



CHAPTER 28

Setting Up Subscriber Workstations

Cisco Unity subscribers can send and manage voice, fax, and e-mail messages by using a touchtone phone, or by using Cisco Unity ViewMail for Microsoft Outlook. They can also send and manage voice and fax messages by using the Cisco Unity Inbox. In addition, subscribers can use the Cisco Unity Assistant to personalize the Cisco Unity phone settings that control how they interact with Cisco Unity by phone.

This chapter reviews the preparations necessary for setting up and customizing Cisco Unity applications so that subscribers can access and use them at their workstations. See the following sections for details:

- [Task List for Setting Up Subscriber Phones and Customizing the Conversation, page 28-2](#)—Lists the tasks that you must do before subscribers access Cisco Unity by phone.
- [Securing and Changing Cisco Unity Phone Passwords, page 28-3](#)—Summarizes how Cisco Unity phone passwords are assigned, secured, and changed.
- [Setting Up Cisco Unity ViewMail for Microsoft Outlook, page 28-3](#)—Lists the tasks for setting up e-mail clients for Unified Messaging subscribers.
- [Setting Up the Cisco Personal Communications Assistant, page 28-5](#)—Summarizes what you must do so that subscribers can use the Cisco Personal Communications Assistant to access the Cisco Unity Assistant and the Cisco Unity Inbox.
- [Securing and Changing Cisco PCA Passwords, page 28-9](#)—Describes how subscriber passwords are changed and secured.
- [Defining Cisco PCA Logon, Password, and Lockout Policies, page 28-10](#)—Summarizes the account policy options that are available for Cisco PCA logons, passwords, and lockouts.
- [Setting Up the Media Master, page 28-10](#)—Explains how subscribers use the Media Master to make and play recordings over the phone, or by using the computer microphone and speakers, and what you need to do to allow them to use the preferred devices.
- [Setting Up FaxMail, page 28-13](#)—Summarizes what you must do so that subscribers can use FaxMail.
- [Setting Up Mobile Message Access for BlackBerry, page 28-14](#)—Summarizes what you must do to allow subscribers to access Cisco Unity voice messages by using their Blackberry devices.
- If you plan to set up text message notifications for subscribers (in addition to the message waiting indicators (MWIs) that you set up), also see the [“Setting Up Text Message Notifications” section on page 23-2](#).

When you have set up subscribers to use the Cisco Unity client applications, review the tasks in the [“Subscriber Orientation”](#) chapter to orient subscribers and operators to Cisco Unity.

For a list of supported versions of Cisco Unity combined with the supported versions of the software on subscriber workstations, see the *Compatibility Matrix: Cisco Unity and the Software on Subscriber Workstations*, at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_device_support_tables_list.html.

Task List for Setting Up Subscriber Phones and Customizing the Conversation

As applicable, do the following tasks before subscribers access Cisco Unity by phone.

1. Set up Cisco Unity to handle busy and unanswered calls—Enable call forwarding to Cisco Unity for each subscriber phone, so that busy and unanswered calls to the subscriber extension are transferred to Cisco Unity to handle. Cisco Unity then uses the call transfer settings specified for each subscriber in the Cisco Unity Administrator to determine, for example, whether callers will be put on hold or sent directly to the subscriber greeting.
2. Specify a “Messages” button for subscriber phones—Enable each subscriber phone so that the subscriber can use a “Messages” button or a similar speed-dial button on the phone to dial the internal Cisco Unity phone number for your organization. This makes calling Cisco Unity to check messages or to change personal settings by phone quick and easy for the subscriber, as the subscriber does not have to dial the number for Cisco Unity from his or her desk phone.
3. Specify phone and TTS languages for prompts—Phone languages are the languages in which Cisco Unity can play system prompts to subscribers and callers; TTS languages are the languages in which Cisco Unity can play e-mail messages over the phone. See the “[Managing Languages](#)” chapter for information on specifying phone and TTS languages.
4. Install TTY prompts—A TTY prompt set, available in U.S. English (ENX) only, can be installed and used just like any other supported phone language. When the TTY prompt set is installed, subscribers and outside callers who use TTY can call Cisco Unity and use the same features that a hearing caller can use.

However, note the following exceptions:

- TTY tones are not available for use in navigating through the Cisco Unity conversation.
- Some TTY phones do not have the capability to send DTMF tones. In this case, TTY users may need to use the phone keypad for system navigation.

To install the TTY prompt set, see the “[TTY Overview](#)” section on page 10-9.

5. Change conversation defaults and enable conversation-specific features—Depending on your organization, you may want to change some default settings for the Cisco Unity conversation to ensure that subscribers have an easier transition from a previous voice messaging system. For example, you can change the default conversation style so that subscribers hear menus that offer a more familiar keypad mapping, and you can specify that Cisco Unity prompts subscribers to record first and then address when they send messages.

In addition, you can enable features such as “Easy” Sign-In, system transfers, Text to Speech, and live reply. For a complete list of customizations and features, as well as details on how to implement them, see the “[Summary of How You Can Customize Cisco Unity Conversations](#)” section on page 14-1.

Securing and Changing Cisco Unity Phone Passwords

You can change the phone password for an individual subscriber on the Subscribers > Subscribers > Phone Password pages in the Cisco Unity Administrator at any time. Alternatively, you can use the Cisco Unity Bulk Import wizard to change the phone passwords for multiple subscribers at the same time. (See the Cisco Unity Bulk Import Help for details.)

As a best practice, each subscriber should be assigned a unique password that is eight or more digits long and non-trivial. If you allow subscribers to set their own passwords, encourage them to follow the same practice or use the settings on the Subscribers > Account Policy > Phone Password Restrictions page in the Cisco Unity Administrator to require them to do so.

When their accounts are configured to allow them, subscribers can use the Cisco Unity phone conversation or the Cisco Unity Assistant to set their phone passwords. Neither the Cisco Unity conversation nor the Cisco Unity Assistant require subscribers to enter their old phone passwords to reset them.

Note that AMIS, Bridge, Internet, and VPIM subscribers cannot log on to Cisco Unity by phone, use the Cisco Unity Assistant, or use the Cisco Unity Inbox.

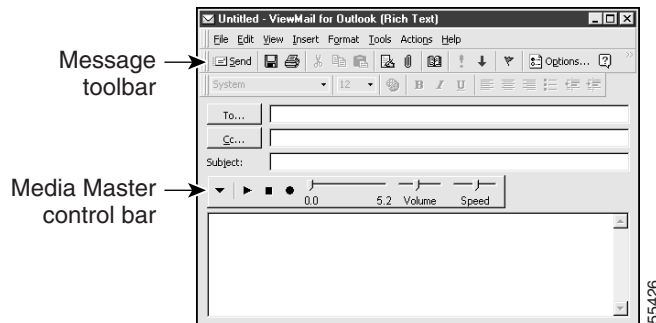
Related Documentation

- For information on specifying the minimum length for phone passwords, and the other ways in which you can secure phone access, such as specifying that Cisco Unity check for trivial passwords, prohibit the use of blank phone passwords and passwords that never expire, and maintain a record of previously used passwords, see the “Password and Account Policy Management” chapter of the *Security Guide for Cisco Unity*. The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.
- For additional security, you can set up Cisco Unity subscriber accounts to use a secure logon method known as two-factor user authentication. To learn more, see the “Authentication for Cisco Unity Applications” chapter of the *Security Guide for Cisco Unity*. The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.
- For suggestions on how to handle distributing initial phone passwords to subscribers, see the “Subscriber Orientation” section on page 29-1.

Setting Up Cisco Unity ViewMail for Microsoft Outlook

By using ViewMail, Cisco Unity subscribers can send and manage voice, fax, and e-mail messages from their Outlook Inbox. Subscribers can use ViewMail to send voice messages to other subscribers, to non-Cisco Unity subscribers, and to public distribution lists. They can play and record voice messages by using the Media Master control bar, as depicted in [Figure 28-1](#). (Cisco Unity may require that subscribers enter their credentials when they use the phone as a playback or recording device for the Media Master, such as when subscriber workstations are in a different domain than Cisco Unity.)

Figure 28-1 Cisco Unity ViewMail for Microsoft Outlook



Task List for Setting Up Cisco Unity ViewMail for Microsoft Outlook

ViewMail is not a licensed feature, nor does it require that you give subscribers special class of service (COS) privileges or passwords to use it. However, ViewMail must be installed on each subscriber workstation. Complete the following tasks to set up ViewMail for subscribers:

1. Review the *Release Notes for Cisco Unity ViewMail for Microsoft Outlook*, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html. The document specifies the requirements and procedures for installing ViewMail.
2. Optional: Set up ViewMail to download messages before playing them and to save only the message headers for sent messages. See the “[Customizing ViewMail for Optimal Performance](#)” section on page 28-4.

Customizing ViewMail for Optimal Performance

If subscribers play recordings by using computer speakers in a low bandwidth deployment (for example, with a slow modem or in a branch office), they should download messages before playing them for best performance and quality. (By default, messages are streamed from the Cisco Unity server during playback.)

You can also customize ViewMail to reduce the amount of disk space needed for storing sent messages on subscriber workstations, so that it saves only the message headers for voice messages that subscribers send, and not the message recordings.

Use the following procedures to set up either of these options on subscriber workstations. Subscribers can also see ViewMail Help or the *Cisco Unity User Guide* to set up these options on their own.

To Download Messages Before Playing Them

-
- Step 1** On the Outlook Tools menu, click **ViewMail Options**.
 - Step 2** Click the **Playback** tab.
 - Step 3** Check the **Download Audio Before Playing** check box.
 - Step 4** Click **OK** to save your changes.
-

To Save Only Message Headers

-
- Step 1** On the Outlook Tools menu, click **ViewMail Options**.
- Step 2** Click the **General** tab.
- Step 3** Check the **Keep Only Message Header in the Sent Items Folder** check box.
- Step 4** Click **OK** to save your changes.
-

Setting Up the Cisco Personal Communications Assistant

Subscribers use the Cisco Personal Communications Assistant (PCA) to access the Cisco Unity Assistant and the Cisco Unity Inbox. The Cisco Unity Assistant is a website that gives subscribers the ability to customize personal settings—including recorded greetings and message delivery options—on their workstations. The Cisco Unity Inbox website lets subscribers listen to, compose, reply to, forward, and delete voice messages, and with the fax option, manage fax messages. (The Cisco Unity Inbox is a licensed feature, and can be accessed only if it is purchased.)

The Cisco PCA is not a licensed feature, nor are subscribers required to have COS rights to access it. Any Cisco Unity subscriber can access the Cisco PCA at <http://<Cisco Unity server>/ciscopca>. (Note that the URL is case-sensitive.) However, subscribers do require proper COS rights to the Cisco Unity Assistant and/or the Cisco Unity Inbox.

Task List for Setting Up the Cisco Personal Communications Assistant

The Cisco PCA is installed on the Cisco Unity server during installation. To allow subscribers to access it, you do not need to install any additional files on subscriber workstations; however, you must complete the following tasks:

1. Confirm that the directory in which Cisco Unity is installed (the default directory is CommServer) and all subdirectories under that directory are excluded from virus scanning. (Typically, this is done during Cisco Unity installation.) See the virus-scanning software Help for information on excluding directories from scanning.
2. As applicable, give subscribers proper COS rights to the Cisco Unity Assistant and/or the Cisco Unity Inbox. See the [“Creating, Modifying, Assigning, and Deleting Classes of Service” section on page 19-2](#).
3. On each subscriber workstation, configure the browser so that Cisco PCA pages display properly and the pages are presented in the appropriate language. See the [“Configuring Subscriber Browsers to Use the Cisco PCA” section on page 28-6](#).
4. Optional: Customize the Cisco Unity Inbox to download messages before playing them. See the [“Customizing Cisco Unity Inbox for Low Bandwidth Deployments” section on page 28-7](#).
5. Optional: Exclude return receipts from the Cisco Unity Inbox. (Return receipts are delivery and read receipts.) For details on setting up this functionality, see Advanced Settings tool Help (in the Unity Settings list, click Unity Inbox—Exclude Return Receipts from the Inbox). The Advanced Settings tool is available in Tools Depot.

6. Optional: Specify that the Cisco Unity Inbox never asks subscribers to confirm deletions, or that subscribers are only asked to confirm their choice if deleting an item will delete it permanently. For details on setting up this functionality, see Advanced Settings tool Help (in the Unity Settings list, click Unity Inbox—Confirm Deletes). The Advanced Settings tool is available in Tools Depot.
7. Optional: As applicable, consider changing the default search scope for the Cisco PCA Address Book so that subscribers do not need to keep track of which Cisco Unity subscribers in your organization are listed in the local directory and which are listed in the global directory. See the [“Changing the Default Search Scope for the Cisco PCA Address Book”](#) section on page 28-8.
8. Optional: If your organization is migrating from a legacy voice messaging system to Cisco Unity in phases, you may want to consider preventing subscribers from using the Cisco Unity Assistant to add individual subscribers to private lists in the interim. See the [“Preventing Subscribers From Adding Individual Subscribers to Private Lists in the Cisco Unity Assistant”](#) section on page 28-8.
9. Optional: As a security precaution, you may want to prevent subscribers from saving any voice message—regardless of its sensitivity—to their hard disks by disabling the Copy to File option on the Options menu of the Media Master control bar in the Cisco Unity Inbox. To learn more, see Advanced Settings tool Help (in the Unity Settings list, click Unity Inbox—Disable Copy to File Option in Media Master). The Advanced Settings tool is available in Tools Depot.

Configuring Subscriber Browsers to Use the Cisco PCA

To allow subscribers to access the Cisco PCA, configure their browsers to:

- Enable Active scripting
- Download and run ActiveX controls
- Enable Java scripting
- Accept all cookies
- Automatically check for newer versions of temporary Internet files
- Enable Medium-High privacy

In addition, on workstations that are running Windows Vista and Internet Explorer 7:

- For Trusted Sites, uncheck the **Enable Protected Mode** check box.
- Add the URL for the Cisco PCA website (<http://<Cisco Unity server name>/ciscopca>) to the list of trusted sites.

To change the GUI language used in the Cisco Personal Communications Assistant (PCA), select a language in the browser. The language selected in the browser must be one of the languages that the Cisco PCA offers. For a list of supported languages, see the “Available Languages for Cisco Unity Components” section of the applicable *Release Notes for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Bookmarking Web Pages

When subscriber browser settings are set to cache temporary Internet pages automatically, subscribers can create a bookmark or Favorite to access a Cisco Unity Assistant or Cisco Unity Inbox web page, but the page will be read-only. Explain to subscribers that they should bookmark the Cisco PCA home page, rather than individual pages in the Cisco Unity Assistant and the Cisco Unity Inbox. (Subscribers should not change their browser settings as a workaround; when the browser is not set to automatically check for newer versions of temporary Internet files, the Media Master control is not displayed correctly.)

Customizing Cisco Unity Inbox for Low Bandwidth Deployments

If subscribers play recordings by using computer speakers in a low bandwidth deployment (for example, with a slow modem or in a branch office), they should download messages before playing them for best performance and quality.

To customize the Cisco Unity Inbox so that messages are downloaded rather than streamed from the Cisco Unity server during playback, use the following procedure to change the registry setting on each subscriber workstation (as applicable). As a best practice, we do not recommend that you allow subscribers to set this up on their own.

To Customize the Cisco Unity Inbox to Download Messages Before Playing Them

Step 1 On the subscriber workstation, on the Windows Start Menu, click **Run**.

Step 2 Start **Regedit**.



Caution Changing the wrong registry key or entering an incorrect value can cause the server to malfunction. Before you edit the registry, confirm that you know how to restore it if a problem occurs. (See the “Restoring” topics in Registry Editor Help.) If you have any questions about changing registry key settings, contact Cisco TAC.

Step 3 If you do not have a current backup of the registry, click **Registry > Export Registry File**, and save the registry settings to a file.

Step 4 Expand the registry key

HKEY_CURRENT_USER\Software\Cisco Systems\Cisco Unity\Media Master\Profiles

Step 5 For the applicable subscriber profile, expand the **Audio Playback Devices\Phone** key.

Step 6 If the DWORD value called Buffer Count does not exist, create it:

- a. On the Edit menu, click **New DWORD Value**, name it **Buffer Count**, and then press **Enter**.
- b. In the Edit DWORD Value window, name the new DWORD **Buffer Count** and click **Decimal**.

Step 7 Double-click the DWORD, **Buffer Count**.

Step 8 In the Value Data field, enter **3**.

Step 9 Click **OK**.

Step 10 If the DWORD value called Buffer Size does not exist, create it:

- a. On the Edit menu, click **New DWORD Value**, name it **Buffer Size**, and then press **Enter**.
- b. In the Edit DWORD Value window, name the new DWORD **Buffer Size** and click **Decimal**.

Step 11 Double-click the DWORD, **Buffer Size**.

Step 12 In the Value Data field, enter **300000**.

Step 13 Click **OK**.

Step 14 Close the **Registry Editor**.

You do not need to restart the workstation for the changes to take effect. TRUE?

Changing the Default Search Scope for the Cisco PCA Address Book

By default, the search scope for the Cisco PCA Address Book is set to the local directory. As a possible convenience to subscribers in your organization, you may want to change the default search scope to the global directory instead. When this is done, subscribers can search for subscribers at different locations without having to change the search scope themselves. In addition, subscribers will not need to keep track of which Cisco Unity subscribers are listed in the local directory and which are listed in the global directory.

Changing the default search scope for the Cisco PCA Address Book changes the default search scope for the following user interfaces:

- The Find Names and Check Names dialog boxes in the Cisco Unity Inbox, which subscribers use to resolve addressing when they send messages.
- The Find Names dialog box in the Cisco Unity Assistant, which subscribers use to add members to private lists.

Use the following procedure to set the global directory as the default search scope for the Cisco PCA Address Book. The change affects all subscribers that are associated with the Cisco Unity server.

Regardless of the default search scope that you specify here, subscribers can still switch between the local and global directory as they use the Cisco PCA Address Book in the Cisco Unity Inbox and Cisco Unity Assistant.

To Set the Default Search Scope to the Global Directory for the Cisco PCA Address Book

-
- Step 1** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
 - Step 2** In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.
 - Step 3** In the Unity Settings pane, click **Unity Inbox and Assistant—Set Default Address Book Search Scope**.
 - Step 4** In the New Value list, click **1**, and then click **Set** so that the Address Book searches for subscribers within the dialing domain.
 - Step 5** When prompted, click **OK**.
 - Step 6** Click **Exit**.
- You do not need to restart Cisco Unity to enable the change.
-

Preventing Subscribers From Adding Individual Subscribers to Private Lists in the Cisco Unity Assistant

In the transition from a legacy voice messaging system to Cisco Unity, your organization may choose to migrate users to Cisco Unity in phases. As a result, Cisco Unity will likely support both regular subscribers and “external” subscribers—Bridge, AMIS, or VPIM contacts (as applicable)—at the same time. Regular subscribers can send messages to external subscribers, and even add them to their private distribution lists during the transition.

However, once external subscribers are converted into regular Cisco Unity subscribers, they are automatically removed from all private lists without notifying private list owners. When this occurs, subscribers may continue to send messages to their private lists without realizing that some of their intended recipients no longer receive them.

When convenient and practical, Cisco Unity Administrators should notify subscribers when external subscribers are converted to regular subscribers, notifying subscribers that they should re-add the newly migrated subscribers to existing private lists, as applicable. During the migration phase, you may also want to consider preventing subscribers from adding subscribers to their private lists in the Cisco Unity Assistant, and asking them not to use the Cisco Unity phone menus to do so—at least until the migration process is complete.

Use the following procedure to prevent all subscribers who are associated with the Cisco Unity server from adding individual subscribers to their private lists in the Cisco Unity Assistant. The procedure does not prevent subscribers from using the Cisco Unity phone menus to add regular and external subscribers to their private lists, nor does it prevent subscribers from addressing messages to regular and external subscribers.

To Prevent Subscribers From Adding Individual Subscribers to Private Lists in the Cisco Unity Assistant

- Step 1** On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 2** In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.
- Step 3** In the Unity Settings pane, click **Unity Assistant—Do Not Allow Subscribers to Add Subscribers to Private Lists**.
- Step 4** In the New Value list, click **1**, and then click **Set** so that when subscribers add members to their lists in the Cisco Unity Assistant, the Find Names dialog box does not display the Subscribers tab. (Subscribers can continue to add distribution lists to their lists from the Distribution Lists tab.)
- Step 5** When prompted, click **OK**.
- Step 6** Click **Exit**.

You do not need to restart Cisco Unity to enable the change.

Securing and Changing Cisco PCA Passwords

Subscribers enter their Active Directory account user names and passwords to log on to the Cisco PCA. (Note that Cisco PCA passwords are not related to Cisco Unity phone passwords, nor are they synchronized with them.)

You can change subscriber passwords by using Active Directory Users and Computers after you create subscriber accounts. Each subscriber should be assigned a unique password. It is a good idea to specify a long—eight or more characters—and non-trivial password. Encourage subscribers to follow the same practice whenever they change their passwords, or set your domain account policy in Active Directory to require them to do so. Subscribers cannot use the Cisco Unity phone conversation or the Cisco Unity Assistant to change their Cisco PCA passwords, nor can administrators change them in the Cisco Unity Administrator. Instead, subscribers can change their Cisco PCA passwords only in Windows by pressing Ctrl-Alt-Delete and then clicking Change Password. (If the Cisco Unity server is in a different domain than the one that subscribers typically access with their Active Directory passwords, subscribers will need to specify the domain name for the Cisco Unity server.)

**Note**

Subscribers may assume that their phone and Cisco PCA passwords are the same. As a result, they may think that they are changing both passwords when Cisco Unity prompts them to change their phone password during first-time enrollment. For this reason, you may find that many subscribers do not consider securing their Cisco PCA passwords in Windows, even though you request that they do so.

The initial password that subscribers use to access the Cisco PCA depends on how the subscriber accounts were created.

Related Documentation

To understand how authentication works with the Cisco PCA, and any security issues that may affect your organization, see the “Authentication for Cisco Unity Applications” chapter of the *Security Guide for Cisco Unity*. The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

Defining Cisco PCA Logon, Password, and Lockout Policies

The account policy that you specify on the Authentication page in the Cisco Unity Administrator determines how Cisco Unity handles situations when subscribers attempt to log on to the Cisco PCA and repeatedly enter incorrect passwords; whether subscribers can use blank passwords; the number of failed logon attempts that Cisco Unity allows before the subscriber account cannot be used to access the Cisco PCA; and the length of time that a user remains locked out.

In addition, you can use the settings on the Authentication page to specify whether the Log On page for the Cisco PCA offers subscribers the following options:

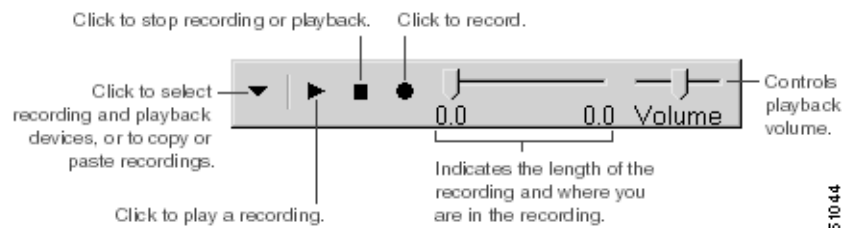
- Remember User Name
- Remember Password
- Remember Domain

When subscribers specify that Cisco Unity will remember their user name, password, or domain, subscribers will not have to enter them the next time that they log on to the Cisco PCA. Instead, the fields are automatically populated in the Log On page. Allowing subscribers to specify whether Cisco Unity will remember their credentials may reduce support desk requests for the information. However, you may not want the Log On page to offer subscribers the above options for security reasons. If this is the case, you can uncheck the Remember Logons for __ Days check box on the Authentication page to prevent the options from appearing on the Cisco PCA Log On page, and to require that subscribers enter their user name, password, and domain each time that they log on to the Cisco PCA.

To customize the logon, password, and lockout policies that Cisco Unity applies when subscribers use the Cisco PCA to access Cisco Unity, see the “[Authentication Settings](#)” section on page 11-1.

Setting Up the Media Master

The Media Master control bar appears on each page of the Cisco Unity Assistant and the Cisco Unity Inbox where subscribers can make and play recordings—either by using the phone, or by using the computer microphone and speakers and clicking the Media Master controls. See [Figure 28-2](#).

Figure 28-2 Media Master Control Bar

The first time that subscribers open a Cisco Unity Assistant or a Cisco Unity Inbox page that contains the Media Master (or when they access a web page that contains the Media Master and there is a newer version available), subscribers are prompted to install it. If they choose not to install, subscribers will be prompted to install each time that they visit a web page which contains the Media Master. When they indicate that they want to install it, the Media Master installs automatically, as long as subscribers have local administrative rights to their workstations. On subsequent visits to web pages that contain the Media Master, it is created from the locally installed copy.

To learn more about how the Media Master works and how to set up subscriber workstations to use it, see the following sections:

- [Task List for Setting Up the Media Master, page 28-11](#)
- [What Happens When Subscribers Use the Phone as Their Recording and Playback Device, page 28-12](#)
- [What Happens When Subscribers Use a Computer Microphone and Speakers as Their Recording and Playback Device, page 28-13](#)
- [How Subscribers Specify Their Recording and Playback Device Preferences, page 28-13](#)

Task List for Setting Up the Media Master

Complete the following tasks before subscribers start using Cisco Unity applications that offer the Media Master:



Note The Media Master control bar relies on DCOM (Distributed Component Object Model), and does not work through a firewall that blocks DCOM communications. Keep this in mind when setting up subscribers for remote access.

1. To allow subscribers to use the phone as a recording and playback device, specify that Cisco Unity has at least one voice messaging port designated for this purpose (see the [“Voice Messaging Port Settings” section on page 11-2](#) for more information). Alternatively, provide sound cards, speakers, and microphones to subscribers who do not want to use the phone as their recording and playback device.

When determining which recording and playback devices that you want subscribers to use, the same considerations apply as when you select the device to use with Media Master in the Cisco Unity Administrator. Review the [“Determining Which Recording and Playback Device to Use” section on page 27-2](#) for the list of considerations.

2. Configure subscriber browsers to download and run ActiveX controls or tell subscribers to do so. Also, make sure that subscribers have local administrative rights to their workstations so that the Media Master installs properly. (Subscribers who do not have their browsers configured to download and run ActiveX controls or do not have the Media Master properly installed will see a red X instead of [Figure 28-2](#).)
3. For subscribers who will play recordings by using computer speakers in a low bandwidth deployment (for example, with a slow modem or in a branch office), set up Cisco Unity ViewMail for Microsoft Outlook and the Cisco Unity Inbox to download messages before playing them; this will result in the best performance and quality. As applicable, see the [“Customizing ViewMail for Optimal Performance”](#) section on page 28-4 and the [“Customizing Cisco Unity Inbox for Low Bandwidth Deployments”](#) section on page 28-7.
4. For subscribers who use Cisco Unity ViewMail for Microsoft Outlook, disable personal firewalls on their workstations, or remove the applicable software. Security software that offers personal firewalls for individual workstations causes ViewMail to stop functioning when subscribers use the phone as a playback device. Alternatively, set up subscriber workstations so that they can play messages in ViewMail with computer speakers.

What Happens When Subscribers Use the Phone as Their Recording and Playback Device

When subscribers use the phone as a recording and playback device in the Cisco Unity Administrator, the Cisco Unity Assistant, the Cisco Unity Inbox, or ViewMail, the following occurs:

1. The subscriber clicks the applicable option in the Cisco Unity application to make or play a voice recording.
2. When subscriber workstations are in a different domain than the Cisco Unity server, Cisco Unity will prompt subscribers to enter credentials. Subscribers are only prompted to enter their credentials once per Outlook session.
3. The Cisco Unity application asks the Cisco Unity server to place a call to the extension specified in the Media Master, and Cisco Unity calls the extension.

By default, when Cisco Unity makes the call, it waits for the subscriber phone to ring four times before displaying the message, “The specified phone number does not answer.” You can adjust the maximum number of rings that Cisco Unity waits for when making such calls. See [Advanced Settings tool Help](#) (in the Unity Settings list, click Administration—Set Maximum Number of Rings to Wait For TRAP Calls). The Advanced Settings tool is available in Tools Depot.

4. When making a recording, the subscriber answers the phone, and records the message, name, or greeting. The recording and storage codec specified for the Cisco Unity server determines the format in which the recording is saved and stored on the Cisco Unity server. When the subscriber hangs up, the Cisco Unity application tells the Cisco Unity server that the recording is finished.

When playing a recording, the subscriber answers the phone, and the application asks Cisco Unity to play the message. Cisco Unity streams the recording over the phone.

What Happens When Subscribers Use a Computer Microphone and Speakers as Their Recording and Playback Device

When subscribers use a computer microphone and speakers as a recording and playback device in the Cisco Unity Assistant, the Cisco Unity Inbox, or ViewMail, the following occurs:

1. The subscriber clicks the applicable option in the Cisco Unity application to make or play a voice recording.
2. When making a recording, the subscriber begins speaking into the microphone. When the subscriber clicks the applicable option to stop recording, the Cisco Unity application tells the Cisco Unity server that the recording is finished. The recording is saved and stored in the G711 codec format—even when this is not the recording and storage codec specified for the Cisco Unity server. The same is true when the subscriber uses the Paste option on the Media Master control bar to insert a WAV file that is stored on the computer into the recording; the file is converted (if applicable) and saved on the Cisco Unity server in the G711 format.

When playing a recording, Cisco Unity 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 subscriber workstation.

How Subscribers Specify Their Recording and Playback Device Preferences

Subscribers can set their own recording and playback device preferences from the Media Master Options menu. Refer subscribers to the “Overview: Changing Recording and Playback Settings” chapter of the *Cisco Unity User Guide*. The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_user_guide_list.html.

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

- A subscriber who is logged on to the Cisco PCA or ViewMail can change recording and playback devices from any Media Master Options menu. The recording and playback devices that a subscriber chooses apply to all Cisco Unity applications, as long as the subscriber accesses the applications from the same workstation on which the changes were initially made.
- If multiple subscribers share the same workstation, each subscriber who uses the workstation must indicate a choice of recording and playback devices.
- If a subscriber has updated the choice of recording and playback devices from one workstation, but also accesses the Cisco Unity Assistant, the Cisco Unity Inbox, or ViewMail on a different workstation (for example, from a computer at home), the choice of recording and playback devices must be indicated for the second workstation as well.

Setting Up FaxMail

Integrating a fax server with Cisco Unity allows subscribers to manage their fax messages.

To allow subscribers to manage fax messages over the phone or from the Cisco Unity Inbox, assign them to a class of service (COS) that has FaxMail enabled. (All Unified Messaging subscribers, regardless of COS, can manage fax messages in their e-mail Inboxes.)

Setting Up Mobile Message Access for BlackBerry

The Mobile Message Access for BlackBerry is not a licensed feature, nor does it require that you give subscribers special class of service (COS) privileges. As long as their BlackBerry devices are connected to a BlackBerry server that has a Mobile Message Access for BlackBerry plug-in installed, and the devices are configured properly, subscribers can use their BlackBerry devices to access Cisco Unity voice messages on a Cisco Unity server that is set up for Unified Messaging.

Voice messages appear along with other messages in the BlackBerry Inbox. To play a Cisco Unity voice message, subscribers use their BlackBerry device to open the message and click the associated link. Cisco Unity calls the phone number specified for message playback, and when the subscriber answers the call, the message begins to play. (Note that the restriction tables associated with the subscriber class of service may prohibit them from specifying certain phone numbers for message playback.)

The menu options available during and after message playback are the same as those available when subscribers log on to Cisco Unity to play messages over the phone. After saving or deleting a message, subscribers can select another message from the BlackBerry Inbox to play, or they can press * to log on to Cisco Unity to perform other tasks.

Task List for Setting Up Mobile Message Access for BlackBerry

Do the following tasks to set up Mobile Message Access for BlackBerry:

1. Optional: Set up Cisco Unity to use the Secure Sockets Layer (SSL) protocol in its communications with the BlackBerry server so that the data exchanged between the Cisco Unity server and the BlackBerry server is sent over an encrypted HTTPS connection. In addition, consider preventing the BlackBerry device from displaying the resulting security alert.

For detailed instructions, see the task list in the “Manually Setting Up the System to Use SSL” section in the “Using SSL to Secure Client/Server Connections” chapter of the *Security Guide for Cisco Unity*, available at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

2. To allow subscribers to use the phone as a recording and playback device, specify that Cisco Unity has at least one voice messaging port designated for this purpose.

For more information, see the “Voice Messaging Port Settings” section on page 11-2.

3. Install the Mobile Message Access for BlackBerry plug-in on the BlackBerry server. See the *Release Notes for Cisco Unity Mobile Message Access for BlackBerry* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html. The document specifies the requirements and procedures for installing the Mobile Message Access for BlackBerry plug-in.

4. Provide subscribers with the procedures in the *User Guide for Mobile Message Access for BlackBerry* at

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_user_guide_list.html.

In addition, the first time that they use the BlackBerry device to access Cisco Unity voice messages, they will need to specify the phone number that Cisco Unity calls to play messages.