



CHAPTER 8

Installing and Configuring Cisco Unity Software

In this chapter, you do the following tasks in the order listed:

1. Determine whether to set up Cisco Unity to use SSL. See the [“Determining Whether to Set Up Cisco Unity to Use SSL”](#) section on page 8-2.



Note

Do Task 2. only on the first server that you install in the failover pair.

2. *If you plan to set up Cisco Unity to use SSL and want to use the Microsoft Certificate Services available with Windows to issue your own certificate:* Install the Microsoft Certificate Services component. See the [“Installing the Microsoft Certificate Services Component”](#) section on page 8-3.
3. Use the Cisco Unity Installation and Configuration Assistant to install and configure Cisco Unity, and to set up the Cisco Personal Communications Assistant to use SSL. See the [“Installing and Configuring Cisco Unity Software”](#) section on page 8-3.



Note

Do Task 4. only on the primary server in the failover pair.

4. Test the phone system integration. See the [“Testing the Phone System Integration”](#) section on page 8-16.
5. *If virus-scanning software is installed on the Cisco Unity server:* Exclude selected directories from scanning. See the [“Excluding Selected Directories from Virus Scanning”](#) section on page 8-16.
6. Delete Apache Tomcat sample directories. See the [“Deleting Apache Tomcat Sample Directories”](#) section on page 8-17.
7. *If you are setting up Cisco Unity to use SSL:* Set up the Cisco Unity Administrator and Status Monitor to use SSL. See the [“Setting Up the Cisco Unity Administrator and Status Monitor to Use SSL”](#) section on page 8-17.
8. *If Windows Server 2003 is installed on the Cisco Unity server:* Configure Internet Explorer. See the [“Configuring Internet Explorer to Display the Cisco Unity Administrator Correctly \(Windows Server 2003 Only\)”](#) section on page 8-19.



Note

Do Task 9. only on the first server that you install in the failover pair.

9. Secure the Example Administrator account against toll fraud. See the [“Securing the Example Administrator Account Against Toll Fraud”](#) section on page 8-21.

10. Move SQL Server databases and transaction logs. See the [“Moving the Data Store Databases and Transaction Logs”](#) section on page 8-21.
11. Install the latest Microsoft service packs qualified for use with Cisco Unity, if any. In addition, run the latest Cisco Unity Server Updates wizard to install the latest updates recommended for use with Cisco Unity. See the [“Installing the Latest Microsoft Service Packs and Updates”](#) section on page 8-24.
12. *If virus-scanning software or Cisco Security Agent for Cisco Unity is installed on the Cisco Unity server:* Re-enable virus-scanning services and the Cisco Security Agent service for Cisco Unity. See the [“Re-enabling Virus-Scanning and Cisco Security Agent Services”](#) section on page 8-24.
13. Secure Cisco Unity and the Cisco Unity server. See the [“Securing Cisco Unity and the Cisco Unity Server”](#) section on page 8-25.

When you are finished with this chapter, return to [Chapter 1, “Overview of Mandatory Tasks for Installing Cisco Unity”](#) to continue installing the Cisco Unity system.

**Note**

The tasks in the list reference detailed instructions in the Cisco Unity installation guide and in other Cisco Unity documentation. Follow the documentation for a successful installation.

Determining Whether to Set Up Cisco Unity to Use SSL

When subscribers log on to the Cisco Personal Communications Assistant (PCA), their credentials are sent across the network to Cisco Unity in clear text. The same is true when the Cisco Unity Administrator and the Status Monitor are configured to use the Anonymous authentication method. In addition, the information that subscribers enter on the pages of the Cisco PCA and of the Cisco Unity Administrator (regardless of which authentication method it uses) is not encrypted.

For increased security, we recommend that you set up Cisco Unity to use the Secure Sockets Layer (SSL) protocol. SSL uses public/private key encryption to provide a secure connection between servers and clients, and uses digital certificates to authenticate servers or servers and clients. (A digital certificate is a file that contains encrypted data that attests to the identity of an organization or entity, such as a computer.)

Using the SSL protocol ensures that all Cisco Unity subscriber credentials—as well as the information that a subscriber enters on any page of the Cisco Unity Administrator and the Cisco PCA—are encrypted as the data is sent across the network. In addition, when you set up Cisco Unity to use SSL, each time that a subscriber tries to access any Cisco Unity web application, the browser will confirm that it is connected with the real Cisco Unity server—and not an entity falsely posing as such—before allowing the subscriber to log on.

To set up a web server such as Cisco Unity to use SSL, you can either obtain a digital certificate from a certificate authority (CA) or use Microsoft Certificate Services available with Windows to issue your own certificate. (A CA is a trusted organization or entity that issues and manages certificates at the request of another organization or entity.) Cost, certificate features, ease of setup and maintenance, and the security policies practiced by the organization are some of the issues to consider when determining whether you should purchase a certificate from a CA or issue your own.

Information on third-party CAs, Microsoft Certificate Services, and SSL is widely available on the Internet, as well as in the Windows and IIS online documentation. Such sources can help you determine whether to use SSL and how to set up a web server to use it.

Installing the Microsoft Certificate Services Component

**Note**

If you do not plan to set up Cisco Unity to use SSL or if you want to use a digital certificate from a certificate authority to set up Cisco Unity to use SSL, skip this section.

Do the procedure in this section if you plan to set up Cisco Unity to use SSL and you want to use the Microsoft Certificate Services available with Windows to issue your own certificate. You may install the component on the Cisco Unity server or on another server.

To Install the Microsoft Certificate Services Component

- Step 1** On the server that will act as your certificate authority (CA) and issue certificates, on the Windows Start menu, click **Settings > Control Panel > Add/Remove Programs**.
- Step 2** Click **Add/Remove Windows Components**.
- Step 3** In the Windows Components dialog box, check the **Certificate Services** check box. Do not change any other items. When the warning appears about not being able to rename the computer, or to join or be removed from a domain, click **Yes**.
- Step 4** Click **Next**.
- Step 5** Click **Stand-alone Root CA**, and click **Next**. (A stand-alone CA is a CA that does not require Active Directory.)
- Step 6** Follow the on-screen prompts to complete the installation. For information, refer to the Windows documentation.

If a message appears that Internet Information Services is running on the computer and must be stopped before proceeding, click **OK** to stop the services.
- Step 7** In the Completing the Windows Components Wizard dialog box, click **Finish**.
- Step 8** Close the Add Remove Programs dialog box and Control Panel.

Installing and Configuring Cisco Unity Software

To install and configure Cisco Unity software, you use the Cisco Unity Installation and Configuration Assistant to run seven programs in a specific order. The programs:

- Check the system and install the Cisco Unity software.
- Install the Cisco Unity licenses.
- Configure the Cisco Unity services.
- Configure Cisco Unity for the message store.
- Set new default passwords for the Default Administrator and the Default Subscriber templates
- Integrate Cisco Unity with the phone system.
- Configure the Cisco Personal Communications Assistant to use SSL.

Do the following seven subsections in the order listed.

Starting the Cisco Unity Installation and Configuration Assistant and Installing Cisco Unity Software

From the Cisco Unity Installation and Configuration Assistant, you run the Cisco Unity Setup program first to install Cisco Unity. The Setup program checks the system, then installs the Cisco Unity software.


Caution

Do not install Cisco Unity remotely by using Windows Terminal Services or other remote-access applications, or the installation may fail.


Caution

Do not install features for which the system is not licensed, or Cisco Unity will shut down.

To Start the Assistant and Install the Cisco Unity Software

Step 1 Log on to Windows by using the Cisco Unity installation account.


Caution

If you have not already done so, disable virus-scanning and Cisco Security Agent services on the server, if applicable. Otherwise, the installation may fail.

Step 2 On Cisco Unity DVD 1, browse to the root directory and double-click **Setup.exe**.

Step 3 Follow the on-screen prompts until the Install Cisco Unity page appears.

Step 4 Click **Run the Cisco Unity Setup Program**.

Step 5 Follow the on-screen prompts until the Enter Installation Locations page appears.

Step 6 Specify locations for the Cisco Unity application, trace logs, and Unity Messaging Repository (UMR) files. Use the locations you made note of in the [“Determining the Locations for Files on the Cisco Unity Server”](#) section on page 2-4.


Caution

Choose the same drive and directory locations on the primary and secondary servers, or failover will not function properly.

Step 7 Click **Next**.

Step 8 In the Select Features dialog box:

- a. Check the **Install Cisco Unity** check box.
- b. If the Cisco Unity license includes text to speech, check the **Enable TTS** check box.
If not, uncheck the **Enable TTS** check box.
- c. If the Cisco Unity server or an attached expansion chassis contains Intel Dialogic voice cards, check the **Install Voice Card Software** check box.
If not, uncheck the **Install Voice Card Software** check box.



Note If Windows Server 2003 is installed on the Cisco Unity server, the Install Voice Card Software check box is not available. Circuit-switched phone system integrations that use voice cards are not supported with a Cisco Unity server on which Windows Server 2003 is installed.

Step 9 Click **Next**.

Step 10 Choose the prompt set to install. Consider the following:

- Cisco Unity should use the same audio format for prompts that the phone system uses for the media stream. Using a consistent audio format minimizes the need for transcoding from one audio format to another and minimizes the performance impact on the Cisco Unity server.
- Callers hear consistent sound quality when the prompts are in the same audio format that is used for recording messages.
- The G.711 Mu-Law audio format offers superior audio quality.
- The G.729a audio format uses less network bandwidth.

Note that choosing a system prompt set does not change the default message recording and storage codec. If necessary, you can change the message recording and storage codec after Cisco Unity is installed.

Step 11 Click **Next**.

Step 12 In the Cisco Unity Languages dialog box, choose the language(s) to install, and click **Next**.

If you installed Windows by using the manufacturer's guided system-setup utility and a retail Windows disc, one of the languages you choose here must match the locale you specified when you installed Windows.



Caution If the locale you specified when you installed Windows does not match any of the installed Cisco Unity system-prompt languages, Cisco Unity will log errors in the event log and may stop taking calls. The system-prompt language you choose here must exactly match the locale you selected when you installed Windows. For example, if you chose English (United Kingdom) for locale, you must also choose English (United Kingdom) as one of the Cisco Unity system-prompt languages. English (Australia) will not work.

If you installed Windows by using the Platform Configuration discs that are shipped with the Cisco Unity server, the locale is automatically set to English (United States). The Cisco Unity Setup program always installs English (United States) system prompts, so you do not need to choose it as one of the languages to install.


Note that if the system will be using text to speech (TTS) and will be using English (Australia) or English (New Zealand) for the system prompts, also install English (United States) or English (United Kingdom) for the TTS language.

Step 13 Set the system-default languages for the phone, graphical user interface (GUI), and TTS, and click **Next**.

For the phone (system prompts) language, choose the language that matches the locale that you specified when you installed Windows.

Step 14 Follow the on-screen prompts until you are prompted to restart the Cisco Unity server.

- Step 15** The remainder of the procedure depends on whether the server contains Intel Dialogic D/120JCT-Euro or D/240PCI-T1 voice cards:

<p>If the server does not contain Intel Dialogic D/120JCT-EURO or D/240PCI-T1 voice cards</p>	<p>Check the Yes, I Want to Restart My Computer Now check box, and click Finish. Cisco Unity software is now installed.</p>
<p>If the server contains Intel Dialogic D/120JCT-EURO or D/240PCI-T1 voice cards</p>	<p>a. Uncheck the Yes, I Want to Restart My Computer Now check box, and click Finish.</p> <p> Caution If the Cisco Unity server contains Intel Dialogic D/120JCT-EURO or D/240PCI-T1 voice cards, do not restart the server now or you will not be able to access the Cisco Unity Administrator after Cisco Unity is installed.</p> <p>b. Do the procedure under “Software Settings” for your voice card in Appendix A, “Voice Cards and PIMG Units.”</p> <p>c. Restart the Cisco Unity server.</p>

Installing License Files

From the Cisco Unity Installation and Configuration Assistant, you run the Cisco Unity Install License File wizard second to install the Cisco Unity license files.

This section contains two procedures. Do the first procedure on the primary Cisco Unity server and the second procedure on the secondary Cisco Unity server.

To Install the License Files on the Primary Server

- Step 1** Log on to Windows by using the Cisco Unity installation account.
- Step 2** On the Install the Cisco Unity License Files page, click **Run the Cisco Unity Install License File Wizard**.
- Step 3** On the Welcome page, click **Next**.
- Step 4** Click **Add**.
- Step 5** Insert the Cisco Unity license file disk, if applicable.
- (When Cisco Unity was registered on Cisco.com, Cisco replied with an e-mail containing attached file(s) with license(s) for Cisco Unity features. The instructions in the e-mail directed that the attached files be saved. For more information, see the [“Obtaining Cisco Unity License Files” section on page 5-4.](#))
- Step 6** Browse to drive A or to the location where the license file(s) have been stored.
- Step 7** Double-click the license file to add it to the License Files list.
- If prompted, click **Yes** to copy the license file to the local system.
- Step 8** If you are adding more than one license file, click **Add**, and repeat [Step 6](#) and [Step 7](#) for each license file.

- Step 9** Click **Next**.
- Step 10** In the Licenses dialog box, confirm that the license information is correct.
- Step 11** Click **Next**.
- Step 12** Click **Finish**.

When the wizard is complete, the Configure the Cisco Unity Services page appears in the main window.

To Install the Default License File on the Secondary Server

- Step 1** Log on to Windows by using the Cisco Unity installation account.
- Step 2** On the Install the Cisco Unity License Files page, click **Run the Cisco Unity Install License File Wizard**.
- Step 3** On the Welcome page, click **Next**.
- Step 4** Click **Add**.
- Step 5** Install the default license file:
- Browse to the **CommServer\Licenses** directory.
 - Double-click **CiscoUnity50.lic**.

Click **Next**.

- Step 6** In the Licenses list, confirm that the license information is correct.
- Step 7** Click **Next**.
- Step 8** Click **Finish**.

When the wizard is complete, the Configure the Cisco Unity Services page appears in the main window.

Configuring Services

From the Cisco Unity Installation and Configuration Assistant, you run the Cisco Unity Services Configuration wizard third to associate the directory, message store, and local services with accounts you specify.

To Configure Services

- Step 1** On the Configure the Cisco Unity Services page, click **Run the Cisco Unity Services Configuration Wizard**. (Note that you should be logged on to Windows with the Cisco Unity installation account.)
- Step 2** On the Welcome page, click **Next**.
- Step 3** Choose the version of Exchange that is installed on the partner Exchange server that you chose in the [“Determining the Partner Exchange Server”](#) section on page 6-1.

Step 4 Click **Next**.

Step 5 Follow the on-screen prompts to complete the configuration.

When the wizard is complete, the Configure the Cisco Unity Message Store page appears in the main window.

Configuring Cisco Unity for the Message Store

From the Cisco Unity Installation and Configuration Assistant, you run the Cisco Unity Message Store Configuration wizard fourth to configure Cisco Unity for the message store.

Note that when Exchange is installed on the secondary Cisco Unity server, the Cisco Unity server is the partner Exchange server.

To Configure Cisco Unity for the Message Store

Step 1 On the Configure the Cisco Unity Message Store page, click **Run the Cisco Unity Message Store Configuration Wizard**. (Note that you should be logged on to Windows with the Cisco Unity installation account.)

Step 2 Confirm that Exchange is running on the partner server that you chose in the “[Determining the Partner Exchange Server](#)” section on page 6-1. If Exchange is not running, configuring the message store on the Cisco Unity server will fail.

Step 3 In the Welcome dialog box, click **Next**.

Step 4 Enter the password for the installation account, and click **Next**.

Step 5 If you did not create a Cisco Unity administration account in the “[Creating the Accounts Required for the Cisco Unity Installation](#)” section on page 7-3, skip to **Step 6**. When installation is complete, you will log on to the Cisco Unity Administrator by using the installation account.

If you created a Cisco Unity administration account in the “[Creating the Accounts Required for the Cisco Unity Installation](#)” section on page 7-3, specify the account:

- a. Click **Change**.
- b. In the Select User dialog box, double-click the name of the Cisco Unity administration account.

Step 6 Click **Next**.

Step 7 In the Select Partner Message Store dialog box, click **Microsoft Exchange 2003**, and click **Next**.

Step 8 Review the onscreen text and check or uncheck the **Disable Active Directory Accounts that Are Created by Cisco Unity** check box, as applicable, and click **Next**.

Step 9 In the Select Mailbox Location dialog box, choose the partner Exchange server and the mailbox store in which to create new mailboxes, and click **Next**.

Step 10 In the Select Active Directory Containers for New Objects dialog box, choose the domain in which you want Cisco Unity to create users and distribution lists.

If you created custom organizational units for users or distribution lists, click the corresponding **Change** button to specify them here.

Step 11 Click **Next**.

Step 12 Click **OK** to stop Cisco Unity services.

- Step 13** In the Select How Subscribers Will Be Created dialog box, set how administrators will create Cisco Unity subscriber accounts in the Cisco Unity Administrator:

Create New Accounts or Import Existing Accounts	Click if administrators will create subscriber accounts either by adding a new user to Exchange or by importing existing user data from Exchange. You cannot use the Cisco Unity Administrator to create subscribers whose mailboxes are homed in Exchange 2007.
Import Existing Accounts Only	Click if administrators will create subscriber accounts only by importing existing user data from Exchange.

- Step 14** Click **Next**.
- Step 15** By default, the account that you created for Cisco Unity directory services appears. If you want to choose a different account, click **Change**.
- Step 16** Specify a password for the account, and click **Next**.
- Step 17** When message store configuration is complete, click **Finish**.
- When the wizard is complete, the Set New Default Passwords page appears in the main window.

Setting New Default Passwords

From the Cisco Unity Installation and Configuration Assistant, you run the Password Hardening wizard fifth to set new default passwords for the Default Administrator and the Default Subscriber templates.

When all of the following conditions are true, Cisco recommends that you specify an extremely long and complex password for the Active Directory password in the Default Subscriber template:

- Subscribers will access messages only by using the phone.
- Subscribers will not have access to the Cisco Personal Communications Assistant.
- You will be creating Cisco Unity subscribers by using the Cisco Unity Administrator.
- You did not choose to disable Active Directory accounts created by Cisco Unity when you ran the Cisco Unity Message Store Configuration wizard.

When a subscriber is created by using the Cisco Unity Administrator, an Active Directory account is automatically created for that subscriber, too. The password on the Active Directory account is the password in the Default Subscriber template.



Caution

If the Active Directory account for a subscriber is not disabled, anyone who knows the password for the account, knows the alias for a subscriber, and knows on which Exchange server the voice messages for that subscriber are stored can access those messages.

To Set New Default Passwords

- Step 1** On the Set New Default Passwords page, click **Run the Password Hardening Wizard**.
- Step 2** Follow the on-screen prompts.
- When the Password Hardening wizard finishes, the Integrate the Phone System with Cisco Unity page appears in the main window.
-

Integrating the Phone System with Cisco Unity

From the Cisco Unity Installation and Configuration Assistant, you run the Cisco Unity Telephony Integration Manager (UTIM) sixth to connect Cisco Unity with the phone system.

This section contains two procedures. Do the first procedure on the primary Cisco Unity server and the second procedure on the secondary Cisco Unity server.

To Integrate the Phone System with Cisco Unity on the Primary Server

- Step 1** On the Integrate the Phone System with Cisco Unity page, click **Run the Cisco Unity Telephony Integration Manager**. (Note that you should be logged on to Windows with the Cisco Unity installation account.)
- Step 2** In the right pane of the UTIM, click **Create Integration**.
- Step 3** Refer to the applicable Cisco Unity integration guide for your phone system to complete the integration. (Cisco Unity integration guides are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.)
- When the integration is complete, the Set Up the Cisco Personal Communications Assistant to Use SSL page appears in the main window.
-

To Integrate the Phone System with Cisco Unity on the Secondary Server

- Step 1** In the main window of the assistant, click **Run the Cisco Unity Telephony Integration Manager**. (Note that you should be logged on to Windows with the Cisco Unity installation account.)
- Step 2** In the right pane of the UTIM, click **Create Integration**.
- Step 3** Fill in the fields with the same values you used for the primary Cisco Unity server, with the exception of the Cisco Unified CM Device Name Prefix field value for a Cisco Unified CM integration. The value used on the primary Cisco Unity server is different from the value used on the secondary Cisco Unity server. See the applicable Cisco Unified CM integration guide.

- Step 4** When the message appears saying that you have entered more ports than you are allowed, click **OK**. (You will deal with port settings later in the installation.)
- Step 5** Continue to fill in the fields with the same values you used for the primary Cisco Unity server. When the integration is complete, the Set Up the Cisco Personal Communications Assistant to Use SSL page appears in the main window.
-

Setting Up the Cisco Personal Communications Assistant to Use SSL

From the Cisco Unity Installation and Configuration Assistant, you can set up the Cisco PCA to use SSL. Using the SSL protocol ensures that all subscriber credentials—as well as the information that a subscriber enters on any page in the Cisco PCA—are encrypted as the data is sent across the network.

After the Cisco Unity Installation and Configuration Assistant is finished and the Cisco PCA is set up to use SSL, you manually set up the Cisco Unity Administrator and Status Monitor to use SSL. The *Cisco Unity Installation Guide* alerts you when to do the procedure.

If you do not want to set up the Cisco PCA to use SSL, see the [“Skipping Cisco PCA Setup for SSL” section on page 8-11](#).

To set up the Cisco PCA to use SSL, do the procedures in the applicable section, depending on whether you are using a certificate authority:

- [Setting Up the Cisco PCA to Use SSL by Creating a Local Certificate Without a Certificate Authority, page 8-12](#)
- [Setting Up the Cisco PCA to Use SSL by Using a Certificate Authority, page 8-13](#)

If the Cisco Unity server is running Windows Server 2003, you can set up the Cisco Personal Communications Assistant to use SSL now. However, the option to do so by creating a local certificate without a certificate authority has not been automated for Windows Server 2003. If you want to set up the Cisco PCA to use SSL by using this method, you must do so manually. Refer to the online help available on this page.

Skipping Cisco PCA Setup for SSL

Do the procedure in this section if you do not want to set up the Cisco PCA to use SSL. (Note that without SSL when subscribers log on to the Cisco PCA, their credentials will be sent across the network to Cisco Unity in clear text. In addition, the information that subscribers enter on the pages of the Cisco PCA will not be encrypted.)

To Skip Cisco PCA Setup for SSL

- Step 1** On the Set Up the Cisco Personal Communications Assistant to Use SSL page, Click **Do Not Set Up Cisco Personal Communications Assistant to Use SSL**.
- Step 2** Click **Continue**.
- Step 3** Click **Close** to exit the Cisco Unity Installation and Configuration Assistant.
-

Setting Up the Cisco PCA to Use SSL by Creating a Local Certificate Without a Certificate Authority

To Set Up the Cisco PCA to Use SSL by Creating a Local Certificate Without a Certificate Authority

-
- Step 1** On the Set Up the Cisco Personal Communications Assistant to Use SSL page, click **Create a Local Certificate Without a Certificate Authority**.
- Step 2** Click **Internet Services Manager**.
- Step 3** Expand the name of the Cisco Unity server.
- Step 4** If the Cisco Unity server is not running Windows Server 2003, skip to [Step 5](#).
If the Cisco Unity server is running Windows Server 2003, expand **Web Sites**.
- Step 5** Right-click **Default Web Site**, and click **Properties**.
- Step 6** In the Default Web Site Properties dialog box, click the **Directory Security** tab.
- Step 7** Under Secure Communications, click **Server Certificate**.
- Step 8** On the Web Server Certificate wizard Welcome page, click **Next**.
- Step 9** Click **Create a New Certificate**, and click **Next**.
- Step 10** Click **Prepare the Request Now, But Send It Later**, and click **Next**.
- Step 11** Enter a name and a bit length for the certificate.

We strongly recommend that you choose a bit length of 512. Greater bit lengths may decrease performance.

- Step 12** Click **Next**.
- Step 13** Enter the organization information, and click **Next**.
- Step 14** For the common name of the site, enter either the system name of the Cisco Unity server or the fully qualified domain name.



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

- Step 15** Click **Next**.
- Step 16** Enter the geographical information, and click **Next**.
- Step 17** Specify the certificate request file name and location, and write down the file name and location because you will need the information later in this procedure.
- Step 18** Click **Next**.
- Step 19** Verify the request file information, and click **Next**.
- Step 20** Click **Finish** to exit the Web Server Certificate wizard.
- Step 21** Click **OK** to Close the Default Web Site Properties dialog box.
- Step 22** Close the Internet Services Manager window.
- Step 23** In the Cisco Unity Installation and Configuration Assistant, in the Enter Certificate Request File box, enter the full path and file name of the certificate request file that you specified in [Step 17](#).
- Step 24** Click **Create Certificate**.
- Step 25** Click **Internet Services Manager**.

- Step 26** Expand the name of the Cisco Unity server.
- Step 27** If the Cisco Unity server is not running Windows Server 2003, skip to [Step 28](#).
If the Cisco Unity server is running Windows Server 2003, expand **Web Sites**.
- Step 28** Right-click **Default Web Site**, and click **Properties**.
- Step 29** In the Default Web Site Properties dialog box, click the **Directory Security** tab.
- Step 30** Under Secure Communications, click **Server Certificate**.
- Step 31** On the Web Server Certificate wizard Welcome page, click **Next**.
- Step 32** Click **Process the Pending Request and Install the Certificate**.
- Step 33** Click **OK**.
- Step 34** In the Process a Pending Request dialog box, click **OK** to accept the default path and file name of the pending certificate request.
- Step 35** In the Certificate Summary dialog box, click **Next**.
- Step 36** Click **Finish** to exit the Web Server Certificate wizard.
- Step 37** Click **OK** to Close the Default Web Site Properties dialog box.
- Step 38** Close the Internet Services Manager window.
- Step 39** In the Cisco Unity Installation and Configuration Assistant, click **Enable Cisco PCA to Use SSL**.
- Step 40** Click **Internet Services Manager**.
- Step 41** Right-click the name of the Cisco Unity server, and click **Restart IIS**.
- Step 42** In the Stop/Start/Restart dialog box, click **Restart Internet Services on <Servername>**.
- Step 43** Click **OK**.
- Step 44** Close the Internet Services Manager window.
- Step 45** In the Cisco Unity Installation and Configuration Assistant, click **Continue**.
- Step 46** Click **Close** to exit the Cisco Unity Installation and Configuration Assistant.
-

Setting Up the Cisco PCA to Use SSL by Using a Certificate Authority

This section contains four procedures.

If you are using Microsoft Certificate Services to issue your own certificate, do all four procedures in the order listed.

If you are using a certificate purchased from a certificate authority (for example, VeriSign), do only the fourth procedure, "[To Install the Certificate](#)."

To Create a Certificate Request by Using Microsoft Certificate Services

- Step 1** On the Set Up the Cisco Personal Communications Assistant to Use SSL page, click **Use a Certificate Authority**.
- Step 2** Click **Internet Services Manager**.
- Step 3** Expand the name of the Cisco Unity server.

- Step 4** If the Cisco Unity server is not running Windows Server 2003, skip to [Step 5](#).
If the Cisco Unity server is running Windows Server 2003, expand **Web Sites**.
- Step 5** Right-click **Default Web Site**, and click **Properties**.
- Step 6** In the Default Web Site Properties dialog box, click the **Directory Security** tab.
- Step 7** Under Secure Communications, click **Server Certificate**.
- Step 8** On the Web Server Certificate wizard Welcome page, click **Next**.
- Step 9** Click **Create a New Certificate**, and click **Next**.
- Step 10** Click **Prepare the Request Now, But Send It Later**, and click **Next**.
- Step 11** Enter a name and a bit length for the certificate.
We strongly recommend that you choose a bit length of 512. Greater bit lengths may decrease performance.
- Step 12** Click **Next**.
- Step 13** Enter the organization information, and click **Next**.
- Step 14** For the common name of the site, enter either the system name of the Cisco Unity server or the fully qualified domain name.



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

- Step 15** Click **Next**.
- Step 16** Enter the geographical information, and click **Next**.
- Step 17** Specify the certificate request file name and location, and write down the file name and location because you will need the information in the next procedure.
Save the file to a disk or to a directory that the certificate authority (CA) server can access.
- Step 18** Click **Next**.
- Step 19** Verify the request file information, and click **Next**.
- Step 20** Click **Finish** to exit the Web Server Certificate wizard.
- Step 21** Click **OK** to Close the Default Web Site Properties dialog box.
- Step 22** Close the Internet Services Manager window.
- Step 23** Click **Close** to exit the Cisco Unity Installation and Configuration Assistant.

To Submit the Certificate Request by Using Microsoft Certificate Services

- Step 1** On the server that is acting as the CA, on the Windows Start menu, click **Run**.
- Step 2** Run **Certreq**.
- Step 3** Browse to the directory where you saved the certificate request file, and double-click the file.
- Step 4** Click the CA to use, and click **OK**.
-

Once the CA submits the certificate request, it assigns a pending status by default for added security. This requires a person to verify the authenticity of the request and to manually issue the certificate.

To Issue the Certificate by Using Microsoft Certificate Services

- Step 1** On the server that is acting as the CA, on the Windows Start menu, click **Programs > Administrative Tools > Certification Authority**.
 - Step 2** In the left pane of the Certification Authority window, expand **Certification Authority**.
 - Step 3** Expand <Certification Authority name>.
 - Step 4** Click **Pending Requests**.
 - Step 5** In the right pane, right-click the request, and click **All Tasks > Issue**.
 - Step 6** In the left pane, click **Issued Certificates**.
 - Step 7** In the right pane, double-click the certificate to open it.
 - Step 8** Click the **Details** tab.
 - Step 9** In the Show list, choose <All>, and click **Copy to File**.
 - Step 10** On the Certificate Export wizard Welcome page, click **Next**.
 - Step 11** Accept the default export file format **DER encoded binary X.509 (.CER)**, and click **Next**.
 - Step 12** Specify a file name and a location that the Cisco Unity server can access, and click **Next**.
 - Step 13** Verify the settings, and click **Finish**.
 - Step 14** Click **OK** to close the Certificate Details dialog box.
 - Step 15** Close the Certification Authority window.
-

To Install the Certificate

- Step 1** On the Cisco Unity server, double-click the **CUICA** icon on the desktop.
- Step 2** In the Cisco Unity Installation and Configuration Assistant, click **Use a Certificate Authority**.
- Step 3** On the Set Up the Cisco Personal Communications Assistant to Use SSL page, at Step 3, click **Internet Services Manager**.
- Step 4** Expand the name of the Cisco Unity server.
- Step 5** If the Cisco Unity server is not running Windows Server 2003, skip to [Step 6](#).
If the Cisco Unity server is running Windows Server 2003, expand **Web Sites**.
- Step 6** Right-click **Default Web Site**, and click **Properties**.
- Step 7** In the Default Web Site Properties dialog box, click the **Directory Security** tab.
- Step 8** Under Secure Communications, click **Server Certificate**.
- Step 9** On the Web Server Certificate wizard Welcome page, click **Next**.
- Step 10** Click **Process the Pending Request and Install the Certificate**, and click **Next**.
- Step 11** Browse to the directory of the certificate (.cer) file, and double-click the file.
- Step 12** Verify the certificate information, and click **Next**.
- Step 13** Click **Finish** to exit the Web Server Certificate wizard.

- Step 14** Click **OK** to close the Default Web Site Properties dialog box.
- Step 15** Close the Internet Services Manager window.
- Step 16** In the Cisco Unity Installation and Configuration Assistant, click **Enable Cisco PCA to Use SSL**.
- Step 17** Restart IIS:
- Click **Internet Services Manager**.
 - Right-click the name of the Cisco Unity server, and click **Restart IIS**.
 - In the Stop/Start/Restart dialog box, click **Restart Internet Services on <Servername>**.
 - Click **OK**.
 - Close the Internet Services Manager window.
- Step 18** Click **Close** to exit the Cisco Unity Installation and Configuration Assistant.
-

Testing the Phone System Integration

Test the integration with the phone system. Refer to the Cisco Unity integration guide for your phone system.

Test only the integration with the primary Cisco Unity server now. You test the integration with the secondary Cisco Unity server after you set up failover. The *Failover Configuration and Administration Guide for Cisco Unity* instructs you when and how to test the secondary server.

Note that you use the Cisco Unity Administrator for part of the integration test. Use the user name and password for the account that you selected to administer Cisco Unity.

Excluding Selected Directories from Virus Scanning

Revised May 1, 2008



Note

If virus-scanning software is not installed on the Cisco Unity server, skip this section.

You exclude selected directories from scanning to improve Cisco Unity performance and reliability.

To Exclude Selected Directories from Virus Scanning

- Step 1** Refer to the virus-scanning software Help for instructions on excluding directories from scanning.
- Step 2** Exclude the following directories from virus scanning:
- The directory in which Cisco Unity is installed (Commserver by default), and all subdirectories.
 - The directory that contains the files UnityDB.mdf and UnityDb_log.ldf.
 - The directory specified in the Temp system variable for the message store services account. (To find this directory, log on as the message store services account. Open a command-prompt window, and run the **set temp** command.)
 - When Exchange Server 2003 is installed on the Cisco Unity server:

- Drive M, the virtual share for Exchange, if you have added the registry key that is required to make drive M visible.
 - The directories that contain Exchange storage group data.
 - When the Cisco Unity Voice Connector is installed on the Cisco Unity server, the directory where the Cisco Unity Voice Gateway is installed (Voicegateway by default), and all subdirectories.
-

Deleting Apache Tomcat Sample Directories

Added May 1, 2008

Apache Tomcat, which is automatically installed on the Cisco Unity server and is required for Cisco Unity to function properly, contains security vulnerabilities in sample applications. To eliminate the security vulnerabilities, do the following procedure to delete the sample directories. For more information, see the CVE-IDs “CVE-2007-1355” and “CVE-2007-2449” on the CVE (Common Vulnerabilities and Exposures) website at <http://cve.mitre.org>.

To Delete Apache Tomcat Sample Applications

- Step 1** In the Services MMC, stop the Tomcat service.
- Step 2** Delete the following directories and their contents under the directory where Cisco Unity is installed (Commserver by default):
- cscoserv\Tomcat\webapps\examples
 - cscoserv\Tomcat\webapps\tomcat-docs
- Step 3** In the Services MMC, restart the Tomcat service.
-

Setting Up the Cisco Unity Administrator and Status Monitor to Use SSL



Note

If you are not setting up Cisco Unity to use SSL, skip this section.

Using the SSL protocol ensures that all subscriber credentials—as well as the information that a subscriber enters on any page in the Cisco Unity Administrator—are encrypted as the data is sent across the network.

To Set Up the Cisco Unity Administrator and Status Monitor to Use SSL

- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Internet Services Manager**.
- Step 2** Expand the name of the Cisco Unity server.

- Step 3** If the Cisco Unity server is not running Windows Server 2003, skip to [Step 4](#).
If the Cisco Unity server is running Windows Server 2003, expand **Web Sites**.
- Step 4** Expand **Default Web Site**.
- Step 5** Under Default Web Site, right-click **Web**, and click **Properties**.
- Step 6** In the Properties dialog box, set the Web directory to use SSL:
- Click the **Directory Security** tab.
 - Under Secure Communications, click **Edit**.
 - Check the **Require Secure Channel (SSL)** check box.
 - Click **OK** to close the Secure Communications dialog box.
 - Click **OK** to close the Properties dialog box.
- Step 7** Under Default Web Site, right-click **SAWeb**, and click **Properties**.
- Step 8** Repeat [Step 6](#) to set the SAWeb directory to use SSL.
- Step 9** Under Default Web Site, right-click **Status**, and click **Properties**.
- Step 10** Repeat [Step 6](#) to set the Status directory to use SSL.
- Step 11** Under Default Web Site, double-click **AvXml**.
- Step 12** In the right pane, right-click **AvXml.dll**, and click **Properties**.
- Step 13** In the Properties dialog box, click the **File Security** tab.
- Step 14** Under Secure Communications, click **Edit**.
- Step 15** Check the **Require Secure Channel (SSL)** check box.
- Step 16** Click **OK** to close the Secure Communications dialog box.
- Step 17** Click **OK** to close the AvXml.dll Properties dialog box.
- Step 18** Close the Internet Services Manager window.

After you have set up the Cisco Unity Administrator and Status Monitor to use SSL, you must make the following changes so the web applications can be started by using the Cisco Unity tray icon and desktop icons:

- Update the Windows registry to change the default HTTP URL to an HTTPS (secure) URL for the tray icon.
- Change the desktop icons to use HTTPS URLs.

Do the following two procedures to change the URLs to secure URLs.

To Change the Default URL for the Cisco Unity Tray Icon to an HTTPS URL

- Step 1** On the Cisco Unity server, 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. (Refer to the “Restoring” topics in Registry Editor Help.) Note that registry changes on one server in a Cisco Unity failover pair must be made manually on the other server, because registry changes are not replicated. If you have any questions about changing registry key settings, contact Cisco TAC.

- Step 2** 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 3** Expand the key
HKEY_LOCAL_MACHINE\SOFTWARE\Active Voice\SystemParameters\1.0.
- Step 4** In the left pane, right-click **1.0**, and click **New > DWORD Value**.
- Step 5** Name the value **EnforceSSL**.
- Step 6** In the right pane, double-click **EnforceSSL**.
- Step 7** Change Value Data to **1**.
- Step 8** Click **OK** to save the change.
- Step 9** Close Registry Editor.
- Step 10** Restart the server.

To Change the Desktop Icons to Use HTTPS URLs

- Step 1** On the Cisco Unity server, right-click the **System Administration** desktop icon, and click **Properties**.
- Step 2** Click the **Web Document** tab.
- Step 3** In the URL field, change the “http” portion of the URL to **https**.
- Step 4** Click **OK**.
- Step 5** Right-click the **Status Monitor** desktop icon, and click **Properties**.
- Step 6** Click the **Web Document** tab.
- Step 7** In the URL field, change the “http” portion of the URL to **https**.
- Step 8** Click **OK**.

Configuring Internet Explorer to Display the Cisco Unity Administrator Correctly (Windows Server 2003 Only)

**Note**

If Windows Server 2003 is not installed on the Cisco Unity server or if you installed Windows Server 2003 using the Cisco Unity Platform Configuration discs, skip this section.

If you created a Cisco Unity administration account as recommended in the “[About the Accounts Required for the Cisco Unity Installation](#)” section on page 7-2, and you log on to Windows by using that account, the changes that the Windows Server 2003 service pack make to the default Internet Explorer security settings cause the Cisco Unity Administrator to display a blank page. Do the following procedure to configure Internet Explorer to display the Cisco Unity Administrator when you log on to Windows by using the administration account.

To Configure Internet Explorer to Display the Cisco Unity Administrator Correctly

-
- Step 1** Log on to the Cisco Unity server by using the Cisco Unity administration account.
- Step 2** Right click the **Cisco Unity** icon in the system tray, and click **Launch System Admin**.
- Step 3** If you are prompted to provide a user name and password, click **Cancel**.
- Step 4** On the Internet Explorer Tools menu, click **Internet Options**.
- Step 5** Click the **Security** tab.
- Step 6** Under Select a Web Content Zone to Specify Its Security Settings, click the **Trusted Sites** icon.
- Step 7** Click **Sites**.
- Step 8** In the Trusted Sites dialog box, in the Add This Website to the Zone field, enter the applicable value depending on whether the Cisco Unity Administrator is set up to use SSL:
- | | |
|-----------------------------------------------------------|---------------------------------------------------|
| Cisco Unity Administrator is set up to use SSL | Enter https:\\<CiscoUnityServerName> |
| Cisco Unity Administrator is not set up to use SSL | Enter http:\\<CiscoUnityServerName> |
- Step 9** If the Cisco Unity Administrator is set up to use SSL, check the **Require Server Verification (https:) for All Sites in This Zone** check box.
- If the Cisco Unity Administrator is not set up to use SSL, uncheck the **Require Server Verification (https:) for All Sites in This Zone** check box.
- Step 10** Click **Add**.
- Step 11** Click **Close** to close the Trusted Sites dialog box.
- Step 12** On the Security tab, click **Custom Level**.
- Step 13** In the Security Settings dialog box, change the value of the Reset To list to **Low**.
- Step 14** Click **Reset**, and click **Yes** to confirm that you want to change the security settings for this zone.
- Step 15** Click **OK** to close the Security Settings dialog box.
- If the Security Settings dialog box does not close:
- a. Close the dialog box by clicking the **X** in the upper-right corner.
 - b. In the “not responding” message box, click **End Now**. (The “not responding” message box may take a few seconds to appear.)
- Step 16** Restart the Cisco Unity Administrator.
-

Securing the Example Administrator Account Against Toll Fraud

It is possible for a malicious user to dial into Cisco Unity, log on as the Example Administrator by using the default extension and password, and configure Cisco Unity to forward calls to phone numbers for which there are charges or to reconfigure greetings so an operator believes the messaging system is personally accepting collect-call charges. To help secure Cisco Unity against toll fraud, we strongly recommend that you change the phone password for the Example Administrator account after Cisco Unity is installed.

To Change the Password on the Example Administrator Account

Step 1 In the Cisco Unity Administrator, go to any **Subscribers > Subscribers** page.

Step 2 Click the **Find** icon.

Step 3 On the Find and Select Subscriber page, click **Find**.

Step 4 Click **Example Administrator**.

Step 5 In the left pane, click **Phone Password**.

Step 6 In the right pane, check the **User Cannot Change Password** check box.

Step 7 Check the **Password Never Expires** check box.

Step 8 Under **Reset Phone Password**, enter and confirm a new password by using digits 0 through 9.

We recommend that you enter a long and nontrivial password; 20 digits or more is desirable. (The minimum length of the password is set on the Subscribers > Account Policy > Phone Password Restrictions page.) In a nontrivial password:

- The digits are not all the same (for example, 9999).
- The digits are not consecutive (for example, 1234).
- The password is not the same as the extension assigned to the example account.
- The password does not spell the name of the example account, the name of the company, the name of the IT manager, or any other obvious words.

Step 9 Click the **Save** icon.

Step 10 Close the Cisco Unity Administrator.

Moving the Data Store Databases and Transaction Logs

The Cisco Unity data store includes several databases and their corresponding transaction logs. Because the Cisco Unity and Reports databases and their transaction logs are the fastest-growing data store files, you place them on the system in a location that makes optimum use of system storage capacity.

As you do the procedure in this section, if applicable, refer to the drive locations you made note of in the [“Determining the Locations for Files on the Cisco Unity Server”](#) section on page 2-4.

For more information on moving SQL Server databases and transaction logs, refer to Microsoft documentation.

To Move the SQL Server Databases and Transaction Logs

- Step 1** Stop Cisco Unity. (Right-click the **Cisco Unity** icon in the system tray, then click **Stop Cisco Unity**; if the Cisco Unity icon is not available, browse to the **CommServer** directory and double-click **AvCsTrayStatus.exe**.)
- Step 2** In Task Manager, end the Cisco Unity tray icon process:
- Right-click in an empty space on the taskbar and click **Task Manager**.
 - Click the **Processes** tab.
 - Click the **Image Name** column twice to sort by process name.
 - Click **AvCsTrayStatus**.
 - Click **End Process**.
 - Click **Yes** to confirm.
 - Close **Task Manager**.
- Step 3** Stop the AvCsGateway service:
- On the Windows Start menu, click **Programs > Administrative Tools > Services**.
 - In the right pane, right-click **AvCsGateway**, and click **Stop**.
 - Close the Services MMC.
- Step 4** Detach the ReportDB and UnityDb databases:
- On the Windows Start menu, click **Programs > Microsoft SQL Server > Enterprise Manager**.
 - In the left pane, expand **Microsoft SQL Servers > SQL Server Group > (local) (Windows NT) > Databases**.
 - Right-click **ReportDb**, and click **All Tasks > Detach Database**.
 - If the OK button is unavailable, click **Clear**, and click **OK** to confirm that you want to clear connections.
 - Click **OK** to detach the ReportDB database.
 - Click **OK** to confirm.
 - Repeat Step **c.** through Step **f.** to detach the UnityDb database.
- Step 5** Close SQL Server Enterprise Manager.
- Step 6** In Windows Explorer, create the new directories for Cisco Unity data and for transaction logs on the drive locations you made note of in the [“Determining the Locations for Files on the Cisco Unity Server”](#) section on page 2-4. Use directory names that are easy to remember, for example:

UnityDb.mdf and ReportDb.mdf	<Database destination drive>\<Path>\UnityData
ReportDb_log.ldf and UnityDb_log.ldf	<Log file destination drive>\<Path>\UnityLogs

- Step 7** In Windows Explorer, move UnityDb.mdf and ReportDb.mdf from Program Files\Microsoft SQL Server\MSSQL\Data to the new directory for Cisco Unity databases.
- Step 8** In Windows Explorer, move ReportDb_log.ldf and UnityDb_log.ldf from Program Files\Microsoft SQL Server\MSSQL\Data to the new directory for Cisco Unity transaction logs.

Step 9 Using OSQL, reattach the databases:



Caution If you put the databases and the transaction log in separate locations, as recommended for most systems, you must use OSQL to reattach the databases because SQL Server Enterprise Manager does not support attaching a database when the corresponding log file is not in the same directory.

- a. On the Windows Start menu, click **Run**.
- b. Run **cmd**.
- c. Start OSQL by entering **OSQL -E** on the command line.



Caution Use **-E**, not **-e**.

- d. Enter **use master** and press **Enter**.
- e. Enter **go** and press **Enter**.
- f. Enter **EXEC sp_attach_db 'UnityDb', '<Database destination drive>\<New database directory path>\UnityDb.mdf', '<Log file destination drive>\<New log file directory path>\UnityDb_log.ldf'** and press **Enter**.
- g. Enter **go** and press **Enter**.

If you specified an invalid path or file name, an error message appears in the command window. Re-run Step **f**. and Step **g**. with the correct information.

- h. Enter **EXEC sp_attach_db 'ReportDb', '<Database destination drive>\<New database directory path>\ReportDb.mdf', '<Log file destination drive>\<New log file directory path>\ReportDb_log.ldf'** and press **Enter**.
- i. Enter **go** and press **Enter**.

If you specified an invalid path or file name, an error message appears in the command window. Re-run Step **h**. and Step **i**. with the correct information.

Step 10 Enter **exit** and press **Enter** to close OSQL.

Step 11 On the Windows Start menu, click **Programs > Startup > AvCsTrayStatus** to restart the Cisco Unity tray icon.

Step 12 When the tray icon appears in the Windows taskbar, use it to restart Cisco Unity.

Installing the Latest Microsoft Service Packs and Updates

You install the latest Microsoft service packs that has been qualified for use with Cisco Unity, if any, as well as the corresponding updates, to enhance the security of the Cisco Unity server. Do the following procedures.

To Install the Latest Microsoft Service Packs, If Any

- Follow the instructions that you printed or downloaded when you downloaded the service pack.
-

To Install the Latest Microsoft Updates Recommended for Use with Cisco Unity

- Step 1** Insert in the drive the disc that you burned with the latest version of the Cisco Unity Server Updates Wizard.
- Step 2** Run **ServerUpdatesWizard.exe**.
- Step 3** Follow the on-screen prompts to complete the installation of Microsoft updates and, optionally, Cisco Security Agent for Cisco Unity.



Note

If you are accessing the server by using Remote Desktop or a VNC client, and you are installing Cisco Security Agent for Cisco Unity, the Remote Desktop or VNC session will be disconnected when Cisco Security Agent for Cisco Unity restarts the network interface. If the session does not reconnect automatically, reconnect manually to finish the Server Updates wizard.

- Step 4** Restart the Cisco Unity server.
-

Re-enabling Virus-Scanning and Cisco Security Agent Services



Note

If virus-scanning software or Cisco Security Agent for Cisco Unity is not installed on the Cisco Unity server, skip this section.

You re-enable virus-scanning and Cisco Security Agent services now that all of the software installations that could have been affected if the services were running are complete.

To Re-enable and Start Virus-Scanning and Cisco Security Agent Services

- Step 1** Refer to the virus-scanning software documentation to determine the names of the virus-scanning services.

- Step 2** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
- Step 3** Re-enable and start each virus-scanning service and the Cisco Security Agent service:
- In the right pane, double-click the service.
 - On the General tab, in the Startup Type list, click **Automatic** to re-enable the service.
 - Click **Start** to start the service.
 - Click **OK** to close the Properties dialog box.
- Step 4** When the services have been re-enabled, close the Services MMC.
-

Securing Cisco Unity and the Cisco Unity Server

We strongly recommend that you secure Cisco Unity and the Cisco Unity server. Refer to the *Security Guide for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

