User Workstation Setup Guide for Cisco Unity Connection

Release 10.x
Published November 2013

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

Text Part Number:

CONTENTS

Preface

Audience and Use

The *User Workstation Setup Guide for Cisco Unity Connection* contains information and instructions that system administrators can use for setting up user workstation access to Cisco Unity Connection web tools, for configuring email accounts to access Unity Connection voice messages, and for conducting orientation sessions for users.

Documentation Conventions

Table 1   *Conventions in the User Workstation Setup Guide for Cisco Unity Connection*

Convention	Description
boldfaced text	Boldfaced text is used for: • Key and button names. (Example: Select **OK**.) • Information that you enter. (Example: Enter **Administrator** in the Username box.)
< > (angle brackets)	Angle brackets are used around parameters for which you supply a value. (Example: In your browser, go to **https://<Cisco Unity Connection server IP address>/cuadmin**.)
- (hyphen)	Hyphens separate keys that must be pressed simultaneously. (Example: Press **Ctrl-Alt-Delete**.)
> (right angle bracket)	A right angle bracket is used to separate selections that you make in the navigation bar of Cisco Unity Connection Administration. (Example: In Cisco Unity Connection Administration, expand **Contacts > System Contacts**.)

The *User Workstation Setup Guide for Cisco Unity Connection* also uses the following conventions:

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

$\mathcal{P}$

Tip Means the following information may help you solve a problem.

⚠

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

Cisco Unity Connection Documentation

For descriptions and URLs of Cisco Unity Connection documentation on Cisco.com, see the *Documentation Guide for Cisco Unity Connection Release 10.x*. The document is shipped with Unity Connection and is available at
http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/roadmap/10xcucdg.html.

Documentation References to Cisco Unified Communications Manager Business Edition

In the Cisco Unity Connection 10.x documentation set, references to "Cisco Unified Communications Manager Business Edition" and "Cisco Unified CMBE" apply to both Business Edition version 10.0.

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.

Cisco Product Security Overview

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

Further information regarding U.S. export regulations can be found at
http://www.access.gpo.gov/bis/ear/ear_data.html.

CHAPTER 1

Setting Up Access to the Cisco Personal Communications Assistant in Cisco Unity Connection

The Cisco Personal Communications Assistant (PCA) is installed on the Cisco Unity Connection server during installation. It is a website that provides users with access to the Cisco Unity web tools, which allow users to manage messages and personal preferences in Unity Connection. The web tools available in the Cisco PCA include:

- Cisco Unity Connection Messaging Assistant
- Cisco Unity Connection Personal Call Transfer Rules

To learn more about the tools listed above, see the applicable *User Guide for Cisco Unity Connection* and the Help for each tool.

See the following sections:

- Configuring a Web Browser to Access the Cisco PCA in Cisco Unity Connection, page 1-1
- Changing the GUI Language for the Cisco PCA in Cisco Unity Connection, page 1-3
- Managing Security Alerts When Using Self-Signed Certificates with SSL Connections in Cisco Unity Connection, page 1-3

Configuring a Web Browser to Access the Cisco PCA in Cisco Unity Connection

The browsers on each user workstation must be set up to use the Cisco PCA and the Cisco Unity Connection web tools. See the applicable section, depending on the browser installed on the computer:

- Apple Safari, page 1-2
- Microsoft Internet Explorer, page 1-2
- Mozilla Firefox, page 1-2

(For the list of versions supported for each browser, see the *Compatibility Matrix: Cisco Unity Connection and the Software on User Workstations*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/compatibility/matrix/cucclientmtx.html .)

Apple Safari

Do the following tasks to set up Safari for accessing the Cisco PCA.

1. Confirm that the software required for correct browser configuration is installed. See the "Software Requirements—User Workstations" section of the *System Requirements for Cisco Unity Connection Release 10.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/requirements/10xcucsysreqs.html.

2. Configure Safari:

   a. Enable Java.

   b. Enable Java Script.

   c. Accept cookies only from sites that you navigate to.

Microsoft Internet Explorer

Do the following tasks to set up Internet Explorer for accessing the Cisco PCA.

1. Confirm that the software required for correct browser configuration is installed. See the "Software Requirements—User Workstations" section of the *System Requirements for Cisco Unity Connection Release 10.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/requirements/10xcucsysreqs.html.

2. Configure Internet Explorer:

   a. Enable Active scripting.

   b. Download and run ActiveX controls.

   c. Enable Java scripting.

   d. Accept all cookies.

   e. Automatically check for newer versions of temporary Internet files.

   f. Enable Medium-High privacy.

Mozilla Firefox

Do the following tasks to set up Firefox for accessing the Cisco PCA.

1. Confirm that the software required for correct browser configuration is installed. See the "Software Requirements—User Workstations" section of the *System Requirements for Cisco Unity Connection Release 10.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/requirements/10xcucsysreqs.html.

2. If users are running Firefox on Apple MAC OS X or Microsoft Windows workstations, skip to Task 3.

If users are running Firefox on Linux Red Hat workstations, confirm that they are using the correct sound card by referring to the sound card support matrix on the Alsa-project.org website. (Note that the Java Runtime Environment (JRE) plug-in software uses the Advanced Linux Sound Architecture (ALSA) driver to access system sound devices and to control playback and recording functionality. Depending on the sound card, playback and recording capabilities may be limited.)

3. Configure Firefox:

    a. Enable Java.

    b. Enable Java Script > Enable Change Images in Java Script Advanced.

    c. Allow sites to set cookies. (For security purposes, we recommend that you set this to Allow Sites to Set Cookies for the Originating Web Site Only.)

Changing the GUI Language for the Cisco PCA in Cisco Unity Connection

Do the following tasks to change the GUI language that is used in the Cisco PCA.

1. Download and install the applicable languages. For instructions, see the applicable documentation:

- For a new Unity Connection server, see the "Installing Additional Languages on the Cisco Unity Connection 10.x Server" chapter of the *Installation Guide for Cisco Unity Connection* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/installation/guide/10xcucigx.html.

- For an existing Unity Connection server, see the "Adding or Removing Cisco Unity Connection 10.x Languages" chapter of the *Upgrade Guide for Cisco Unity Connection* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/upgrade/guide/10xcucrugx.html.

2. On the user workstation, select a language in the web browser. The language selected in the browser must be one of the languages that the Cisco PCA offers and it must be installed on the Unity Connection server. For a list of supported languages, see the "Available Languages for Cisco Unity Connection Components" section of the applicable *System Requirements* document:

- *System Requirements for Cisco Unity Connection Release 10.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/requirements/10xcucsysreqs.html

- *System Requirements for Cisco Unity Connection in Cisco Unified CMBE Release 10.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/requirements/10xcucmbesysreqs.html

Managing Security Alerts When Using Self-Signed Certificates with SSL Connections in Cisco Unity Connection

If you use the self-signed certificate generated during installation to provide an SSL Unity Connection to the Cisco PCA, the web browser of the user displays a message to alert the user that the authenticity of the site cannot be verified, and therefore its content cannot be trusted. Similarly, if you use a self-signed SSL certificate to secure IMAP email client access to Unity Connection, some email clients supported for use with Unity Connection display SSL security messages.

Although users can still access Unity Connection despite the alerts, consider one of the following options to manage or eliminate security alerts when users browse to the Cisco PCA and/or access their messages from an IMAP email client:

- Add the SSL certificate to the Trusted Root Store on each user workstation. In this way, you can ensure that users never see the security alert. Do the following "To Add the SSL Certificate to the Trusted Root Store on User Workstations" procedure.

- Tell users to choose the "Accept Permanently" (or similar) option when the browser or email client displays the alert and asks them how to proceed. After instructing the browser and/or email client to always accept the certificate, the user will not see the alert again.

Do the following procedure if you want users to never see the security alert.

To Add the SSL Certificate to the Trusted Root Store on User Workstations

Step 1   From the OS Administration application on the Cisco Unity Connection server, right-click to download the certificate and save it as a file.

Step 2   Copy the certificate to each user workstation, and then import it by using tools in the browser or IMAP client, as applicable.

Setting Up Playback and Recording Devices for the Media Master in Cisco Unity Connection

The Media Master is used to make and play recordings in the Cisco Unity Connection web tools.

See the following sections:

- About the Cisco Unity Connection Media Master, page 2-1
- Determining Which Recording and Playback Devices Users Will Use for the Media Master in Cisco Unity Connection, page 2-2
- How Users Specify Their Recording and Playback Device Preferences in Cisco Unity Connection, page 2-3

About the Cisco Unity Connection Media Master

The Media Master appears on the pages of the Cisco Unity Connection Messaging Inbox and Cisco Unity Connection Personal Call Transfer Rules web tools on which users can make or play recordings. Depending on how Cisco Unity Connection is set up, the Media Master may also appear on some Unity Connection Messaging Assistant pages. Users can use the phone or the computer microphone and speakers with the Media Master controls to make and play recordings. See Figure 2-1.

Figure 2-1 **Media Master**
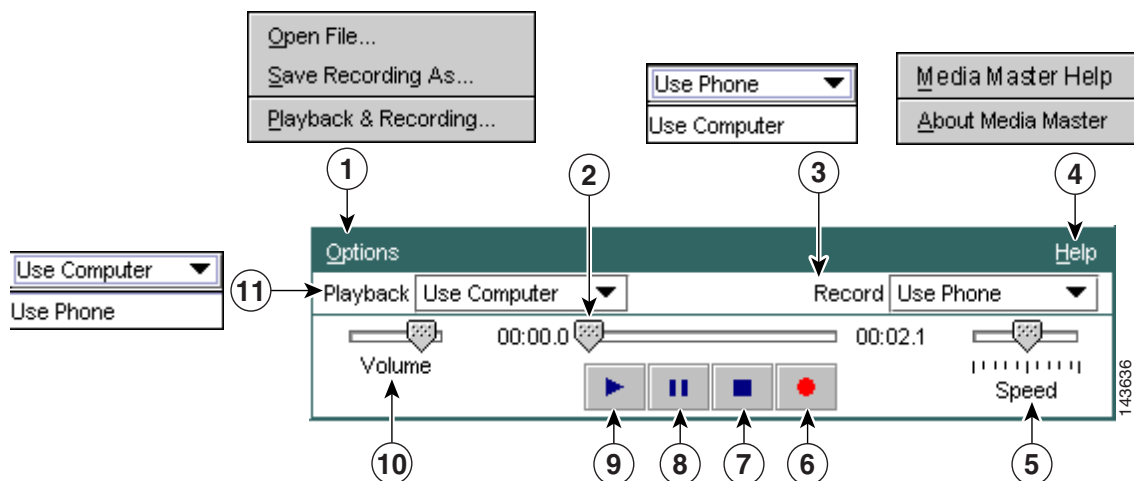
1	Options menu	**7**	Stop
2	Recording/playback progress	**8**	Pause
3	Record list	**9**	Play
4	Help menu	**10**	Volume control
5	Playback speed control	**11**	Playback list
6	Record		

The Media Master is a Java 2 Platform, Standard Edition (J2SE) application, and the Java plug-in component must be installed on the user workstation for it to run properly.

Note Depending on the web browser, if the Java plug-in component is not installed, the Media Master does not appear in the browser window or the user is prompted to install the component. (See the "Configuring a Web Browser to Access the Cisco PCA in Cisco Unity Connection" section on page 1-1.)

Before users start using the Cisco Unity Connection web tools that offer the Media Master, specify that Unity Connection has at least one voice messaging port designated to allow users to use the phone as a recording and playback device, by adjusting the Allow TRAP Connections setting on the Telephony Integrations > Port page in Cisco Unity Connection Administration.

Determining Which Recording and Playback Devices Users Will Use for the Media Master in Cisco Unity Connection

When determining the recording and playback devices that you want users to use, note the following considerations:

- The phone offers the best sound quality for recordings, and serves as the default recording and playback device for the Media Master.

- In order for users to use the phone as a recording and playback device, Cisco Unity Connection must have at least one voice messaging port designated for this purpose. Note that when a user listens to messages or other recordings by using a computer microphone and speakers, no ports are used, which decreases the load on the Unity Connection server and leaves ports open for other functions.

- You must provide sound cards, speakers, and microphones to users who do not want to use the phone as their recording and playback device.

See the following sections for detailed descriptions of the events that occur when using the phone or the computer microphone and speakers for recording and playback:

- What Happens When the Phone Is Used as the Recording and Playback Device, page 2-3

- What Happens When a Computer Microphone and Speakers Are Used as the Recording and Playback Devices, page 2-3

What Happens When the Phone Is Used as the Recording and Playback Device

When users use the phone as a recording and playback device in the web tools that are accessed through the Cisco PCA (and in Cisco Unity Connection Administration), the following events occur:

1. The user selects the applicable option in the client application to make or play a recording.

2. The client application asks Cisco Unity Connection to place a call to the user extension, and Unity Connection calls the extension.

3. When making a recording, the user answers the phone, and begins recording the message, name, or greeting. When the user hangs up, the client application tells Unity Connection that the recording is finished.

4. When playing a recording, the user answers the phone, and the client application asks Unity Connection to play the message. Unity Connection streams the recording by phone.

What Happens When a Computer Microphone and Speakers Are Used as the Recording and Playback Devices

When users use a computer microphone and speakers as the recording and playback devices, the following events occur:

1. The user selects the applicable option in the client application to make or play a recording.

2. When making a recording, the user begins speaking into the microphone. When the user selects the applicable option in the client application to stop recording, the client application tells Cisco Unity Connection that the recording is finished.

3. When playing a recording, Unity Connection streams the message to the client application. Streaming occurs on demand, regardless of network traffic. The client application begins to play the message through the speakers as soon as a few seconds of the message are buffered in memory on the user workstation.

How Users Specify Their Recording and Playback Device Preferences in Cisco Unity Connection

Users can set their own recording and playback device preferences. For example, the Options menu in the Media Master allows users to choose their own recording and playback devices.

Media Master recording and playback settings are saved per user, per workstation. This means that:

*   A user can change recording and playback devices from the Options menu and from both the Playback and Record lists of any Media Master on the web-tool pages. The recording and playback devices that a user chooses apply to all Cisco Unity Connection web tools, as long as the user accesses the applications from the same workstation on which the changes were initially made.

*   If multiple users share the same workstation, each user who uses the workstation must indicate a choice of recording and playback devices.

*   If a user has updated the choice of recording and playback devices from one workstation but also accesses the web tools on a different workstation (for example, from a computer at home), the choice of recording and playback devices must be set for the second workstation as well.

Configuring an Email Account to Access Cisco Unity Connection Voice Messages

Cisco Unity Connection allows licensed users to use a third-party IMAP client to access voice messages from their desktop machines. You can also forward voice messages with text and reply to voice messages with text; the text portion of the message is accessible through the Unity Connection text-to-speech feature.

See the following sections:

Note When users change their Cisco Personal Communications Assistant (PCA) password (also known as the web-application password) in the Unity Connection Messaging Assistant, they also must update the password in their IMAP client application. Passwords are not synchronized between IMAP clients and

the Cisco PCA. If users have trouble receiving voice messages in an IMAP client even after updating their Cisco PCA password in both applications, see the "To create the registry entries for Microsoft Outlook, do the following:" section on page 3-21.

Considerations When Configuring IMAP Email Clients in Cisco Unity Connection

Note the following considerations when configuring IMAP email clients to access Cisco Unity Connection voice messages:

- In Cisco Unity Connection Administration, configure the following settings on the System Settings > SMTP Configuration > Server page to match the SSL settings in the IMAP email clients:
  - Allow Connections From Untrusted IP Addresses
  - Require Authentication From Untrusted IP Addresses
  - Transport Layer Security From Untrusted IP Addresses Is (Disabled, Required, Optional)

- IMAP email clients all include two fields in which you can enter either the IP address or the fully qualified domain name of the Unity Connection server. When a Unity Connection cluster is configured, enter the fully qualified domain name of a DNS A record that includes the Unity Connection publisher and subscriber servers. If your DNS server allows you to specify the order in which DNS tries to contact Unity Connection servers, specify that the server that is available most often is the first server contacted. This usually is the publisher server.

  Some IMAP email clients do not respect DNS A records. For those clients, if the first Unity Connection server is not available, the client does not try to access the other Unity Connection server.

- When a user forwards or replies to a voice message from an IMAP email client, the message will be sent to recipients on the Unity Connection server unless the user specifically configures the message to be sent through another account.

Creating and Configuring an Account to Access Cisco Unity Connection in Apple Mail

To use Apple Mail to access Cisco Unity Connection voice messages, create and configure a new Apple Mail account for the user. You need the following information:

- Unity Connection username (alias).
- Cisco Personal Communications Assistant (PCA) password. (This is the web application password that is set on the User pages in Cisco Unity Connection Administration.)
- The IP address, or if DNS is configured, the fully qualified domain name of the Unity Connection server.

To Create and Configure a New Account in Apple Mail

Step 1   Start Apple Mail.

Step 2   In Apple Mail, on the Mail menu, select **Preferences**.

Step 3   At the top of the Preferences dialog box, select **Accounts**.

Step 4   In the lower left corner, select **+**.

Step 5   In the Account Type list, select **IMAP**.

Step 6   In the Description field, enter a name for the account. This name appears only in Apple Mail.

Step 7   In the E-Mail Address field, enter the Unity Connection SMTP Address of the user and the name of the Unity Connection server. You can find this information in the SMTP Address field on the User Basics page in Cisco Unity Connection Administration. The E-Mail Address typically follows this format:

<alias>@<fully qualified domain name of the Unity Connection server>

Step 8   In the Full Name field, enter the username.

Step 9   In the Incoming Mail Server field, enter the IP address or the fully qualified domain name of the Unity Connection server.

⚠️
Caution   Do not use the fully qualified domain name of the Unity Connection server unless DNS is configured for the network.

Step 10   In the User Name field, enter the Unity Connection username.

Step 11   In the Password field, enter the Cisco PCA password.

Step 12   In the Outgoing Mail Server (SMTP) field, select the IP address or the fully qualified domain name of the Unity Connection server.

Step 13   Select **Server Settings**.

Step 14   Optionally, in the SMTP Server Options dialog box, check the **Use Secure Sockets Layer (SSL)** check box.

⚠️
Caution   If you do not configure Apple Mail to use SSL, the Unity Connection username and password that are sent to Unity Connection over the network and the voice messages sent back from Unity Connection are not encrypted.

Step 15   In the Authentication list, select **Password**.

Step 16   Select **OK** to close the SMTP Options dialog box.

Step 17   Select the **Advanced** tab.

Step 18   In the Keep Copies of Messages for Offline Viewing list, select the applicable option.

Step 19   Close the Preferences dialog box.

Step 20   In the Save Changes dialog box, select **Save**.

Creating and Configuring an Account to Access Cisco Unity Connection in Eudora

To use Eudora to access Cisco Unity Connection voice messages, create and configure a new Eudora account for the user. You need the following information:

- Unity Connection username (alias).
- Cisco Personal Communications Assistant (PCA) password. (This is the web application password that is set on the User pages in Cisco Unity Connection Administration.)
- The IP address, or if DNS is configured, the fully qualified domain name of the Unity Connection server.

To Create and Configure a New Account in Eudora

Step 1 Start Eudora.

Step 2 On the Eudora Tools menu, select **Personalities**.

Step 3 Right-click anywhere in the Personalities tab, and select **New**.

Step 4 In the New Account wizard, on the Account Settings page, select **Next** to accept the default value, Create a Brand New E-Mail Account.

Step 5 On the Personality Name page, enter a display name for the account. The value that you enter here is visible only in Eudora.

Step 6 Select **Next**.

Step 7 On the Personal Information page, enter the username.

Step 8 Select **Next**.

Step 9 On the E-Mail Address page, enter the Unity Connection SMTP Address of the user and the name of the Unity Connection server. You can find this information in the SMTP Address field on the User Basics page in Cisco Unity Connection Administration. The E-Mail Address typically follows this format:

<alias>@<fully qualified domain name of the Unity Connection server>

Step 10 Select **Next**.

Step 11 On the User Name page, enter the Unity Connection username.

Step 12 Select **Next**.

Step 13 On the Incoming E-Mail Server page, enter the IP address or the fully qualified domain name of the Unity Connection server.

⚠

Caution   Do not use the fully qualified domain name of the Unity Connection server unless DNS is configured for the network.

Step 14 For the type of server, select **IMAP**.

Step 15 Select **Next**.

Step 16 On the IMAP Location Prefix page, do not enter a value.

Step 17 Select **Next**.

Step 18   On the Outgoing E-Mail Server page, enter the IP address or the fully qualified domain name of the Unity Connection server.

Step 19   Select **Next**.

Step 20   On the Success page, select **Finish** to create the account and close the wizard.

Step 21   In the Enter Password dialog box, enter the Cisco PCA password of the user.

Step 22   Select **OK**.

Step 23   Optionally, configure the new account to use SSL. For more information, see Eudora Help.

> ⚠
> **Caution**   If you do not configure Eudora to use SSL, the Unity Connection username and password that are sent to Unity Connection over the network and the voice messages sent back from Unity Connection are not encrypted.

Creating and Configuring an Account to Access Cisco Unity Connection in IBM Lotus Notes

> ⚠
> **Caution**   If you plan to configure user accounts to use Cisco Unity Connection ViewMail for IBM Lotus Notes, do not follow the instructions in this section. Instead, follow the configuration instructions in the *Release Notes for Cisco Unity Connection ViewMail for IBM Lotus Notes*, available at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.

To use Notes to access Cisco Unity Connection voice messages, create and configure a new Notes account for the user. You need the following information:

- Unity Connection username (alias).
- Cisco Personal Communications Assistant (PCA) password. (This is the web application password that is set on the User pages in Cisco Unity Connection Administration.)
- The IP address, or if DNS is configured, the fully qualified domain name of the Unity Connection server.

> ⚠
> **Caution**   When using Lotus Notes version 7.x to access Unity Connection voice messages, you must first configure Notes to connect to a Domino account before configuring the Unity Connection account.

To Create and Configure a New Account in IBM Lotus Notes

Step 1   Start IBM Lotus Notes.

Step 2   On the Notes File menu, select **Preferences > Client Reconfiguration Wizard**.

Step 3   In the Lotus Notes Client Configuration wizard, on the Additional Services page, check the **Internet Mail Servers (POP or IMAP, SMTP)** check box.

Step 4   Select **Next**.

Step 5 On the Set Up Internet Mail page, in the Select the Type of Server Used for Retrieving Incoming Mail list, select **IMAP**.

Step 6 In the Enter a New Account Name list, select **Incoming Internet Mail**.

Step 7 In the Incoming Mail Server field, enter the IP address or the fully qualified domain name of the Cisco Unity Connection server.

> ⚠️
> **Caution**   Do not use the fully qualified domain name of the Unity Connection server unless DNS is configured for the network.

Step 8 Select **Next**.

Step 9 On the Set Up Internet Mail page, in the Account Name field, enter the Unity Connection SMTP Address of the user and the name of the Unity Connection server. You can find this information in the SMTP Address field on the User Basics page in Cisco Unity Connection Administration. The Account Name typically follows this format:

<alias>@<fully qualified domain name of the Unity Connection server>

Step 10 In the Password fields, enter and confirm the Cisco PCA password of the user.

Step 11 If you want to encrypt voice messages and other data that are sent between Notes and Unity Connection, check the **Log On Using SSL** check box. If not, skip to Step 12.

> ⚠️
> **Caution**   If you do not configure Notes to use SSL, the Unity Connection username and password that are sent to Unity Connection over the network and the voice messages that are sent back from Unity Connection are not encrypted.

Step 12 Select **Next**.

Step 13 On the second Set Up Internet Mail page, in the Enter a New Account Name list, select **Outgoing Internet Mail**.

Step 14 In the Outgoing SMTP Mail Server list, enter the IP address or the fully qualified domain name of the Unity Connection server.

Step 15 Select **Next**.

Step 16 On the third Set Up Internet Mail page, in the E-Mail Address field, enter the Unity Connection alias of the user and the name of the Unity Connection server. Use the following format:

<alias>@<fully qualified domain name of the Unity Connection server>

Step 17 In the Internet Domain field, enter the Internet domain name of the Domino mail server.

Step 18 Select **Next**.

Step 19 Select **OK**.

Creating and Configuring an Account to Access Cisco Unity Connection in Microsoft Outlook

⚠️

Caution   If you plan to configure user accounts to use Cisco ViewMail for Microsoft Outlook, do not follow the instructions in this section. Instead, follow the configuration instructions in the applicable *Release Notes for Cisco ViewMail for Microsoft Outlook*, available at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.

To use Microsoft Outlook to access Cisco Unity Connection voice messages, create and configure a new Microsoft Outlook account for the user. You need the following information:

- Unity Connection username (alias).
- Cisco Personal Communications Assistant (PCA) password. (This is the web application password that is set on the User pages in Cisco Unity Connection Administration.)
- The IP address, or if DNS is configured, the fully qualified domain name of the Unity Connection server.

In addition to configuring Microsoft Outlook to access Unity Connection voice messages, you can also install the optional ViewMail for Outlook plug-in. See the "Creating and Configuring an Account to Access Cisco Unity Connection in Microsoft Outlook Express" section on page 3-9.

To Create and Configure a New Account in Outlook

Step 1   Start Microsoft Outlook.

Step 2   On the Microsoft Outlook Tools menu, select **E-Mail Accounts**.

Step 3   In the E-Mail Accounts wizard, select **Add a New E-Mail Account**.

Step 4   Select **Next**.

Step 5   On the Server Type page, select **IMAP**.

Step 6   Select **Next**.

Step 7   Enter values in the User Information section:

    a.   In the Your Name field, enter a display name for the account. The value that you enter here is visible only in Microsoft Outlook.

    b.   In the E-Mail Address field, enter one of the following:

- The Unity Connection SMTP Address of the user and the name of the Unity Connection server. You can find this information in the SMTP Address field on the User Basics page in Cisco Unity Connection Administration. The E-Mail Address typically follows this format:

  <alias>@<SMTP domain name of the Unity Connection server or cluster>

- The proxy address for the user.

Step 8   Enter values in the Server Information Section:

    a.   In the Incoming Server field, enter the IP address or the fully qualified domain name of the Unity Connection server.

> ⚠️
>
> **Caution**   Do not use the fully qualified domain name of the Unity Connection server unless DNS is configured for the network.

    b.   In the Outgoing Server field, select the IP address or the fully qualified domain name of the Unity Connection server.

Step 9   Enter values in the Logon Information section:

    a.   In the User Name field, enter the Unity Connection username.

    b.   In the Password field, enter the Cisco PCA password of the user.

    c.   Verify that the Remember Password check box is not checked. If this option is checked, and the Unity Connection password of the user expires, changes, or is locked, Microsoft Outlook does not prompt the user to enter the Unity Connection password. The result is that users do not receive voice messages from Unity Connection.

Step 10   If you do not want to encrypt voice messages and other data that are sent over the network between Microsoft Outlook and Unity Connection, skip to Step 15.

> ⚠️
>
> **Caution**   If you do not configure Microsoft Outlook to use SSL, the Unity Connection username and password that are sent to Unity Connection over the network and the voice messages sent back from Unity Connection are not encrypted.

If you want to encrypt voice messages and other data that are sent between Microsoft Outlook and Unity Connection, continue with Step 11.

Step 11   Select **More Settings**.

Step 12   In the Internet E-Mail Settings dialog box, select the **Advanced** tab.

Step 13   Under Incoming Server (IMAP), check the **This Server Requires an Encrypted** Unity Connection **(SSL)** check box.

Step 14   Select **OK** to close the Internet E-Mail Settings dialog box.

Step 15   If the Unity Connection SMTP server is configured to allow connections from untrusted IP addresses, skip to Step 21.

If the Unity Connection SMTP server is configured to require authentication from untrusted IP addresses, continue with Step 16.

Step 16   Select **More Settings**.

Step 17   In the Internet E-Mail Settings dialog box, select the **Outgoing Server** tab.

Step 18   Verify that the My Outgoing Server (STMP) Requires Authentication check box is checked.

Step 19   Verify that Use Same Settings as My Incoming Mail is selected.

Step 20   Select **OK** to close the Internet E-Mail Settings dialog box.

Step 21   Select **Next**.

Step 22   Select **Finish**.

Step 23   In the left pane of Microsoft Outlook, select the **Inbox** folder for the new account.

Step 24   On the Microsoft Outlook Tools menu, select **Send/Receive > This Folder**.

Step 25   If prompted, enter the Unity Connection username and Cisco PCA password.

Creating and Configuring an Account to Access Cisco Unity Connection in Microsoft Outlook Express

To use Microsoft Outlook Express to access Cisco Unity Connection voice messages, create and configure a new Microsoft Outlook Express account for the user. You need the following information:

- Unity Connection username (alias).
- Cisco Personal Communications Assistant (PCA) password. (This is the web application password that is set on the User pages in Cisco Unity Connection Administration.)
- The IP address, or if DNS is configured, the fully qualified domain name of the Unity Connection server.

To Create and Configure a New Account in Microsoft Outlook Express

Step 1   Start Microsoft Outlook Express.

Step 2   On the Microsoft Outlook Express Tools menu, select **Accounts**.

Step 3   In the Internet Accounts dialog box, select the **Mail** tab.

Step 4   Select **Add > Mail**, and the Internet Unity Connection wizard appears.

Step 5   On the Your Name page, in the **Display Name** field, enter the username.

Step 6   Select **Next**.

Step 7   On the Internet E-Mail Address page, select **I Already Have an E-Mail Address That I'd Like to Use**.

Step 8   In the **E-Mail Address** field, enter the Unity Connection SMTP Address of the user and the name of the Unity Connection server. You can find this information in the SMTP Address field on the User Basics page in Cisco Unity Connection Administration. The E-Mail Address typically follows this format:

<alias>@<fully qualified domain name of the Unity Connection server>

Step 9   Select **Next**.

Step 10   On the E-Mail Server Names page, in the My Incoming Mail Server Is a <protocol> Server list, select **IMAP**.

Step 11   In the Incoming Mail (POP3, IMAP, or HTTP) Server field, enter the IP address or the fully qualified domain name of the Unity Connection server.

⚠

Caution   Do not use the fully qualified domain name of the Unity Connection server unless DNS is configured for the network.

Step 12   In the Outgoing Mail (SMTP) Server field, enter the IP address or the fully qualified domain name of the Unity Connection server.

Step 13   Select **Next**.

Step 14   On the Internet Mail Logon page, in the Account Name and Password fields, enter the Unity Connection username and Cisco PCA password.

Step 15   Verify that the **Remember Password** check box is not checked.

If this option is checked, and the Unity Connection password of the user expires, changes, or is locked, Microsoft Outlook Express does not prompt the user to enter the Unity Connection password. The result is that users do not receive voice messages from Unity Connection.

Chapter 3   Configuring an Email Account to Access Cisco Unity Connection Voice Messages
Creating and Configuring an Account to Access Cisco Unity Connection in Novell GroupWise

Step 16   Select **Next**.

Step 17   On the Congratulations page, select **Finish**.

Step 18   In the Internet Accounts dialog box, select the account that you created in Step 4, and select **Properties**.

Step 19   In the <account name> Properties dialog box, select the **IMAP** tab.

Step 20   Uncheck the **Store Special Folders** check box.

Step 21   In the Root Folder Path field, enter **INBOX** (all upper-case letters).

Step 22   If you do not want to encrypt voice messages and other data that are sent over the network between Microsoft Outlook Express and Unity Connection, skip to Step 25.

> ⚠️
> **Caution**   If you do not configure Microsoft Outlook Express to use SSL, the Unity Connection username and password that are sent to Unity Connection over the network and the voice messages sent back from Unity Connection are not encrypted.

If you want to encrypt voice messages and other data that are sent between Microsoft Outlook Express and Unity Connection, continue with Step 23.

Step 23   Select the **Advanced** tab.

Step 24   Under Incoming Mail, check the **This Server Requires a Secure** Unity Connection **(SSL)** check box.

Step 25   Select **OK** to close the <account name> Properties dialog box.

Step 26   Select **Close** to close the Internet Accounts dialog box.

Creating and Configuring an Account to Access Cisco Unity Connection in Novell GroupWise

To use GroupWise to access Cisco Unity Connection voice messages, create and configure a new GroupWise account for the user. You need the following information:

- Unity Connection username (alias).
- Cisco Personal Communications Assistant (PCA) password. (This is the web application password that is set on the User pages in Cisco Unity Connection Administration.)
- The IP address, or if DNS is configured, the fully qualified domain name of the Unity Connection server.

To Create and Configure a New Account in GroupWise

Step 1   Start GroupWise.

Step 2   On the GroupWise Tools menu, select **Accounts > Account Options**.

Step 3   In the Accounts dialog box, select **Add**.

Step 4   In the Create Account dialog box, in the Account Name field, enter a name for the account. This name appears only in GroupWise.

Step 5   In the Account Type list, select **IMAP4**.

Step 6   Select **Next**.

User Workstation Setup Guide for Cisco Unity Connection Release 10.x

3-10

Step 7 In the Create Internet Account dialog box, in the **Incoming Mail Server (IMAP4)** field, enter the IP address or the fully qualified domain name of the Unity Connection server.

⚠️

Caution Do not use the fully qualified domain name of the Unity Connection server unless DNS is configured for the network.

Step 8 In the Login Name field, enter the Unity Connection username.

Step 9 In the Outgoing Server field, enter the IP address or the fully qualified domain name of the Unity Connection server.

Step 10 In the E-Mail Address field, enter the Unity Connection SMTP Address of the user and the name of the Unity Connection server. You can find this information in the SMTP Address field on the User Basics page in Cisco Unity Connection Administration. The E-Mail Address typically follows this format:

<alias>@<fully qualified domain name of the Unity Connection server>

Step 11 In the From Name field, enter the username.

Step 12 Select **Next**.

Step 13 Follow the on-screen prompts to complete the configuration.

Step 14 If you do not want to encrypt voice messages and other data that are sent over the network between GroupWise and Unity Connection, skip to Step 20.

⚠️

Caution If you do not configure GroupWise to use SSL, the Unity Connection username and password that are sent to Unity Connection over the network and the voice messages sent back from Unity Connection are not encrypted.

If you want to encrypt voice messages and other data that are sent between GroupWise and Unity Connection, continue with Step 15.

Step 15 In the Accounts dialog box, select the name of the account that you just created.

Step 16 Select **Properties**.

Step 17 Select the **Advanced** tab.

Step 18 Under Incoming Mail Server (IMAP4), check the **Use SSL** check box.

Step 19 Select **OK** to close the <Account Name> Properties dialog box.

Step 20 Select **Close** to close the Accounts dialog box.

Step 21 Create the inbox for the new account, and download Unity Connection voice messages:

   a. In the left pane of GroupWise, select the name of the new account.

   b. In the Logon to <AccountName> dialog box, enter the Cisco PCA password for the user.

   c. Verify that the **Remember Password** check box is not checked.

   If this option is checked, and the Unity Connection password of the user expires, changes, or is locked, GroupWise does not prompt the user to enter the Unity Connection password. The result is that users do not receive voice messages from Unity Connection.

   d. Select **OK** to close the Logon to <AccountName> dialog box.

   e. With the name of the new account still selected in the left pane, on the GroupWise Tools menu, select **Send/Receive > This Folder**.

Creating and Configuring an Account to Access Cisco Unity Connection in Opera

To use Opera to access Cisco Unity Connection voice messages, create and configure a new Opera account for the user. You need the following information:

- Unity Connection username (alias).

- Cisco Personal Communications Assistant (PCA) password. (This is the web application password that is set on the User pages in Cisco Unity Connection Administration.)

- The IP address, or if DNS is configured, the fully qualified domain name of the Unity Connection server.

To Create and Configure a New Account in Opera

Step 1   Start Opera.

Step 2   On the Opera Tools menu, select **Mail and Chat Accounts**.

Step 3   In the Manage Accounts dialog box, select **New**.

Step 4   In the New Account wizard, select **IMAP**.

Step 5   Select **Next**.

Step 6   In the Real Name field, enter the account name.

Step 7   In the E-Mail Address field, enter the Unity Connection SMTP Address of the user and the name of the Unity Connection server. You can find this information in the SMTP Address field on the User Basics page in Cisco Unity Connection Administration. The E-Mail Address typically follows this format:

<alias>@<fully qualified domain name of the Unity Connection server>

Step 8   In the Organization field, enter the applicable value.

Step 9   Select **Next**.

Step 10   In the Login Name field, enter the Unity Connection username.

Step 11   In the Password field, enter the Cisco PCA password.

Step 12   Select **Next**.

Step 13   In the Incoming Server field, enter the IP address or the fully qualified domain name of the Unity Connection server.

⚠

Caution   Do not use the fully qualified domain name of the Unity Connection server unless DNS is configured for the network.

Step 14   If you want to encrypt voice messages and other data that are sent between Opera and Unity Connection, check the Use Secure Unity Connection (TLS) check box. (TLS is an updated version of SSL.)

⚠

Caution   If you do not configure Opera to use SSL, the Unity Connection username and password that are sent to Unity Connection over the network and the voice messages sent back from Unity Connection are not encrypted.

Step 15 In the Outgoing Server field, enter the IP address or the fully qualified domain name of the Unity Connection server.

Step 16 Select **Finish**.

Step 17 Select **OK** to close the Subscribe IMAP Folders dialog box.

Step 18 Select **OK** to close the Manage Accounts dialog box.

Creating and Configuring an Account to Access Cisco Unity Connection in Thunderbird

To use Thunderbird to access Cisco Unity Connection voice messages, create and configure a new Thunderbird account for the user. You need the following information:

- Unity Connection username (alias).
- Cisco Personal Communications Assistant (PCA) password. (This is the web application password that is set on the User pages in Cisco Unity Connection Administration.)
- The IP address, or if DNS is configured, the fully qualified domain name of the Unity Connection server.

To Create and Configure a New Account in Thunderbird

Step 1 Start Thunderbird.

Step 2 On the Thunderbird File menu, select **New > Account**.

Step 3 In the Account wizard, on the New Account Setup page, select **E-Mail Account**.

Step 4 Select **Next**.

Step 5 On the Identity page, in the Your Name field, enter the username.

Step 6 In the E-Mail Address field, enter the Unity Connection SMTP Address of the user and the name of the Unity Connection server. You can find this information in the SMTP Address field on the User Basics page in Cisco Unity Connection Administration. The E-Mail Address typically follows this format:

<alias>@<fully qualified domain name of the Unity Connection server>

Step 7 Select **Next**.

Step 8 On the Server Information page, under Select the Type of Incoming Server You Are Using, select **IMAP**.

Step 9 In the Incoming Server field, enter the IP address or the fully qualified domain name of the Unity Connection server.

⚠️

Caution Do not use the fully qualified domain name of the Unity Connection server unless DNS is configured for the network.

Step 10 Select **Next**.

Step 11 On the User Names page, enter the Unity Connection username.

Step 12 Select **Next**.

Step 13 On the Account Name page, enter a name for the account. This name appears only in Thunderbird.

Step 14   Select **Next**.

Step 15   On the Congratulations page, confirm that the settings are correct, then select **Finish**.

Step 16   If you do not want to encrypt voice messages and other data that are sent over the network between Thunderbird and Unity Connection, you are finished creating and configuring a new account.

If you want to encrypt voice messages and other data that are sent between Thunderbird and Unity Connection, continue with Step 17.

Step 17   In the left pane of Thunderbird, select the name of the account that you just created.

Step 18   In the right pane of Thunderbird, under Accounts, select **View Settings for This Account**.

Step 19   In the Account Settings dialog box, under the account that you just created, select **Server Settings**.

Step 20   Under Server Settings, select the **Use Secure** Unity Connection (**SSL**) check box.

> ⚠
> **Caution**   If you do not configure Thunderbird to use SSL, the Unity Connection username and password that are sent to Unity Connection over the network and the voice messages sent back from Unity Connection are not encrypted.

Step 21   Select **OK** to close the Account Settings dialog box.

Creating and Configuring an Account to Access Cisco Unity Connection in Windows Mail for Windows Vista

To use Windows Mail for Windows Vista to access Cisco Unity Connection voice messages, create and configure a new Windows Mail account for the user. You need the following information:

- Unity Connection username (alias).
- Cisco Personal Communications Assistant (PCA) password. (This is the web application password that is set on the User pages in Cisco Unity Connection Administration.)
- The IP address, or if DNS is configured, the fully qualified domain name of the Unity Connection server.

To Create and Configure a New Account in Windows Mail

Step 1   Start Windows Mail.

Step 2   On the Tools menu, select **Accounts**.

Step 3   In the Internet Accounts dialog box, select **Add**.

Step 4   On the Select Account Type page, select **E-Mail Account**.

Step 5   Select **Next**.

Step 6   On the Your Name page, in the Display Name field, enter the username.

Step 7   Select **Next**.

Step 8   On the Internet E-Mail Address page, in the E-Mail Address field, enter the Unity Connection SMTP Address of the user and the name of the Unity Connection server. You can find this information in the SMTP Address field on the User Basics page in Cisco Unity Connection Administration. The E-Mail Address typically follows this format:

<alias>@<fully qualified domain name of the Unity Connection server>

Step 9   Unity ConnectionSelect **Next**.

Step 10   On the Set Up E-Mail Servers page, under Incoming E-Mail Server Type, select **IMAP**.

Step 11   In the Incoming Mail (POP3 or IMAP) Server field, enter the IP address or the fully qualified domain name of the Unity Connection server.

⚠️
Caution   In Step 11 and Step 12, do not use the fully qualified domain name of the Unity Connection server unless DNS is configured for the network.

Step 12   In the Outgoing E-Mail Server (SMTP) Name field, enter the IP address or the fully qualified domain name of the Unity Connection server.

Step 13   If the Unity Connection SMTP server is configured to allow connections from untrusted IP addresses, skip to Step 15.

If the Unity Connection SMTP server is configured to require authentication from untrusted IP addresses, continue with Step 14.

Step 14   Check the **Outgoing Server Requires Authentication** check box.

Step 15   Select **Next**.

Step 16   On the Internet Mail Logon page, enter the user Unity Connection alias and Cisco PCA password.

Step 17   Select **Next**.

Step 18   On the Congratulations page, select **Finish**.

Step 19   Select **Close** to close the Internet Accounts dialog box.

Step 20   If you do not want to encrypt voice messages and other data that are sent over the network between Windows Mail and Unity Connection, you are finished creating and configuring a new account.

If you want to encrypt voice messages and other data that are sent between Windows Mail and Unity Connection, continue with Step 21.

Step 21   On the Tools menu, select **Accounts**.

Step 22   In the Internet Accounts dialog box, select the name of the mail account that you just created and select **Properties**.

Step 23   In the Properties dialog box, select the **Advanced** tab.

Step 24   Under both the Outgoing Mail field and the Incoming Mail field, check the **This Server Requires a Secure** Unity Connection **(SSL)** check box.

Step 25   Select **OK**.

⚠️
Caution   If you do not configure Windows Mail to use SSL, the Unity Connection username (alias) and password that are sent to Unity Connection over the network and the voice messages sent back from Unity Connection are not encrypted.

Step 26   Select **Close** to close the Internet Accounts dialog box.

Setting Up ViewMail for Outlook in Cisco Unity Connection

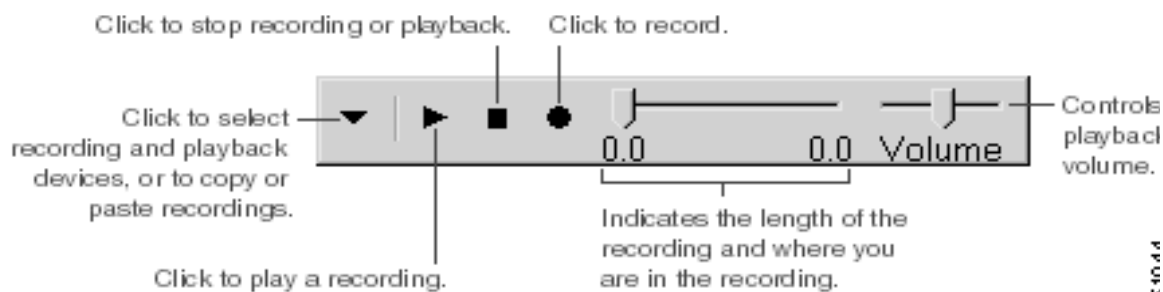## Cisco ViewMail for Microsoft Outlook 8.5 and Later

To install and set up Cisco ViewMail for Microsoft Outlook, see the applicable *Release Notes for Cisco ViewMail for Microsoft Outlook* at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html.

Cisco Unity Connection ViewMail for Microsoft Outlook 8.0

By using ViewMail for Outlook 8.0 to access Cisco Unity Connection voice messages, users can play and record voice messages by using the Media Master. See Figure 3-1.

Figure 3-1   *Media Master*

See the following sections:

- Task List for Setting Up ViewMail for Outlook 8.0, page 3-16
- Configuring the IMAP Account for ViewMail for Outlook 8.0, page 3-17
- Configuring ViewMail for Outlook 8.0 Settings for Secure Messaging and TRAP, page 3-17

Task List for Setting Up ViewMail for Outlook 8.0

ViewMail must be installed on each user workstation. Complete the following tasks to set up ViewMail 8.0 for users:

1. Review the applicable *Release Notes for Cisco Unity Connection ViewMail for Microsoft Outlook*, available at http://www.cisco.com/en/US/products/ps6509/prod_release_notes_list.html. The document specifies the requirements and procedures for installing 8.0.

2. If you have not already done so, install ViewMail 8.0 according to the procedures in the *Release Notes for Cisco Unity Connection ViewMail for Microsoft Outlook*.

3. If you have not already done so, configure an IMAP account in Microsoft Outlook. See the "Creating and Configuring an Account to Access Cisco Unity Connection in Microsoft Outlook" section on page 3-7.

4. If users have more then one IMAP account configured, you must configure ViewMail 8.0 to use the IMAP account that is used to access Unity Connection. See the "Configuring the IMAP Account for ViewMail for Outlook 8.0" section on page 3-17.

5. If you use secure messaging or TRAP, you must configure several ViewMail 8.0 settings. See the "Configuring ViewMail for Outlook 8.0 Settings for Secure Messaging and TRAP" section on page 3-17.

Configuring the IMAP Account for ViewMail for Outlook 8.0

If users have more than one IMAP account configured, you must configure ViewMail 8.0 to use the IMAP account that is used to access Unity Connection. This ensures that messages composed by using ViewMail are sent to the Unity Connection server. If users have only one IMAP account configured, ViewMail automatically uses it to send messages to Unity Connection.

Do the following procedure on each user workstation.

To Configure ViewMail for Outlook 8.0 Settings

Step 1   From the Microsoft Outlook Tools menu, select **ViewMail Options**.

Step 2   Select the **Accounts** tab.

Step 3   In the Select the Account to Access Cisco Unity Connection With field, select the IMAP account that is used to access Unity Connection.

Step 4   Select **Save**.

Configuring ViewMail for Outlook 8.0 Settings for Secure Messaging and TRAP

If you have configured Unity Connection for secure messaging or if you want users to be able to record or play messages by phone by using Telephone Record and Playback (TRAP), you must configure several ViewMail 8.0 settings.

After ViewMail 8.0 has been installed, do the following procedure on each user workstation.

To Configure ViewMail for Outlook 8.0 Secure Message and TRAP Settings

Step 1   From the Microsoft Outlook Tools menu, select **ViewMail Options**.

Step 2   Select the **Server** tab.

Step 3   Enter the following settings:

Table 3-1   Server Settings

Field	Setting
Cisco Unity Connection Server Name	Enter the name of the Unity Connection server. (Required for secure messaging and TRAP.)
Username	Enter the Unity Connection username (alias).

Table 3-1   Server Settings (continued)

Field	Setting
Password	*(Optional)* Enter the Cisco PCA password (also known as the web-application password) of the user. If you do not enter the password, the user is prompted for it each time Microsoft Outlook is restarted. If you do not want the user to be prompted for the password each time Microsoft Outlook is restarted, you must also check the Remember Password check box.
Remember Password	*(Optional)* Check this check box if you want ViewMail to remember the user password so that the user does not have to re-enter it each time Microsoft Outlook is restarted.
Proxy Server Address	If you have a firewall that blocks HTTPS traffic between user workstations and the Unity Connection server, enter the IP address of the HTTPS proxy server.
Proxy Server Port	If you have a firewall that blocks HTTPS traffic between user workstations and the Unity Connection server, enter the server port to use when connecting to the HTTPS proxy server.
Validate HTTPS Certificate	If you replace the default self-signed certificate with a certificate from a certificate authority, check the Validate HTTPS Certificate check box. If you are using the default certificate installed with Unity Connection, this check box must not be checked.
Extension	Enter the extension of the user. This setting is required only if you want the user to be able to record or play messages by phone.

Step 4   Select **Save**.

Configuring Cisco Unity Connection for HTML-based Message Notification

Cisco Unity Connection can be configured to send message notifications in the form of an HTML template to an email address. All HTML notifications in Unity Connection require an HTML-based notification template. The HTML-based templates can be selected and applied by the administrator to allow HTML notification for a device. The template selected can either be a default or a custom template that the administrator has created.

For more information on how to create a template, refer to To get the HTML notifications exactly as per the template defined by the administrator, the user's email client must support the display of images and icons. For more information on whether your email client support the display of images and icons, refer to documentation of your email service provider.

HTML notifications are supported with the following email clients:

- Microsoft Outlook 2007
- Microsoft Outlook 2010

- IBM Lotus Notes

- Gmail (Web based access only)

The user must ensure to select the authentication or non-authentication mode as desired. In addition, make sure the signed SSL certificates are installed in order to access the notifications via email and the voice message via Unity Connection Mini Web Inbox.

See the following sections:

Configuring the Authentication Mode

If the administrator has created a template that include images, icons, and/or status items, then the authentication mode ensures that the user authenticates with his or her Unity Connection credentials before the images are displayed as an HTML email on an email client.

By default, the system is configured for the authentication mode. The administrator can configure the authentication mode using the Cisco Unity Connection Administration.

To Configure the Authentication Mode

Step 1   In Cisco Unity Connection Administration, select **System Settings > General Configuration**.

Step 2   On the Edit General Configuration page, select the **Authenticate Graphics for HTML Notification** option to turn on the authentication mode.

Step 3   Click **Save**.

✎
Note
- The Unity Connection credentials are required only once for each session of Microsoft Outlook.

- If the user clicks on the **Cancel** button and does not enter Unity Connection credentials when prompted at the first instance then no image will be displayed in the email notification. You must restart the Microsoft Outlook to enter the Unity Connection credentials and view the images.

- If the user enters wrong password thrice then Unity Connection will not prompt again and the user must restart the Microsoft Outlook.

Configuring the Non-Authentication Mode

The non-authentication mode does not prompt user for credentials and the embedded images or icons are displayed without authentication in the email notification.

To Configure the Non-Authentication Mode

Step 1   In Cisco Unity Connection Administration, select **System Settings > General Configuration**.

Step 2   On the Edit General Configuration page, deselect the **Authenticate Graphics for HTML Notification** option to turn off the authentication mode.

Step 3   Click **Save**.

Configuring Microsoft Outlook to Display Images in an HTML Message Notification

In the authentication mode, to view all the custom graphics or administrative replaceable images as per the HTML-based template, you must make sure that your Microsoft Outlook client has all the required hotfixes and registry entries.

If the non-authentication mode is configured then your Microsoft Outlook client does not require any hotfixes or registry entries.

⚠

Caution   The user workstation must have the SSL certificates installed irrespective of the mode selected (authentication or non-authentication).

If you are using Microsoft Internet Explorer version 8, refer to the settings given in the Configuring Microsoft Internet Explorer 8 for Cisco Unity Connection Mini Web Inbox, page 3-24 section.

✎

Note   If due to certain security implications you are not allowed to install the required hotfixes or update registry entries, then you can create the templates without images, MWI status, and message status.

Table 3-2   Microsoft Outlook Settings Required for Authentication Mode

Microsoft Outlook Version	Microsoft Outlook 2007	Microsoft Outlook 2010 (32 bit and 64 bit)

Windows XP SP3, Windows 7 (32 and 64 bit), and Windows Vista (32 and 64 bit)	• Microsoft Outlook 2007
	   – Registry entry for AllowImageProxyAuth, where value=1.
	   – **Either** Install 2007 Office suite SP2. To install 2007 Office suite SP2, refer to http://support.microsoft.com/kb/953195. Then, install Microsoft Outlook 2007 hotfix package. To install hotfix, refer to http://support.microsoft.com/kb/2596993. **OR**
	   – Install 2007 Office suite SP3. To install 2007 Office suite SP3, refer to http://support.microsoft.com/kb/2526086.
	• Microsoft Outlook 2007 with SP2
	   – Install Microsoft Outlook 2007 hotfix package. To install hotfix, refer to http://support.microsoft.com/kb/2596993.
	   – Registry entry for AllowImageProxyAuth, where value=1.
	• Microsoft Outlook 2007 with SP3
	   – Registry entry for AllowImageProxyAuth, where value=1.
		• Install Microsoft Outlook 2010 hotfix package. For more information, refer to http://support.microsoft.com/kb/2459116.
		• Registry entry for AllowImageProxyAuth, where value=1.

To create the registry entries for Microsoft Outlook, do the following:

Step 1   Go to **Start** > **Run**. Type regedit and press **Enter**.

Step 2   Browse to the following path for Microsoft Outlook 2007:

HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common

Step 3   Browse to the following path for Microsoft Outlook 2010:

HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common

Step 4   Add "AllowImageProxyAuth = 1" as new DWORD value.

Configuring Microsoft Outlook for Automatic Image Download

Even after updating your Microsoft Outlook with required hotfixes and registry entries, you need to right click on the image, if any given in the template, and select **Show images**. You can also right click on the prompt appearing at the above of message window to show the images.

To automatically download images without performing these steps with every session, you must select the required options given under the **Tools > Trust Center > Automatic Download** section in your Microsoft Outlook email client.

Configuring Cisco Unity Connection to Send Voice Message as an Attachment

Starting with Cisco Unity Connection 10.0(1) release, the administrator can now configure Unity Connection to send the voice message as an attachment in the HTML notification to the user. Along with the link to access Unity Connection Mini Web Inbox through the HTML notification email, the user can now access the voice message attachment in the .wav format that can be played on PC or mobile using any player. Prior to Unity Connection 10.0(1) version, the end user received only a link in the HTML notifications to access Unity Connection Mini Web Inbox and listen to voice messages through Mini Web Inbox only.

> **Note** In case of forwarded messages, the attachment is sent only for the latest voice message.

If a user tries to access the voice message attachment using mobile, the following mobile clients are supported:

- Supported versions of iPhone 4 and above
- Supported versions of Android

> **Note** The secure and private voice messages cannot be sent as an attachment.

By default, the system is configured for not to send the voice message as an attachment. The administrator can configure to send voice message as an attachment using the Cisco Unity Connection Administration.

To Configure Unity Connection to Send Voice Message as an Attachment

Step 1 In Cisco Unity Connection Administration, select **Advanced > Messaging**.

Step 2 On the Messaging Configuration page, select the **Allow voice mail as attachments to HTML notifications** option to send the voice message as an attachment.

Step 3 Click **Save**.

Configuring the Size of Voice Messages Sent as an Attachment with HTML Notification

The administrator can configure the size of voice messages sent as an attachment with HTML notifications. The user can access the voice message attachment in the .wav format that can be played on PC or mobile using any player.

By default, the system is configured to send the voice message as an attachment upto 2048KB and maximum size can be 12288 KB. The administrator can configure the size of the voice message using the Cisco Unity Connection Administration.

To Configure the Size of Voice Message Sent as an Attachment

Step 1   In Cisco Unity Connection Administration, select **Advanced > Messaging**.

Step 2   On the Messaging Configuration page, enter the size of voice message in the **Max size of voice mail as attachment to HTML notifications (KB)** text box.

Step 3   Click **Save**. Make sure to restart the Connection Notifier service in order to changes take effect.

Configuring Cisco Unity Connection for Cisco Unity Connection Mini Web Inbox

See the following sections:

Configuring IBM Lotus Notes for Cisco Unity Connection Mini Web Inbox

Cisco Unity Connection Mini Web Inbox does not support the default IBM Lotus Notes supported browser. When a user receives a message notification on his IBM Lotus Notes email client and clicks a link in the notification to open Unity Connection Mini Web Inbox, the Unity Connection Mini Web Inbox must open in the default operating system browser.

To Configure the Web Browser as Operating System Default Browser in Lotus Notes Email Client

Step 1   In your Lotus Notes client, select **File > Preferences > Web Browser**.

Step 2   Select the **Use the browser I have set as the default for this operating system** option.

Step 3   Click **Apply** and then **Ok**.

Configuring Microsoft Internet Explorer 8 for Cisco Unity Connection Mini Web Inbox

To Configure Microsoft Internet Explorer 8 for Cisco Unity Connection Mini Web Inbox

Step 1   In your browser window, go to **Tools > Intranet Options** and select the **Security** tab.

Step 2   Select the **Local intranet** option and click **Sites**.

Step 3   Uncheck all the check boxes and click **Ok**.

Step 4   Select the **Trusted sites** option and click **Sites**.

Step 5   Add the website that you are using for Unity Connection, for example, https://ucbu-cisco-vmxyz.cisco.com.

Step 6   Click **Close** and then **Ok**.

Configuring Windows Vista and Windows 7 (32 bit and 64 bit) for Cisco Unity Connection Mini Web Inbox

To Configure Windows Vista and Windows 7 (32 bit and 64 bit) for Cisco Unity Connection Mini Web Inbox

Step 1   Select **Start > Control Panel > Flash Player**.

Step 2   Select the **Camera and Mic** tab in the Flash Player Settings Manager window.

Step 3   Click **Camera and Microphone Settings by Site**.

Step 4   Select the **Ask me when a site wants to use the camera or microphone** option in the **Camera and Microphone Settings by Site** window.

Step 5   Click **Add**.

Step 6   Add the website that you are using for Unity Connection, for example, ucbu-cisco-vmxyz.cisco.com.

Step 7   Click **Allow** and then **Close**.

Troubleshooting IMAP Client Sign-In Problems in Cisco Unity Connection

When users change their Cisco PCA password (also known as the web-application password) in the Cisco Unity Connection Messaging Assistant, they also must update the password in their IMAP client application so that the client can continue to access Unity Connection and retrieve voice messages.

If users have trouble receiving voice messages in an IMAP client, consider the following possibilities:

- If the IMAP client application prompts a user for the Cisco PCA password, but does not accept it, the Cisco PCA password may have expired or changed, or is locked. Users can change their password in the Unity Connection Messaging Assistant first and then update it from their IMAP client application.

- If Microsoft Outlook users are not prompted for their Cisco PCA password, verify that the Remember Password check box on the Internet E-mail Settings (IMAP) page is not checked. If this option is checked, and the password of the user has expired, changed, or is locked, Microsoft Outlook does not prompt the user to enter the Cisco PCA password. The result is that the user does not receive voice messages from Unity Connection, and Microsoft Outlook prompts for the username and password.

User Orientation in Cisco Unity Connection

See the following sections:

- Orientation Task List for Cisco Unity Connection Users, page 4-1
- Settings That Cisco Unity Connection Users Can Change, page 4-3

Orientation Task List for Cisco Unity Connection Users

After you set up the client applications that users will use to access Cisco Unity Connection from their phones and computers, use the following task list to acquaint users with Unity Connection. If you are planning supplemental Unity Connection training, also consider reviewing the potential user concerns and misconceptions listed in the "Support Desk Orientation in Cisco Unity Connection" section on page 5-2.

Offer User Documentation and Contact Information

1. Give users a *Cisco Unity Phone Menus and Shortcuts* wallet card. Use the Wallet Card wizard to produce the card. The templates in the wizard list frequently used menu options and shortcuts for managing Unity Connection messages and user preferences by phone; the wizard fills in the applicable keys based on the conversation that you specify. The resulting PDF is formatted as a wallet card that can be printed, then cut out and folded by users.

    Procedures in the *User Guide for the Cisco Unity Connection Phone Interface* do not contain the keys that users press for Unity Connection menu options. Instead, the procedures use the prompts that users hear to specify the menu options to choose. To provide users with key information, you must use the Wallet Card wizard.

    The Wallet Card wizard also allows you to customize technical support information and instructions for signing in to Unity Connection. The Wallet Card wizard is a Windows-based remote database administration tool. Download the tool and view Help at
    http://www.ciscounitytools.com/Applications/CxN/WalletCardWizard/WalletCardWizard.html.

2. Give each user applicable user guides. The following Cisco Unity Connection user guides are available at http://www.cisco.com/en/US/products/ps6509/products_user_guide_list.html.

    - *User Guide for the Cisco Unity Connection Phone Interface*
    - *User Guide for the Cisco Unity Connection Messaging Assistant Web Tool*
    - *User Guide for the Cisco Unity Connection Messaging Inbox Web Tool*
    - *User Guide for Accessing Cisco Unity Connection Voice Messages in an Email Application*
    - *User Guide for the Cisco Unity Connection Personal Call Transfer Rules Web Tool*

– *Quick Start Guide: Using the Cisco Unity Connection Web Inbox*

– *Quick Start Guide: Using Cisco ViewMail for Microsoft Outlook*

Information in the guides is generally organized by feature. You can distribute the guides for the interfaces that users are using, or you can distribute feature-specific information to users for whom you have enabled the features. (On Cisco.com, select the link for the topics you want, and print the PDF files.)

3. Give users the phone numbers that they dial to access Unity Connection from within your organization and from outside the organization. As applicable, show users which button or key to use on their desk phones to access Unity Connection.

4. Give users the URL to the Cisco PCA website: http://<Cisco Unity Connection server name>/ciscopca.

5. Give users the URL to the Cisco Unity Connection Web Inbox: http://<Cisco Unity Connection server name>/inbox.

6. Give users the name, extension, and/or email address of the Unity Connection administrator and any support desk contact information.

7. Depending on the conversation version that users in your organization are familiar with, you may want to provide them with a list of phone menu differences between Unity Connection and a former voice messaging system—especially if you choose not to offer them an alternative to the standard conversation, which is specified by default in the Voice Mail User template.

Provide PINs, Passwords, and Security Guidelines

8. Provide users with their initial phone PINs. Alternatively, tell users to sign in to the Cisco Personal Communications Assistant (PCA) website to set their phone PINs before they call Unity Connection to complete first-time enrollment. (Users are not required to enter an existing phone PIN in order to change it in the Cisco PCA.)

   If users choose not to initially change their PIN in the Cisco PCA, they are prompted to change their phone PIN during first-time enrollment.

9. Provide users with their initial Cisco PCA passwords. Users must use the Unity Connection Messaging Assistant to change their Cisco PCA passwords.

10. Explain to users how to secure their phone and Cisco PCA PINs and passwords so that they adequately protect their Unity Connection mailboxes from unauthorized access. Detail the security guidelines for your organization. Encourage users to enter secure PINs and passwords whenever they change them.

11. Make sure users understand that their Cisco PCA passwords are not related to their Unity Connection phone PINs, nor are the passwords and PINs synchronized. Users may assume that their phone and Cisco PCA PIN and password are the same. As a result, they may think that they are changing both when the Unity Connection conversation prompts them to change their phone PIN during first-time enrollment. For this reason, you may find that many users do not consider securing their Cisco PCA passwords, even though you request that they do so.

Remind Users to Complete First-Time Enrollment

12. Make sure that users know that they need to complete first-time enrollment by phone. They do not need to refer to any Unity Connection documentation during enrollment. Unity Connection indicates when the enrollment process is complete. If users hang up before they have completely enrolled, none of their changes are saved and the first-time enrollment conversation plays again the next time that they sign in to Unity Connection.

The "Enrolling as a Cisco Unity Connection User" chapter of the *User Guide for the Cisco Unity Connection Phone Interface* details the tasks that users are asked to complete as part of enrollment.

Explain How Unity Connection Features and Functionality Work

13. Provide training on how to personalize user settings by using the phone and the Unity Connection Messaging Assistant, as summarized in Table 4-1. In particular, users may benefit from a hands-on demonstration of the Messaging Assistant, as they may not be accustomed to using a web interface to set voice messaging options.

14. Provide training on how to use the Cisco Unity Connection Personal Call Transfer Rules web tool, and how call transfers, call holding and screening, and caller options are used, as summarized in Table 4-2.

Users can refer to the *User Guide for the Cisco Unity Connection Personal Call Transfer Rules Web Tool* or to Cisco Unity Connection Personal Call Transfer Rules Help for further guidance after orientation.

15. Explain how full mailboxes work with Unity Connection. See the "Support Desk Orientation in Cisco Unity Connection" section on page 5-2 for issues that users may encounter. Refer users to the appropriate user guides for similar information.

16. *If single inbox is configured:* Discuss single-inbox behavior with users.

17. If your organization has users who will use RSS readers to access voice messages, provide training on using RSS with Unity Connection.

18. If your organization has users who will use TTY and the TTY prompt set, provide training on using TTY with Unity Connection.

19. Make sure that users who own call handlers or system distribution lists understand their responsibilities (if applicable).

20. As applicable, tell users how to use the Cisco Unity Greetings Administrator and System Broadcast Administrator.

Settings That Cisco Unity Connection Users Can Change

See the following tables:

- Settings That Users Can Change By Using the Cisco Unity Connection Messaging Assistant and the Phone Menus
- Settings That Users Can Change By Using the Cisco Unity Connection Personal Call Transfer Rules Web Tool and the Phone Menus

Table 4-1   Settings That Users Can Change By Using the Cisco Unity Connection Messaging Assistant and the Phone Menus

Settings That Can Be Changed by Using the Unity Connection Messaging Assistant	Settings That Can Be Changed by Using the Phone Menus
Call Holding and Screening[1]: • Select how Unity Connection handles indirect calls when the user phone is busy, including placing the caller on hold, prompting the caller to hold or leave a message, and sending the caller directly to the greeting • Select how Unity Connection handles indirect calls, including telling the user who the call is for, announcing that Unity Connection is transferring the call, prompting the user to accept or refuse a call, and prompting callers to say their names	Call Holding and Screening[1]: • None
Call Transfers[2]: • Configure the three basic transfer rules: standard, alternate, and closed hours • Enable or disable personal call transfer rules for each of the basic transfer rules • Transfer indirect calls to an extension or send them to the user greeting • Change extensions	Call Transfers[2]: • Configure the three basic transfer rules: standard, alternate, and closed hours • Enable or disable personal call transfer rules for each of the basic transfer rules • Transfer indirect calls to an extension or send them to the user greeting • Change extensions • Configure alternate contact numbers for caller input keys that are assigned to the Transfer to Alternate Contact Number action
Caller Options: • Allow callers to edit messages • Allow callers to mark messages urgent	Caller Options: • None
Phone Menu Options: • Set language for Unity Connection prompts • Specify whether users use the phone keypad or voice-recognition input style • Set speed and volume of prompts, recorded names, and user greetings • Select full or brief Unity Connection conversation menus • Select the action that Unity Connection performs when the user calls Unity Connection, including greeting the user by name, and announcing the number of new messages by type • Change the time format used for message time stamps • Specify alternate extensions	Phone Menu Options: • Select full or brief Unity Connection conversation menus

Table 4-1   Settings That Users Can Change By Using the Cisco Unity Connection Messaging Assistant and the Phone Menus (continued)

Settings That Can Be Changed by Using the Unity Connection Messaging Assistant	Settings That Can Be Changed by Using the Phone Menus
Greetings: • Record a personal greeting • Enable or disable greeting • Specify an expiration date for an enabled greeting • Switch between system prompt and personal greeting	Greetings: • Record a personal greeting • Enable or disable greeting • Specify an expiration date for an enabled greeting
Message Notification: • Enable or disable a notification device • Specify dialing or recipient options • Select the types of messages and message urgency for which Unity Connection generates a notification • Specify a list of message senders (by username or calling phone number) for which Unity Connection generates a notification • Set up a notification schedule, and specify what happens when a device does not answer, is busy, or fails	Message Notification: • Enable or disable a notification device, and change its number
Message Playback: • Specify the speed and volume of messages that are played by phone • Specify message playback order • Specify whether Unity Connection plays the Message Type menu • Select the action that Unity Connection performs when messages are played, including announcing the name and number of the sender who left a message, and whether the time stamp is played before or after the message • Specify that messages are marked saved upon hang-up or disconnect • Specify whether Unity Connection asks to confirm deletions of new and saved messages	Message Playback: • Speed and volume of message as it is played

Table 4-1   ***Settings That Users Can Change By Using the Cisco Unity Connection Messaging Assistant and the Phone Menus (continued)***

Settings That Can Be Changed by Using the Unity Connection Messaging Assistant	Settings That Can Be Changed by Using the Phone Menus
Message Sending and Addressing: • Specify that Unity Connection prompts to confirm message recipients by name • Specify that Unity Connection prompts to continue adding names after each recipient • Specify that Unity Connection sends messages when users hang up or a call is disconnected • Switch between addressing messages to other users by name, or by extension • Specify order for addressing messages by name (last name then first name, or vice versa)	Message Addressing: • Switch between addressing to other users by name or by extension (by pressing ##)[3] • Review, add, or remove names in the addressing priority list[4]
Personal Settings: • Record a name • Specify alternate names • Change directory listing status • Change password or PIN • Add user-defined alternate extensions[5]	Personal Settings: • Record a name • Change directory listing status • Change password or PIN • Add user-defined alternate extensions[5] • Edit alternate contact numbers, if an administrator has configured one or more caller input keys to transfer to an alternate contact number during the user greeting
Private Lists: • Enter a display name • Record a list name • Add and delete members	Private Lists: • Record a list name • Add and delete members
Contacts: • Set up contacts to use for both name dialing and call transfer rules	Contacts: • None

1. Call holding and screening options apply only to incoming calls that were routed to the user from the automated attendant or a directory handler, and not on direct calls. Holding and screening options do not apply when an outside caller or another user dials a user extension directly. In addition, holding and screening options are only available when supervised transfers are enabled. These settings apply if the user does not have personal call transfer rules enabled.

2. Call transfer options apply only to incoming calls that were routed to the user from the automated attendant or a directory handler, and not on direct calls. Transfer options do not apply when an outside caller or another user dials a user extension directly.

3. Note that this depends on whether you have enabled spelled name addressing.

4. To enable users to access the setup conversation that allows them to review, add, or remove names in the addressing priority list, the users must be assigned to a custom conversation, and you must use the Custom Keypad Mapping tool to map the Addressing Priority List conversation to a key in the Message Settings menu for that conversation.

5. Users must belong to a class of service with the Allow Users to Manage Their User-Defined Alternate Extensions option enabled. To enable users to access the phone menu conversation that allows them to review, add, or remove alternate extensions, the users must be assigned to a custom conversation, and you must use the Custom Keypad Mapping tool to map the Edit User-Defined Alternate Extensions option to a key in the Preferences Menu for that conversation.

Table 4-2   Settings That Users Can Change By Using the Cisco Unity Connection Personal Call Transfer Rules Web Tool and the Phone Menus

Settings That Can Be Changed by Using the Cisco Unity Connection Personal Call Transfer Rules Web Tool	Settings That Can Be Changed by Using the Phone Menus
Call Holding and Screening: • Set up personal call transfer rules to specify how Unity Connection handles direct and indirect calls when the user phone is busy, including placing the caller on hold, prompting the caller to hold or leave a message, and sending the caller directly to the greeting • Set up personal call transfer rules to specify how Unity Connection handles direct and indirect calls, including telling the user who the call is for, announcing that Unity Connection is transferring the call, prompting the user to accept or refuse a call, and prompting callers to say their names	Call Holding and Screening: • None
Call Transfers: • Set up personal call transfer rules to transfer direct and indirect calls to an extension, to an external phone number, or to the greeting	Call Transfers: • Enable or disable personal call transfer rules to transfer direct or indirect calls to an extension, to an external phone number, or to the greeting • Enable or disable the Transfer All rule set to forward all calls to voicemail or to another phone number • Forward all incoming calls directly to Unity Connection, rather than to phone extension
Caller Options: • Allow callers to edit messages • Allow callers to mark messages urgent	Caller Options: • None
Destinations: • Set up phone numbers or notification devices to use when transferring calls • Set up groups of destinations to use in personal call transfer rules • Specify the number of rings that Unity Connection waits before transferring the call to the next destination or to voicemail	Destinations: • None
Caller Groups • Create groups of user-defined contacts, administrator-defined contacts, or Unity Connection users to use in personal call transfer rules	Caller Groups • None

Operator and Support Desk Orientation in Cisco Unity Connection 10.x

Operators in your organization need information about Cisco Unity Connection that is specific to your installation. In addition, if your organization has a support desk, the staff need to be prepared to answer the questions that users may ask, and to be aware of the resources that are available to assist them in answering user questions.

See the following sections:

- Operator Orientation in Cisco Unity Connection, page 5-1
- Support Desk Orientation in Cisco Unity Connection, page 5-2

Operator Orientation in Cisco Unity Connection

Operator orientation should address the same points as user orientation, but in greater detail. Operators must be familiar with how users use Cisco Unity Connection. Depending on the size of your organization, the operator may be the person users are likely to ask when they have questions about Unity Connection.

In addition to the information in the "User Orientation in Cisco Unity Connection" chapter and the "Support Desk Orientation in Cisco Unity Connection" section on page 5-2 (as applicable), operators also need to understand the following concepts and tasks.

Roles of the Operator and the Automated Attendant

The way your organization uses the automated attendant determines what the operator responsibilities are. The automated attendant is a call handler that is used in place of a human operator to answer and direct calls by playing greetings and responding to caller input. The automated attendant can provide a menu of options (for example, "For Sales, press 1; for Service, press 2."), and it can also provide information (for example, "Our normal business hours are Monday through Friday, 8 a.m. to 5 p.m.").

Directing Calls

Regardless of how your organization uses the automated attendant, many calls go to the operator. The operator must know how to direct calls to voicemail and to user phones. With Cisco Unified Communications Manager, you can program the phone to direct calls to voicemail. For details on setting this up, see the tech note *How to Transfer a Caller Directly into a Cisco Unity Mailbox*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_tech_notes_list.html.

Forwarding Messages to Intended Recipients

If an operator also owns a call handler or system distribution list, make sure that the operator knows to review messages frequently, and to forward messages as necessary to the applicable recipients.

Using the Cisco Unity Greetings Administrator

An operator who is responsible for changing call handler greetings for the organization can use the Cisco Unity Greetings Administrator when it is not practical to change a greeting in Cisco Unity Connection Administration. For example, if the office is unexpectedly closed because of bad weather, the operator can call from home to use the Cisco Unity Greetings Administrator to enable the alternate Opening Greeting, or to rerecord a call handler greeting stating that the office is closed.

Using the Cisco Unity Broadcast Message Administrator

If an operator is responsible for sending recorded announcements to everyone in an organization (or to particular locations within an organization), explain how to access and use the Cisco Unity Broadcast Message Administrator to send broadcast messages.

Support Desk Orientation in Cisco Unity Connection

Support desk orientation should address the same points as user and operator orientation, but in greater detail. Support desk staff must be familiar with how users and operators use Cisco Unity Connection, and the common problems that users may encounter when using Unity Connection. Instead of using the Unity Connection server, it may be helpful to set up a test server that support desk staff can use to browse to Cisco Unity Connection Administration, and troubleshoot and test client applications.

To prepare for possible calls to the support desk at your organization, familiarize the support desk staff with the resources listed in the following "Support Desk Resources" section, and with the potential user concerns and misconceptions listed in the "Potential User Concerns and Misconceptions" section on page 5-3. (See also the "Operator Orientation in Cisco Unity Connection" section on page 5-1 and the "User Orientation in Cisco Unity Connection" chapter.)

Support Desk Resources

- User documentation is available at
  http://www.cisco.com/en/US/products/ps6509/products_user_guide_list.html.
- The *Compatibility Matrix: Cisco Unity Connection and the Software on User Workstations* is available at
  http://www.cisco.com/en/US/products/ps6509/products_device_support_tables_list.html.
- The following chapters in this guide provide information on how user workstations should be set up, and describes how users use Unity Connection client applications:
  - Setting Up Access to the Cisco Personal Communications Assistant in Cisco Unity Connection
  - Setting Up Playback and Recording Devices for the Media Master in Cisco Unity Connection
  - Configuring an Email Account to Access Cisco Unity Connection Voice Messages
- The *Troubleshooting Guide for Cisco Unity Connection Release 10.x* is available at
  http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/troubleshooting/guide/10xcuct sgx.html.

- For descriptions and the URLs of all Unity Connection documentation on Cisco.com, see the *Documentation Guide for Cisco Unity Connection Release 10.x*. The document is shipped with Unity Connection and is available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/roadmap/10xcucdg.html.

Potential User Concerns and Misconceptions

Table 5-1 describes potential user issues, which are typically based on misconceptions about how Cisco Unity Connection works. Users who encounter such issues are often those who are accustomed to another voice messaging system, have not yet completed Unity Connection training, or are unaware of a new feature or functionality change to an existing system.

Table 5-1   Potential User Concerns and Misconceptions

Potential Issue	Description
Delayed messages	Users may believe that their messages are delayed for the following reasons: • While listening to new messages, users may skip a message and inadvertently mark it new. Later, when they check messages again, they hear the skipped message and believe that the message arrived after a delay. • Users may skip more messages than they intend while listening to their messages, and later check messages again only to hear one or more of the skipped messages, and believe that the messages arrived after a delay. • While listening to messages, other new messages arrive that users may not be aware of. Later, when they check messages again, they hear the new messages and believe that they were delayed.
Deleted messages	By default, when users delete a new or saved message, Cisco Unity Connection does not ask them to confirm the deletion. You may want to enable Unity Connection to request confirmation from users before proceeding with the deletion, especially if many users do not belong to a class of service that allows them to retain and review their deleted messages. You can set up Unity Connection to confirm deletion of messages on the System Settings > Advanced > Conversations page in Cisco Unity Connection Administration. For information on deleted messages, refer users to the "Deleting Messages" chapter of the *User Guide for the Cisco Unity Connection Phone Interface*, available at http://www.cisco.com/en/US/products/ps6509/products_user_guide_list.html.

Table 5-1   Potential User Concerns and Misconceptions (continued)

Potential Issue	Description
Deleted messages: IMAP and MAPI behavior	When users access messages stored on a Microsoft Exchange server both from a Microsoft Outlook client and from Cisco Unity Connection, they may experience unexpected and confusing behavior when deleting messages. The difference in behavior occurs when the Microsoft Outlook client is configured to use MAPI, the Microsoft interface for connecting to Exchange, and stems from the fact that MAPI and IMAP—the protocol used by Unity Connection—use different mechanisms for marking messages as deleted.
	If you have users who access a Microsoft Exchange server by using Outlook (with MAPI) or Outlook Web Access, and who also use Unity Connection to manage messages on the same message store, be sure to alert them to this behavior.
	Deleted Messages—IMAP Behavior
	When a user deletes a message from Microsoft Outlook, the message is moved from the Inbox to the Deleted Items folder. At this point, Unity Connection can no longer access the message, and no longer indicates that the message exists either as a new, saved, or deleted message.
	Deleted Messages—MAPI Behavior
	When a user deletes a message from Unity Connection, the message remains in the Inbox but is flagged to indicate that it has been marked deleted by the user. However, when configured to use MAPI, Microsoft Outlook does not recognize this flag as a deletion, and continues to display the message as a new or saved message in the Inbox.
Device for recording or playback does not show in ViewMail for Outlook device lists	When users add or turn on a new recording or playback device, they must restart the ViewMail for Outlook add-in so it can recognize the new device. To restart ViewMail, restart Outlook.
Directory listing: users are not listed as expected	When users do not have a recorded name, they are not listed in the corporate directory and as a result, outside callers are not be able to find them when searching for them by name. By default, Cisco Unity Connection prompts users to record a name during first-time enrollment, but it does not prevent them from completing the enrollment process if they do not.
	To address this issue, consider the following options:
	• You can change whether recording a name is required to complete first-time enrollment on the System Settings > Advanced > Conversations page in Cisco Unity Connection Administration.
	• You can provide recorded names for users in Cisco Unity Connection Administration.
	• Users with class of service rights can record their own names by using the Unity Connection conversation or the Unity Connection Messaging Assistant.
	Note This problem does not occur for internal users, but only for outside callers; Unity Connection users who address messages by name are still able to find other users even if they have not recorded a name.
Fax: attached files are not delivered to fax machines (fax integrations only)	Users may be unaware that when they add attachments to an email message and then send the message to a fax machine, Unity Connection renders only those attachments with the file extensions specified during Unity Connection setup. All other attachments are removed.

Table 5-1   Potential User Concerns and Misconceptions (continued)

Potential Issue	Description

IMAP client: Differences in client behavior	Users who use different third-party IMAP clients to access voice messages from their desktop machines may note the following discrepancies in behavior:
	
	• Microsoft Outlook client:
	
	  – For new messages, the "Mark as Unread" feature marks messages as new on the Cisco Unity Connection server, regardless of whether the WAV file message attachment is downloaded or not.
	
	  – Voice messages that are deleted by phone are marked for deletion in the Outlook client and are changed to strikethrough text when users select the "Send/Receive" command.
	
	• Novell GroupWise client:
	
	  – When new messages with the WAV file message attachment have been downloaded to the GroupWise client, the "Read Later" feature no longer marks the message as new on the Unity Connection server.
	
	  – Voice messages that are deleted by phone are not marked for deletion in GroupWise; users need to manually delete them from this client.
	
	  – GroupWise users need to use the "Send/Retrieve" command to update message status from the Unity Connection server.

Mailbox fills up quickly	Users may complain that their mailboxes are filling up too quickly, for any of the following reasons: • Cisco Unity Connection does not automatically delete messages when they reach a certain age. This means that user messages are saved until the user deletes them permanently. (For information on how to permanently delete messages, refer users to the "Managing the Size of Your Mailbox" chapter of the applicable user guides available at http://www.cisco.com/en/US/products/ps6509/products_user_guide_list.html.) • When users receive nondelivery receipts (NDRs) to messages that they send, their email client mailbox can quickly increase in size—especially if the original message included large attachments. For users who have access to email messages via TTS, if their email clients are configured to save their sent messages, the original message and attachments are stored in their Sent Items folders and another copy is sent to their Inboxes along with the NDR, increasing their mailbox size accordingly. • Users may receive messages that have been forwarded many times over, which increases message size. The original message plus all recorded introductions that were added during forwarding equal the total message size. As a result, users who have relatively few messages stored in their mailboxes may still find that their mailboxes exceed the storage limits. • User mailboxes can fill up while users are on vacation or on an extended leave of absence. To prevent this, specify that Unity Connection prevents callers from leaving messages when users have their alternate greetings enabled.
Message notification: repeat notification options	When a user chooses not to have Cisco Unity Connection restart notification each time a new message arrives, setting a long interval between repeat notification calls may lead the user to believe that Unity Connection is delaying notification.

Table 5-1   *Potential User Concerns and Misconceptions (continued)*

Potential Issue	Description
Media Master: opening a file that is saved on a workstation	When a user attempts to use a previously recorded WAV file (for example, an announcement that was recorded earlier) rather than recording by using a phone or a computer microphone, the Media Master may display an error message. The error occurs when the WAV file was recorded in the G.729a audio format. To resolve the problem, the user must do one of the following: • Convert the WAV file to another audio format (for example, convert it to the G.711 audio format). • Use a WAV file that is recorded in a supported audio format other than G.729a. • Make the recording by using a phone or a computer microphone.
MWIs	To gain an understanding of when MWIs turn on and off, what causes them to turn on and off, and what causes MWIs to behave differently than expected, see the "Troubleshooting Message Waiting Indicators (MWIs) in Cisco Unity Connection 10.x" chapter of the *Troubleshooting Guide for Cisco Unity Connection Release 10.x*.
Passwords and PINs are not secure, or users use the wrong password or PIN	Users may assume that their phone PINs and Cisco Personal Communications Assistant (PCA) passwords are the same or are synchronized. As a result, they may think that they are changing both PIN and password when Cisco Unity Connection prompts them to change their phone PIN during first-time enrollment. Additionally, they may try to use their phone PIN to sign in to the Cisco PCA.
Speed for elements of the Unity Connection conversation varies	Users may report that the speed at which Cisco Unity Connection plays menus, recorded names, greetings, and messages is inconsistent. For example, users may report that when they listen to their messages, the message is played at a different speed than the recorded names of users who leave them messages and the message properties (for example, the time stamp and message number). Such inconsistencies are expected when you consider the following: • Unity Connection plays recorded names and greetings at the speed at which they were recorded. Neither you nor users can affect the playback speed of recorded names and greetings. • Messages played via Text to Speech (TTS) are always played at normal speed by default, regardless of message playback settings. • The speed that you or a user specifies for system prompts—the standard recordings that come with the Unity Connection system, including prompts for message properties—does not affect the playback speed of messages. • The speed that users specify for message playback does not affect system prompts.
Unread messages	Depending on how Cisco Unity Connection is set up at your organization, users may be surprised at how Unity Connection handles messages when calls are intentionally or unintentionally disconnected (for example, when a user hangs up or when a mobile phone loses its charge or signal) while users are in the process of listening to new messages. Some users may incorrectly assume that Unity Connection marks the message as read, which is not the case. You can change how Unity Connection handles unread messages when calls are disconnected by adjusting the "Mark Message Saved If User Hangs Up" setting on the System Settings > Advanced > Conversations page of Cisco Unity Connection Administration.

Table 5-1   *Potential User Concerns and Misconceptions (continued)*

Potential Issue	Description
Unsent messages	Depending on how Cisco Unity Connection is set up at your organization, users may be surprised at how Unity Connection handles messages when calls are intentionally or unintentionally disconnected (for example, when a user hangs up or when a mobile phone loses its charge or signal) while users are in the process of sending, replying to, or forwarding a message. Some users may incorrectly assume that Unity Connection offers a draft folder for unsent messages, which is not the case.
	You can change how Unity Connection handles unsent messages when calls are disconnected by adjusting the "Send Message If User Hangs Up During Recording" setting on the System Settings > Advanced > Conversations page of Cisco Unity Connection Administration.

INDEX

S

security alerts, managing when using SSL
connections   **1-3**

support desk

orientation   **5-2**

resources   **5-2**

T

Thunderbird, configuring to access voice messages   **3-13**

U

unsent messages, addressing user concerns   **5-7**

user misconceptions, potential   **5-3**

user orientation   **4-1**

V

ViewMail for Microsoft Outlook

configuring IMAP account   **3-17**

secure messaging   **3-17**

task list   **3-16**

W

Windows Mail, configuring to access voice
messages   **3-14**