



## Setting Up Client Applications

---

Cisco Unity subscribers can send and manage voice, fax, and e-mail messages by using a touchtone phone or by using ViewMail and the Cisco Unity Inbox on their computers. In addition, the Cisco Unity Assistant lets subscribers personalize the Cisco Unity phone settings that control how they interact with Cisco Unity by phone. 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.

This chapter reviews the preparations necessary for setting up subscriber phones and computers so that subscribers can use Cisco Unity client applications. See the following sections for details:

- [Setting Up Subscriber Phones, page 5-1](#)—This section summarizes what you must do so that subscribers can access Cisco Unity by phone.
- [Setting Up ViewMail for Microsoft Outlook, page 5-2](#)—This section lists the tasks for setting up e-mail clients for unified messaging subscribers.
- [Setting Up the Cisco Personal Communications Assistant, page 5-6](#)—This section provides a list of tasks to perform so that subscribers can use the Cisco Personal Communications Assistant to access Cisco Unity.
- [Setting Up Recording and Playback Devices, page 5-9](#)—This section explains how subscribers make and play recordings from the various Cisco Unity applications, and what you need to do to set them up.

When you have set up subscribers to use the Cisco Unity client applications, review the tasks presented in the [“Subscriber and Operator 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 computers, refer to the *Compatibility Matrix: Cisco Unity and the Software on Subscriber Workstations*, available on Cisco.com at

[http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products\\_device\\_support\\_tables\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_device_support_tables_list.html).

## Setting Up Subscriber Phones

For each subscriber phone, do the following tasks:

- Enable call forwarding to Cisco Unity, 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 for each subscriber, for example, to determine whether callers are put on hold or sent directly to the subscriber greeting.

- Enable easy message access, 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.

If desired, you can also change the phone password for individual subscribers. By default, subscriber template settings include an initial phone password for subscribers, which is 12345. You can change this setting for an individual subscriber or use the Bulk Edit utility in the Tools Depot to change this setting for multiple existing subscribers (see the “[Subscriber Settings](#)” chapter for details). For increased security, you can prohibit the use of blank phone passwords (see the “[Phone Password Settings](#)” section on page 17-1 for details.)

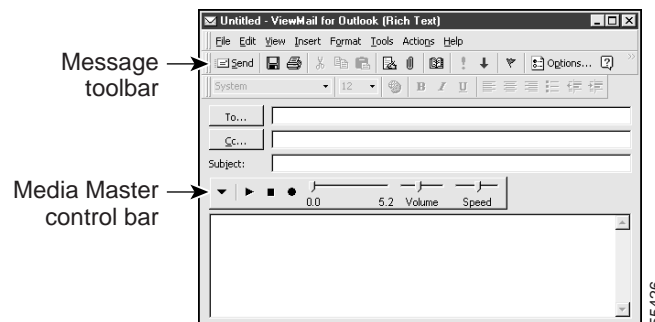
Subscribers can use the Cisco Unity phone conversation to change their phone passwords. Depending on the class of service associated with a subscriber account, they may also be able to use the Cisco Unity Assistant to change their phone passwords.

## Setting Up ViewMail for Microsoft Outlook

With 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 5-1](#).

Cisco Unity may require that subscribers enter their credentials when they use the phone as a playback or recording device in ViewMail for Outlook, such as when subscriber computers are in a different domain than Cisco Unity.

**Figure 5-1** ViewMail for Microsoft Outlook



ViewMail is not a licensed feature, nor does it require that you give subscribers special class of service privileges or passwords to use it. To set up ViewMail for subscribers in your organization, see the following sections in this chapter:

- [Deploying ViewMail for Outlook, page 5-3](#)—There are several ways to deploy ViewMail to subscriber workstations.
- [Upgrading From an Earlier Version of ViewMail, page 5-4](#)—This section explains how to upgrade subscriber workstations to the latest version of ViewMail.
- [Customizing ViewMail for Optimal Performance, page 5-5](#)—This section explains how remote subscribers in low bandwidth deployments can improve ViewMail performance, and how subscribers can reduce the amount of disk space needed for storing sent messages on their computers.

## Deploying ViewMail for Outlook

You can install ViewMail for Outlook on subscriber workstations throughout your organization in a number of ways. Typically, organizations provide subscribers with network access to the ViewMail setup application so that they can set it up themselves.

For example, you can:

- Install ViewMail from the Cisco Unity CD. To do so, see the procedure, [To install ViewMail from CD or network drive, page 5-4](#).
- Install ViewMail on a shared network drive that subscribers can access so that they can install it themselves. You can also install ViewMail for multiple subscribers who share a workstation.
- Utilize software publishing tools, such as Microsoft IntelliMirror and version 1.2 or 2.0 of Systems Management Server (SMS), to deploy ViewMail to multiple subscriber workstations at one time. (When using IntelliMirror, deploy ViewMail by assigning or publishing it to a computer, rather than to an individual user.)

You can also use IntelliMirror or SMS for future upgrades of ViewMail. For details on using either of these software publishing tools, refer to the Microsoft website.

- Deploy ViewMail with Microsoft Office, as part of the Office 2000 or Office XP suites.

By default, ViewMail files are installed to the C:\Program Files\ViewMail directory. You can change this if desired. ViewMail installs and uses the following files and registry keys:

---

### Files Utilized by ViewMail (in the C:\Winnt directory)

---

AvVox.acm

---

AvTsmSL.dll

---

AvWavSL.dll

---

SL\_g729a.acm

---



---

### Registry Keys Utilized by ViewMail

---

HKLM/Software/Microsoft/Exchange/Client/Extensions/Viewmail Extensions

---

HLU/Software/Active Voice

---

HKLM/Software/Active Voice

---

Use the following procedure to install ViewMail from a CD or a network drive on the workstations used by subscribers, as appropriate. Before doing so, consider the following:

- To install ViewMail, you must have local administrator rights on the subscriber computer.
- If subscribers are already using a previous version of ViewMail, see the [“Upgrading From an Earlier Version of ViewMail” section on page 5-4](#) before proceeding.
- Outlook should not be running and virus-scanning services should be disabled on subscriber computers when ViewMail is installed.
- Do not install Outlook on the Cisco Unity server as it is incompatible with Exchange.
- When installing a new version of Microsoft Outlook, you must first uninstall ViewMail. After you have installed Outlook, reinstall ViewMail. Otherwise, ViewMail will seem to be installed properly with the new version of Outlook, but it will not work.

### To install ViewMail from CD or network drive

- 
- Step 1** If applicable, remove any previously installed version of ViewMail 2.4(6.x) before installing ViewMail 4.0(1). To do so, follow the instructions in the [“Uninstalling ViewMail 2.4\(6.x\)”](#) section on page 5-4, and then continue with [Step 2](#) below.
- Step 2** Browse to the ViewMail directory on Cisco Unity Disc 1 or the network folder to which you copied the ViewMail files.
- Step 3** In the ViewMail directory, browse to the appropriate folder (the ViewMail directory has a different folder for each supported language of ViewMail).
- Step 4** Double-click the **ViewMail.msi** file.




---

**Note** If your version of Windows NT, Windows ME or Windows 98 does not support MSI packages, you can download an MSI installer from Microsoft (search the Microsoft website for “Windows Installer downloads”). Also, Windows Installer logging is not on by default. For details on how to turn logging on before installing ViewMail, or afterward for troubleshooting purposes, search for MSI Logging topics on the Microsoft website.

---

- Step 5** Follow the on-screen prompts to complete the installation.
- 

## Upgrading From an Earlier Version of ViewMail

If subscribers are using ViewMail 2.4(6.x), see the [“Uninstalling ViewMail 2.4\(6.x\)”](#) section on page 5-4 for specific instructions on how to uninstall 2.46 versions of ViewMail.




---

**Note** It is not necessary or advisable to uninstall 3.0(x) or 3.1(x) versions of ViewMail. Attempting to do so may result in a Dr. Watson error (refer to Caveat CSCdv16845, page 7).

---

When you are ready to install ViewMail 4.0(1), do so in the same directory used for the previous install of ViewMail. See the [“Deploying ViewMail for Outlook”](#) section on page 5-3 for a detailed procedure.

## Uninstalling ViewMail 2.4(6.x)

Any previously installed 2.4(6.x) version of ViewMail and the associated LightningFAX registry keys, if applicable, must be removed from client workstations before ViewMail 4.0(1) is installed. The uninstall process removes ViewMail menu items and the ViewMail toolbar icon from the Outlook Inbox.

Note that the first time that the subscriber receives a voice message after ViewMail is uninstalled, the ViewMail icon identifies the message as a voice message. When the subscriber tries to open the message, Outlook displays a message informing the subscriber that the message form is not available. However, the error message does not prevent the subscriber from opening the message. Subsequent voice messages appear as e-mail with WAV attachments without the ViewMail icon, and no error message is displayed when a subscriber open them.

### To remove ViewMail and associated LightningFAX registry keys

---

- Step 1** On each client workstation running ViewMail, on the Windows Start menu, click **Settings > Control Panel > Add/Remove Programs**.
- Step 2** In the Currently Installed Programs list, click **View Mail for Outlook**, and click **Change/Remove**.
- Step 3** Follow the on-screen prompts to remove ViewMail for Outlook. If prompted to delete a shared file, such as a DLL, click **No to All**.
- Step 4** If the system was using LightningFAX, start Regedit.



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

---

- Step 5** 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 6** Remove the following registry keys:
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Management\ARPCache\LightningFAX 6.5 - PrintToMail.
  - HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet002\Control\Print\Monitors\LightningFAX.
- Step 7** Exit Regedit.
- 

## Customizing ViewMail for Optimal Performance

When subscribers use ViewMail 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.

You can also reduce the amount of disk space needed for storing sent messages on subscriber computers by customizing ViewMail 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 refer to the ViewMail online 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 or message delivery options—on their computers. The Cisco Unity Inbox website lets subscribers listen to, compose, reply to, forward, and delete voice 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 class of service rights to access it. Any Cisco Unity subscriber can access Cisco PCA at the following URL: `http://<Cisco Unity server>/ciscopca`. (Note that the URL is case-sensitive.) In version 3.1 and earlier, the Cisco Unity Assistant was known as the ActiveAssistant, or AA; the Cisco Unity Inbox was known as the Visual Messaging Interface, or VMI. Subscribers who use the following ActiveAssistant URLs will be automatically redirected to the Cisco PCA website:

- `http://<Cisco Unity server>/web/aa`
- `http://<Cisco Unity server>/ActiveAssistant`

Likewise, subscribers who use `http://<Cisco Unity server name>/web/vmi` will also be automatically redirected to the Cisco PCA website.

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. As appropriate, give subscribers proper class of service rights to the Cisco Unity Assistant and/or the Cisco Unity Inbox. See the [“Class of Service Features Settings”](#) section on page 12-10 for details.
2. Understand how authentication works with the Cisco PCA and the security issues that may affect your organization. See the [“About Cisco Personal Communications Assistant Authentication”](#) section on page 5-7 for details.
3. Confirm that you have defined an appropriate logon, password, and lockout policy for all subscribers who will access the Cisco PCA. See the [“Defining Subscriber Account Policies for Logons, Passwords, and Lockouts”](#) section on page 5-8.
4. Configure subscriber browsers to use Cisco Unity web applications. See the [“Configuring Subscriber Browsers To Use the Cisco PCA”](#) section on page 5-8 for details.

## About Cisco Personal Communications Assistant Authentication

Cisco Unity offers application-level authentication to allow subscribers to access the Cisco Personal Communications Assistant (PCA). This means that IIS is configured so that the Cisco PCA uses Anonymous authentication, and that Cisco Unity authenticates the credentials that subscribers enter when they log on to the Cisco PCA. Review the [“How authentication for the Cisco Personal Communications Assistant works”](#) section on page 5-7 for further details. (Note that unlike the Cisco Unity Administrator, you cannot change the authentication method that is used by the Cisco PCA.)

By default, when subscribers log on to the Cisco PCA, their user names and passwords are sent across the network to Cisco Unity in clear text. The information that a subscriber enters on the Cisco PCA pages is also not encrypted. For increased security, we recommended that you set up Cisco Unity to use the Secure Sockets Layer (SSL) protocol. To set up a web server like Cisco Unity to use SSL, you can either obtain a digital certificate from a Certificate Authority (CA), or you can use Microsoft Certificate Services available with Windows to issue your own certificate. (See the [“Setting Up Cisco Unity To Use SSL”](#) chapter for details.)

As a best practice, it is recommended that Cisco Unity administrators not use the same subscriber account to log on to the Cisco Unity Administrator, as they do to log on to the Cisco PCA.

### How authentication for the Cisco Personal Communications Assistant works

1. A Cisco Unity subscriber starts Internet Explorer and attempts to browse to the Cisco PCA website.
2. Internet Explorer tries to get the home page for the Cisco PCA from IIS.
3. IIS allows access to Cisco Unity based on the privileges for the IUSR\_[computer name] account. (This is the anonymous account that by default IIS uses for Anonymous authentication.)
4. Cisco Unity presents the Cisco Unity Log On page, which is displayed in the browser.
5. The Log On page prompts subscribers to enter their Windows domain account credentials, as shown in [Table 5-1](#).

**Table 5-1** Cisco Unity Log On Page for Windows Credentials

Field Name	Description
User Name	Subscribers enter the alias for the Windows domain account that is associated with their Cisco Unity subscriber account. (For example, they can enter <b>tcampbell</b> or they can enter the full path <b>tcampbell@&lt;domain name&gt;</b> .) If subscribers enter the full path for their alias, they do not need to complete the Domain field.
Password	Subscribers enter the password for their Windows domain account.
Domain	Subscribers enter the name of the domain in which their Windows domain account resides, unless they entered a full path for their alias in the User Name field. If that is the case, subscribers can leave this field blank.

6. Internet Explorer sends the credentials—in clear text—to Cisco Unity. (To solve this security problem, you can set up Cisco Unity to use SSL.)
7. Cisco Unity requests authentication of the credentials from Windows.

8. If Cisco Unity can authenticate the Windows credentials, Cisco Unity then confirms that there is a subscriber account associated with the Windows domain account used to authenticate the subscriber and that the subscriber account has COS rights to access the Cisco PCA. The process continues with Step 9.

If the credentials cannot be authenticated, Cisco Unity presents a web page that indicates that the subscriber does not have permission to view the Cisco PCA website.

9. If the subscriber account exists and it has the proper COS rights, Cisco Unity presents the first page of the Cisco PCA website, which is displayed in the browser.

If the subscriber account does not exist or does not have the proper COS rights, Cisco Unity presents a web page, which indicates that the subscriber does not have permission to view the Cisco PCA website.

## Defining Subscriber Account Policies for Logons, Passwords, and Lockouts

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; 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.

When you add a subscriber by using the Cisco Unity Administrator, subscriber template settings include initial Windows passwords that subscribers can use to access the Cisco PCA. The default password for new Windows accounts is 12345678. However, when you use either the Cisco Unity Administrator or the Cisco Unity Bulk Import wizard to create subscriber accounts by importing data from Exchange, the passwords that subscribers use to access the Cisco PCA is inherited from the Windows domain accounts.

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. However, for increased security, you can use the settings on the Authentication page to prohibit the use of blank passwords, even when the Windows account allows them. To customize the logon, password, and lockout policies that Cisco Unity applies whenever subscribers use the Cisco PCA to access Cisco Unity, see the [“Authentication Settings” section on page 26-11](#).

## 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.

If you set up Cisco Unity to use SSL, consider that the Cisco PCA website automatically uses an SSL connection every time that a subscriber points the browser to either website. However, until the digital certificate is added to the trusted root store on the subscriber computer, the browser will display a message to alert the subscriber that the authenticity of the site cannot be verified and therefore, its content cannot be trusted.

To prevent the browser from displaying the security alert, you can distribute the certificate to the trusted root store for all users in the domain by adding it to the Group Policy (see the “[Setting Up Cisco Unity To Use SSL](#)” chapter) or you can tell subscribers how to add the certificate to the trusted root store on their own computers by providing them with the following procedure.

Depending on your organization, it may be a good idea to provide subscribers with the following procedure—even if you distributed the certificate to the trusted root store for all users in the domain by adding it to the Group Policy, as the browser will display the security alert any time that subscribers access the Cisco PCA from a computer that does belong to a trusted domain (for example, a computer at home).

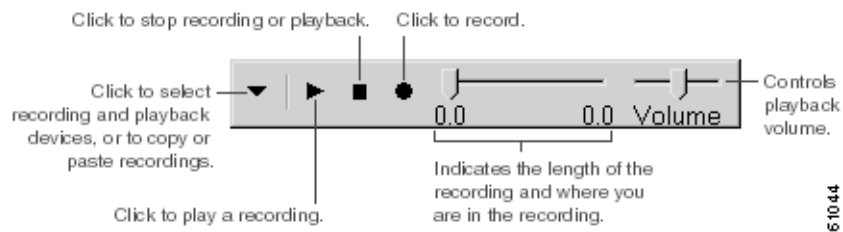
#### To add the Cisco Unity certificate to the trusted root store on subscriber computers

- 
- Step 1** On each subscriber computer, start Internet Explorer.
- Step 2** Go to **http://<the Certificate Authority server>/certsrv**.
- Step 3** On the Microsoft Certificate Services page, under Select a Task, click **Retrieve the CA Certificate Or Certificate Revocation List**.
- Step 4** Click **Next**.
- Step 5** Click the **Install This CA Certification Path** link.
- Step 6** When prompted, click **Yes** to add the certificate to the Root Store.
- 

## Setting Up Recording and Playback Devices

In the Cisco Unity Assistant, the Cisco Unity Inbox, and ViewMail, subscribers can make and play recordings—either by using the phone, or by using computer microphone and speakers, and clicking the Media Master controls. Subscribers with the appropriate class of service settings can also use the Media Master in the Cisco Unity Administrator to make and play recordings.

**Figure 5-2** Media Master Control Bar



See the following sections for more information:

- [Using the Phone as a Recording and Playback Device, page 5-10](#)
- [Using a Microphone and Speakers as the Recording and Playback Device, page 5-10](#)
- [Determining Recording and Playback Devices for Subscriber Use, page 5-10](#)
- [Specifying Recording and Playback Device Preferences in Cisco Unity Applications, page 5-11](#)

## Using the Phone as a 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:

- a. The subscriber clicks the appropriate option in the client application to make or play a voice recording.
- b. When subscriber computers 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.
- c. The client application asks Cisco Unity to place a call to the subscriber extension, and Cisco Unity calls the extension.
- d. When recording, the subscriber answers the phone, and begins recording the message, name, or greeting. When the subscriber hangs up, the client application tells Cisco Unity that the recording is finished.

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

Note that subscribers must manually change the server name field during failover and failback. Refer to the *Cisco Unity Failover Configuration and Administration Guide* for details, available on Cisco.com at [http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products\\_installation\\_and\\_configuration\\_guide\\_books\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guide_books_list.html).

## Using a Microphone and Speakers as the Recording and Playback Device

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

- a. The subscriber clicks the appropriate option in the client application to make or play a voice recording.
- b. When recording, the subscriber begins speaking into the microphone. When the subscriber clicks the appropriate option in the client application to stop recording, the client application tells Cisco Unity that the recording is finished.

When playing recordings, 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 computer.

## Determining Recording and Playback Devices for Subscriber Use

When determining recording and playback devices that you want subscribers use, consider the following:

- 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 subscribers to use the phone as a recording and playback device, Cisco Unity must have at least one port designated per session for this purpose (see the [“Voice Messaging Port Settings” section on page 26-13](#) for more information). Note that when a subscriber listens to messages or other recordings by using a computer microphone and speakers, no ports are used, which decreases the load on the Cisco Unity server and leaves ports open for other functions.
- You must provide sound cards, speakers, and microphones to subscribers who do not want to use the phone as their recording and playback device.
- Media Master relies on DCOM (Distributed Component Object Model), and does not work through a firewall. Keep this in mind when setting up subscribers for remote access.

## Specifying Recording and Playback Device Preferences in Cisco Unity Applications

Subscribers can set up their own recording and playback device preferences. For example, the Media Master Options menu allows subscribers to choose their own recording and playback devices. Media Master recording and playback settings are saved per user, per computer. This means that:

- A subscriber who is logged on to the Cisco Unity Administrator, 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 these applications from the same computer on which the changes were initially made.
- If multiple subscribers share the same computer, each subscriber who uses the computer must indicate a choice of recording and playback devices.
- If a subscriber has updated the choice of recording and playback devices from one computer, but also accesses the Cisco Unity Assistant, the Cisco Unity Inbox, or ViewMail on a different computer (for example, a computer at home), the choice of recording and playback devices must be indicated for the second computer as well.

