**.
- Step 13** Click **Next**.
- Step 14** Enter a name for the certificate, and accept the default bit length.
- Step 15** Click **Next**.
- Step 16** Enter the organization information.
- Step 17** Click **Next**.

Step 18 For the common name of the site, enter either the computer name or the fully qualified domain name of the Exchange server.

Remember whether you specified the computer name or the fully qualified domain name. You will need this information in a later procedure.

**Caution**

The name must exactly match the host portion of any URL that will access the system by using a secure connection.

Step 19 Click **Next**.

Step 20 On the Geographical Information page, enter the applicable information.

Step 21 Click **Next**.

Step 22 On the Certificate Request File Name page, enter a path and file name, and write down the information. You will need it in a later procedure.

If this is not the server on which you installed Microsoft Certificate Services in the “[To Install the Microsoft Certificate Services Component](#)” procedure on page 4-6, try to choose a network location that you can access from the current server and from the server on which Microsoft Certificate Services is installed.

Step 23 Click **Next**.

Step 24 On the Request File Summary page, verify the request file information.

Step 25 Click **Next**.

Step 26 On the Completing the Web Server Certificate Wizard page, click **Finish**.

Step 27 Click **OK** to close the Default Web Site Properties dialog box.

Step 28 Close Internet Information Services Manager.

Step 29 If Microsoft Certificate Services is on another server and you were not able to save the certificate request file in a network location accessible to that server, copy the certificate request file to a removable medium (diskette, CD, or DVD).

Step 30 Repeat [Step 1](#) through [Step 29](#) to create a certificate signing request for each additional Exchange server that contains calendar and contact data that you want Connection users to be able to access.

Step 31 If you are not using an external certification authority, you are finished with this procedure.

If you are using an external certification authority, send the certificate request files to the CA. When the certificates return from the CA, skip to the “[To Install the Certificate](#)” procedure on page 4-10.

Do the following procedure for each additional Exchange server that contains calendar and contact data that you want Connection users to be able to access.

To Issue the Certificate (Only When You Are Using Microsoft Certificate Services to Issue the Certificate)

Step 1 On the server on which you installed Microsoft Certificate Services, log on to Windows by using an account that is a member of the Domain Admins group.

Step 2 On the Windows Start menu, click **Programs > Administrative Tools > Certification Authority**.

- Step 3** In the left pane, expand **Certification Authority (Local) > <Certification authority name>**, where <Certification authority name> is the name that you gave to the certification authority when you installed Microsoft Certificate Services in the [“To Install the Microsoft Certificate Services Component” procedure on page 4-6](#).
- Step 4** Right-click the name of the certification authority, and click **All Tasks > Submit New Request**.
- Step 5** In the Open Request File dialog box, browse to the location of the first certificate signing request file that you created in the [“To Create a Certificate Signing Request” procedure on page 4-7](#), and double-click the file.
- Step 6** In the left pane of Certification Authority, click **Pending Requests**.
- Step 7** Right-click the pending request that you submitted in [Step 5](#), and click **All Tasks > Issue**.
- Step 8** In the left pane of Certification Authority, click **Issued Certificates**.
- Step 9** Right-click the new certificate, and click **Open**.
- Step 10** In the Certificate dialog box, click the **Details** tab.
- Step 11** Click **Copy to File**.
- Step 12** On the Welcome to the Certificate Export Wizard page, click **Next**.
- Step 13** On the Export File Format page, click **Base-64 Encoded X.509 (.CER)**.
- Step 14** Click **Next**.
- Step 15** On the File to Export page, click **Browse**.
- Step 16** In the Save As dialog box, choose a location and enter a file name.
- If this is not a server on which Internet Information Services Manager is installed, try to choose a network location that you can access from the current server and from the server on which Microsoft Certificate Services is installed.
- Step 17** Write down the path and file name. You will need it in a later procedure.
- Step 18** Click **Save** to close the Save As dialog box.
- Step 19** Click **Next**.
- Step 20** On the Completing the Certificate Export Wizard page, click **Finish**.
- Step 21** Click **OK** to clear the message that indicates that the export was successful.
- Step 22** Click **OK** to close the Certificate dialog box.
- Step 23** If you created more than one certificate signing request in the [“To Create a Certificate Signing Request” procedure on page 4-7](#), repeat [Step 9](#) through [Step 22](#) of this procedure for each certificate signing request listed under Issued Certificates.
- Step 24** Close Certification Authority.
- Step 25** If Internet Information Services Manager is on another server and you were not able to save the certificate request files in a network location accessible to that server, copy the certificate request files to a removable medium (diskette, CD, or DVD).
-

Do the following procedure for each additional Exchange server that contains calendar and contact data that you want Connection users to be able to access.

To Install the Certificate

-
- Step 1** On one of the Exchange servers on which you created a certificate signing request in the “[To Create a Certificate Signing Request](#)” procedure on page 4-7, log on to Windows by using an account that is a member of the Domain Admins group.
- Step 2** On the Windows Start menu, click **Programs > Administrative Tools > Internet Information Services Manager**.
- Step 3** In the left pane, expand the name of this Exchange server.
- Step 4** Right-click **Default Web Site**, and click **Properties**.
- Step 5** In the Default Web Site Properties dialog box, click the **Directory Security** tab.
- Step 6** Under Secure Communications, click **Server Certificate**.
- Step 7** On the Web Server Certificate Wizard Welcome page, click **Next**.
- Step 8** On the Pending Certificate Request page, click **Process the Pending Request and Install the Certificate**.
- Step 9** Click **Next**.
- Step 10** On the Process a Pending Request page, browse to the location where you saved the certificates, and specify the applicable file, depending on the CA that you used:

Sent the certificate request to an external CA	Specify the file that you got from the external CA.
Issued the certificate using the Windows Certification Authority application	Specify the file that you created in Step 9 through Step 22 of the “ To Issue the Certificate (Only When You Are Using Microsoft Certificate Services to Issue the Certificate) ” procedure on page 4-8.

You may have to change the value of the Files of Type list to All Files (*.*) to see the certificates.

- Step 11** On the Certificate Summary page, verify the certificate information.
- Step 12** Click **Next**.
- Step 13** On the Completing the Web Server Certificate Wizard page, click **Finish** to exit the Web Server Certificate wizard.
- Step 14** Click **OK** to close the Default Web Site Properties dialog box.
- Step 15** Restart IIS:
- In the left pane of Internet Information Services Manager, right-click the name of this Exchange server, and click **Restart IIS**.
 - In the Stop/Start/Restart dialog box, click **Restart Internet Services on <Server name>**.
 - Click **OK**.
 - Close Internet Information Services Manager.
- Step 16** Repeat [Step 1](#) through [Step 15](#) for each certificate that you want to install.
-

Creating Connection External Services to Specify the Exchange Servers That Users Can Access

In Cisco Unity Connection Administration, you create and configure one WebDav external service for each additional Exchange server that contains calendar and contact data that you want Connection users to be able to access.

To Create Connection External Services to Specify the Exchange Servers That Users Can Access

-
- Step 1** In Cisco Unity Connection Administration, expand **System Settings**, then click **External Services**.
- Step 2** Click **Add New**.
- Step 3** In the Type list, click **WebDav Service**.
- Step 4** In the Display Name field, enter a name that will help you identify the service when you configure Connection users to access their calendar and contact information. (For example, in the name of the service, you might include the name of the Exchange server that contains the calendar and contact data users are accessing.)
- Step 5** In the Server Base URL field, enter the URL for the Exchange server that contains calendar and contact data that you want Connection users to be able to access. Use the format **https://<Exchange server>/Exchange/** where <Exchange server> is the computer name, the fully qualified domain name, or the IP address of the Exchange server.

If you enter the computer name or the fully qualified domain name of the Exchange server, the value that you enter for <Exchange server> must exactly match the value that you entered in [Step 18](#) of the “[To Create a Certificate Signing Request](#)” procedure on page 4-7.



Caution

If you enter **http** instead of **https**, and if you do the procedure in the “[Requiring Secure Communication Between Connection and Exchange \(Optional But Recommended\)](#)” section on page 4-13, attempts to transfer calendar and contact data from Exchange to Cisco Unity Connection will fail. If you enter **http** instead of **https**, and if you do not do the procedure in that section, calendar and contact data will not be encrypted before it is transferred from Exchange to Cisco Unity Connection.

-
- Step 6** Confirm that the **Access Enabled** check box is checked.
- Step 7** In the Service Login field, enter the Active Directory user logon name of the service account that you created in the “[To Create the AD Service Account that Cisco Unity Connection Uses to Access Exchange Data](#)” procedure on page 4-3. Use the format **<Domain name>\<Account name>**.
- Note the “\” between <Domain name> and <Account name>. If you use a “/”, the WebDav service will not work.
- Step 8** In the Service Password field, enter the password for the service account.
- Step 9** Click **Save**.
- Step 10** If you have created external services for all of the Exchange servers that you want to allow users to access, skip the rest of this procedure.
- If you want users to be able to access additional Exchange servers, on the External Service menu, click **New External Service**.
- Step 11** Repeat [Step 3](#) through [Step 10](#) until you have created all of the required external services.
-

Configuring the Connection Server to Trust Exchange Certificates

To make the Cisco Unity Connection server trust the certificates for the additional Exchange servers, you need to add the certification authority's signing certificate to the root certificate store for the Connection server.

To Configure the Cisco Unity Connection Server to Trust Exchange Certificates

-
- Step 1** On the server on which you installed certification authority, log on to Windows by using an account that is a member of the local Administrators group.
 - Step 2** On the Windows Start menu, click **Programs > Administrative Tools > Certification Authority**.
 - Step 3** In the left pane, expand **Certification Authority (Local)**.
 - Step 4** Right-click the name of the certification authority, and click **Properties**.
 - Step 5** In the <Certification authority name> Properties dialog box, on the General tab, in the CA Certificates list, click the name of one of the certificates that you created for the Exchange servers.
 - Step 6** Click **View Certificate**.
 - Step 7** In the Certificate dialog box, click the **Details** tab.
 - Step 8** Click **Copy to File**.
 - Step 9** On the Welcome to the Certificate Export Wizard page, click **Next**.
 - Step 10** On the Export File Format page, click **Base-64 Encoded X.509 (.CER)**.
 - Step 11** Click **Next**.
 - Step 12** On the File to Export page, enter a temporary path and file name of the certificate export file (for example, c:\cacert.cer).
 - Step 13** Click **Next**.
 - Step 14** On the Completing the Certificate Export Wizard page, click **Finish**.
 - Step 15** Click **OK** to close the "Export successful" message box.
 - Step 16** Click **OK** to close the Certificate dialog box.
 - Step 17** Click **OK** to close the <Server name> Properties dialog box.
 - Step 18** Close **Certification Authority**.
 - Step 19** Copy the certificate export file that you specified in [Step 12](#) to the Connection server, and save it in the Utilities directory on the drive where Connection software is installed (usually drive G).
 - Step 20** On the Windows Start menu, click **Programs > Accessories > Command Prompt**.
 - Step 21** Change to the **Utilities** directory.
 - Step 22** Run the following command, where <Certificate export file.cer> is the name of the certificate export file that you created in [Step 12](#):

```
certmgr /add /c <certificate export file.cer> /r localMachine /s root
```

Note that the name of the application is certmgr, not CuCertMgr, which is in the same directory.

Requiring Secure Communication Between Connection and Exchange (Optional But Recommended)

Several of the procedures earlier in this chapter help to secure, by encryption, the calendar and contact data that is transferred from Exchange to Cisco Unity Connection. However, if you specified an http URL instead of an https URL when you did the procedure in the “[Creating Connection External Services to Specify the Exchange Servers That Users Can Access](#)” section on page 4-11, the data is not encrypted before it is sent over the network.

Do the following procedure on each additional Exchange server so that if a Connection administrator accidentally specifies an http URL when updating the list of Exchange servers that users can access, any attempt to transfer unencrypted Exchange data will fail. However, note that this is a global setting. For every Exchange server on which you have done this procedure, all web clients that access Exchange data on that server will be required to use an https URL.

To Configure Exchange to Require Secure Communication with Connection

-
- Step 1** Confirm that no other applications will be affected when Internet Information Services is configured to require Web clients to use https URLs to access Exchange data.
 - Step 2** Log on to an Exchange server that contains mailboxes from which Cisco Unity Connection users want to import calendars or contacts.
 - Step 3** If the server is running Exchange Server 2003, on the Windows Start menu, click **Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
If the server is running Exchange 2000 Server, on the Windows Start menu, click **Programs > Administrative Tools > Internet Services Manager**.
 - Step 4** In the left pane of Internet Information Services, expand the name of this Exchange server.
 - Step 5** If the server is running Exchange 2000 Server, skip to [Step 6](#).
If the server is running Exchange Server 2003, expand **Web Sites**.
 - Step 6** Right-click **Default Web Site**, and click **Properties**.
 - Step 7** In the Default Web Site Properties dialog box, click the **Directory Security** tab.
 - Step 8** Under Secure Communications, click **Edit**.
 - Step 9** In the Secure Communications dialog box, check the **Require Secure Channel (SSL)** check box.
 - Step 10** Click **OK** to close the Secure Communications dialog box.
 - Step 11** Click **OK** to close the Default Web Site Properties dialog box.
 - Step 12** Close Internet Information Services.
 - Step 13** If you are prompted to turn on this setting for child nodes, select the child nodes on which you want to enable this setting and click **OK**.
 - Step 14** Repeat [Step 1](#) through [Step 13](#) on each additional Exchange server that contains mailboxes from which Cisco Unity Connection users want to import calendar or contact data.
-

Updating or Creating Connection User External Service Accounts to Access the Additional Exchange Servers

In this section you update existing external service accounts for each Cisco Unity Connection user—or create new accounts—to allow users to access calendar and contact data on the additional Exchange servers. It assumes the following conditions have been met:

- The Connection user accounts to which you want to give access to calendar and contact data exist.
- The accounts are assigned to a class of service in which the option Allow Users to Use Personal Call Transfer Rules is enabled.

This section contains two procedures. Do the applicable procedure, depending on whether you are updating existing user external service accounts or creating new accounts.

To Update Existing Connection User External Service Accounts to Access the Additional Exchange Servers

- Step 1** In Cisco Unity Connection Administration, expand **Users**.
- Step 2** On the Search Users page, in the Search Results table, click the alias of the applicable user.
If the user does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and click **Find**.
- Step 3** On the Edit User Basics page, on the Edit menu, click **External Service Accounts**.
- Step 4** On the External Service Accounts page, click the name of the external service account that was originally created for Connection access to Exchange calendar and contact data.
If there is more than one external service account, use the account for which the value in the Service Type list is **WebDav**.
- Step 5** Confirm that the value of the Account Login field is the Active Directory user logon name for the user.
- Step 6** Change the value of the Server URL Suffix field to the new Exchange account logon name for the user.
- Step 7** Click **Save**.
- Step 8** Repeat [Step 2](#) through [Step 7](#) for each additional user.
-

To Create New Connection User External Service Accounts to Access the Additional Exchange Servers

- Step 1** In Cisco Unity Connection Administration, expand **Users**.
- Step 2** On the Search Users page, in the Search Results table, click the alias of the applicable user.
If the user does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and click **Find**.
- Step 3** On the Edit User Basics page, on the Edit menu, click **External Service Accounts**.
- Step 4** Click **Add New**.
- Step 5** In the Account Login field, enter the Active Directory user logon name for the user.
- Step 6** In the Service Type list, select **WebDav**.
- Step 7** In the Remote Server list, select the name of the WebDav service.
- Step 8** In the Server URL Suffix field, enter the Exchange account logon name for the user.

Step 9 Click **Save**.

Step 10 Repeat [Step 2](#) through [Step 9](#) for each additional user.



Removing Software

This chapter contains the following sections:

- [Removing Cisco Unity Connection and Voice-Recognition Software from the Connection Server, page A-1](#)
- [Removing Voice-Recognition Software from a Separate Voice-Recognition Server, page A-2](#)

Removing Cisco Unity Connection and Voice-Recognition Software from the Connection Server

**Caution**

Removing Cisco Unity Connection software also deletes all Connection data and all voice messages.

To Remove Cisco Unity Connection and Voice-Recognition Software from the Connection Server

- Step 1** Log on to the Cisco Unity Connection server by using an account that is a member of the local Administrators group.
- Step 2** Back up Cisco Unity Connection by using the Connection Disaster Recovery Backup tool.
To access the Disaster Recovery Backup tool, double-click the **Cisco Unity Tools Depot** icon on the Windows desktop, and expand **Administration Tools**. (To display Help for the tool, click **Disaster Recovery Backup**. To run the tool, double-click **Disaster Recovery Backup**.)
- Step 3** In the Windows task bar, right-click the **Cisco Unity Connection** icon, and click **Stop > Cisco Unity Connection**.
- Step 4** On the Windows task bar, click the **Cisco Unity Connection Status** icon.
- Step 5** Click the **Server Roles** tab.
- Step 6** In the right pane, click **Media Service Watcher**.
- Step 7** In the left pane, click **Stop the Server Role**.
- Step 8** On the Windows Start menu, click **Settings > Control Panel > Add or Remove Programs**.
- Step 9** If any Connection languages are installed, remove them before you remove Cisco Unity Connection.
- Step 10** Click **Cisco Unity Connection**.

- Step 11** Click **Remove**.
- Step 12** Follow the on-screen prompts.
-

Removing Voice-Recognition Software from a Separate Voice-Recognition Server

To Remove Voice-Recognition Software from a Separate Voice-Recognition Server

- Step 1** If you are replacing one voice-recognition server with another, reconfigure Cisco Unity Connection to access the new server. Do the procedures in the “Configuring Voice-Recognition Software (Separate Voice-Recognition Server Only)” section in the “Configuring Software on the Server, and Installing a Service Release” chapter of the *Cisco Unity Connection Installation Guide* at http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html.
- Step 2** Log on to the voice-recognition server by using an account that is a member of the local Administrators group.
- Step 3** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
- Step 4** Click **Nuance Watcher Daemon**.
- Step 5** Click **Stop the Service**.
- Step 6** Close the Services MMC.
- Step 7** On the Windows Start menu, click **Settings > Control Panel > Add or Remove Programs**.
- Step 8** Click **Cisco Unity Connection**.
- Step 9** Click **Remove**.
- Step 10** Follow the on-screen prompts.
-



INDEX

A

access

- to Cisco Unity Inbox web tool, adding (task list) [3-1](#)
- to Exchange data on additional servers, configuring Connection (task list) [4-2](#)
- to Exchange e-mails through TTS, adding (task list) [3-1](#)

adding

- Exchange servers to which Connection access to Exchange data is configured (task list) [4-2](#)
- licensed features (task list) [3-1](#)

C

calendar and contact data

- configuring Connection access to Exchange on additional servers (task list) [4-2](#)
- moving Exchange mailboxes between servers to which Connection access to Exchange is configured [4-1](#)

Cisco Security Agent for Cisco Unity

- downloading Server Updates wizard for latest version of [1-4](#)
- installing [1-6](#)
- uninstalling [1-6](#)

Cisco Unity, migrating from 4.0(5) or later to shipping version of Cisco Unity Connection [2-1](#)

Cisco Unity Connection Disaster Recovery tools. *See* Disaster Recovery tools

Cisco Unity Connection server

- removing Connection and voice-recognition software from [A-1](#)
- upgrading Connection software on [1-7](#)
- upgrading Connection software to shipping version (task list) [1-2](#)

Cisco Unity Connection Server Updates wizard. *See* Server Updates wizard

Cisco Unity Connection software

- downloading [1-5](#)
- removing from Connection server [A-1](#)
- upgrading on Connection server [1-7](#)
- upgrading to shipping version on Connection server (task list) [1-2](#)

configuring Connection access to Exchange data on additional servers (task list) [4-2](#)

conventions, documentation [v](#)

D

DiRT. *See* Disaster Recovery tools

Disaster Recovery tools, downloading [1-5](#)

documentation conventions [v](#)

downloading

- Cisco Unity Connection languages [1-5](#)
- Cisco Unity Connection service release [1-5](#)
- Cisco Unity Connection software [1-5](#)
- Disaster Recovery tools [1-5](#)
- recommended Microsoft service packs [1-6](#)
- Server Updates wizard [1-4](#)
- software for upgrade [1-4](#)

E

Exchange

- adding servers to which Connection access to Exchange data is configured (task list) [4-2](#)
- moving mailboxes between servers to which Connection access to Exchange data is configured [4-1](#)

I

IMAP client access to Connection voice messages, adding (task list) [3-1](#)

installing

Cisco Security Agent for Cisco Unity [1-6](#)

license files for additional features [3-2](#)

Microsoft updates [1-6](#)

recommended Microsoft service packs [1-6](#)

See also reinstalling *and* upgrading

L

languages

downloading Cisco Unity Connection [1-5](#)

reinstalling [1-8](#)

licensed features, adding (task list) [3-1](#)

license files, obtaining and installing for additional features [3-2](#)

M

Microsoft updates, downloading Server Updates wizard for latest version of [1-4](#)

migrating from Cisco Unity 4.0(5) or later to shipping version of Cisco Unity Connection [2-1](#)

moving Exchange mailboxes between servers to which Connection access to Exchange data is configured [4-1](#)

O

obtaining license files for additional features [3-2](#)

P

ports. *See* voice messaging ports

R

reinstalling Cisco Unity Connection languages [1-8](#)

removing

Cisco Unity Connection and voice-recognition software from Connection server [A-1](#)

voice-recognition software from separate voice-recognition server [A-2](#)

S

server. *See* Cisco Unity Connection server *or* voice-recognition server

Server Updates wizard, downloading [1-4](#)

service packs

downloading recommended Microsoft [1-6](#)

installing recommended Microsoft [1-6](#)

service release, downloading Cisco Unity Connection [1-5](#)

software

downloading Cisco Unity Connection [1-5](#)

downloading Cisco Unity Connection languages [1-5](#)

downloading Cisco Unity Connection service release [1-5](#)

downloading Disaster Recovery tools [1-5](#)

downloading for upgrade [1-4](#)

downloading recommended Microsoft service packs [1-6](#)

downloading Server Updates wizard [1-4](#)

installing Cisco Security Agent for Cisco Unity [1-6](#)

installing Microsoft updates [1-6](#)

installing recommended Microsoft service packs [1-6](#)

reinstalling Cisco Unity Connection languages [1-8](#)

upgrading Cisco Unity Connection on Connection server [1-7](#)

upgrading Cisco Unity Connection to shipping version on Connection server (task list) [1-2](#)

upgrading voice-recognition on separate voice-recognition server [1-7](#)

upgrading voice-recognition on separate voice-recognition server (task list) [1-3](#)

U

uninstalling

Cisco Security Agent for Cisco Unity [1-6](#)

See also removing

updates, installing Microsoft [1-6](#)

upgrading

Cisco Unity Connection software on Connection server [1-7](#)

Cisco Unity Connection software to shipping version on Connection server (task list) [1-2](#)

voice-recognition software on separate voice-recognition server [1-7](#)

voice-recognition software to shipping version on separate voice-recognition server (task list) [1-3](#)

users, adding licensed (task list) [3-1](#)

V

voice messaging ports, adding (task list) [3-1](#)

voice recognition, adding (task list) [3-1](#)

voice-recognition server

upgrading voice-recognition software on [1-7](#)

upgrading voice-recognition software to shipping version (task list) [1-3](#)

voice-recognition software

removing from separate voice-recognition server [A-1, A-2](#)

upgrading on separate voice-recognition server [1-7](#)

upgrading to shipping version on separate voice-recognition server (task list) [1-3](#)

