



# 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**

---

*Failover:* If you are installing the secondary Cisco Unity server now, skip Task 2.

---

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.
4. Install the latest Cisco Unity 4.0(4) service release, if any. See the [“Installing the Latest Cisco Unity 4.0\(4\) Service Release, If Any”](#) section on page 8-17.



**Note**

---

*Failover:* If you are installing the secondary Cisco Unity server now, skip Task 5.

---

5. Test the phone system integration. See the [“Testing the Phone System Integration”](#) section on page 8-17.
6. *If virus-scanning software is installed on the Cisco Unity server:* Exclude from scanning the directory in which Cisco Unity is installed. See the [“Excluding from Virus Scanning the Directory in Which Cisco Unity Is Installed”](#) 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 8-18.



**Note**

---

*Failover:* If you are installing the secondary Cisco Unity server now, skip Task 8.

---

8. Secure the Example Administrator account against toll fraud. See the [“Securing the Example Administrator Account Against Toll Fraud”](#) section on page 8-19.

9. Move SQL Server or MSDE database files and transaction logs. See the “[Moving the Data Store Databases and Transaction Log Files](#)” section on page 8-20.
10. *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 8-22.
11. *If the Cisco Unity server is connected to the corporate network:* Harden the Cisco Unity server. See the “[Hardening the Cisco Unity Server](#)” section on page 8-23.

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-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 the Microsoft Certificate Services application available with Windows to create a local certificate without a certificate authority. (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, the Microsoft Certificate Services application, 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 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 service.
- 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.
- Set new default passwords for the Default Administrator and the Default Subscriber templates
- Configure the Cisco Unity services.
- Configure Cisco Unity for the message store.
- 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.

If Windows Server 2003 is installed on the Cisco Unity server and you are installing Cisco Unity over the network, in Internet Explorer add the computer on which the Cisco Unity CD or DVD image files are stored to the local intranet zone.



### 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 or CD 1, or from the location to which you saved the downloaded Cisco Unity CD 1 image file, browse to the root directory and double-click **Setup.exe**.

**Step 3** If prompted, double-click the language of your choice to continue the installation.

**Step 4** On the Cisco Unity Installation and Configuration Assistant Welcome screen, click **Continue**.

If the Pre-Installation Requirements screen appears, saying that you need to run the Permissions wizard, close the Cisco Unity Installation and Configuration Assistant and see the [“Setting Rights and Permissions with the Cisco Unity Permissions Wizard”](#) section on page 7-7. Then log on to Windows by using the Cisco Unity installation account, and return to Step 2.

**Step 5** Click **Run the Cisco Unity Setup Program**.

**Step 6** If prompted, double-click the language of your choice to continue the installation.

**Step 7** On the Welcome screen, click **Next**.

**Step 8** Enter your name and the company name, and click **Next**.

**Step 9** 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 Drive Locations for Files on the Cisco Unity System”](#) section on page 2-5.

**Step 10** Click **Next**.

- Step 11** In the Select Features dialog box:
- Check the **Install Cisco Unity** check box.
  - If the Cisco Unity license includes text to speech, check the **Enable TTS** check box.  
If not, uncheck the **Enable TTS** check box.
  - 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.  
If Windows Server 2003 is installed on the Cisco Unity server, the **Install Voice Card Software** check box is not available.

**Step 12** Click **Next**.

**Step 13** Choose the prompt set to install. Use the G.729a system prompt set if voice messages will be recorded and stored in G.729a format. Otherwise, use G.711 (the default).

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 later in the installation process.

**Step 14** Click **Next**.

**Step 15** In the Cisco Unity Languages dialog box, choose the language(s) to install, and click **Next**.

If you installed Windows 2000 Server by using the manufacturer's guided system-setup utility and a retail Windows 2000 Server disc, one of the languages you choose here must match the locale you specified when you installed Windows 2000 Server.



**Caution**

If the locale you specified when you installed Windows 2000 Server does not match any of the installed Cisco Unity languages, Cisco Unity will log errors in the event log and may stop taking calls. The language you choose here must exactly match the locale you selected when you installed Windows 2000 Server. For example, if you chose English (United Kingdom) for locale, you must also choose English (United Kingdom) as one of the Cisco Unity languages. English (Australia) will not work.


If you installed Windows 2000 Server 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), 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) as the phone language, also install English (United States) or English (United Kingdom) for the TTS language.

**Step 16** Set the system-default languages for the phone, graphical user interface (GUI), and TTS, and click **Next**.

**Step 17** Follow the on-screen prompts until you are prompted to restart the Cisco Unity server.

- Step 18** The remainder of the procedure depends on whether the server contains Intel Dialogic D/120JCT-Euro or D/240PCI-T1 voice cards:

<p><b>If the server does not contain Intel Dialogic D/120JCT-EURO or D/240PCI-T1 voice cards</b></p>	<p>Check the <b>Yes, I Want to Restart My Computer Now</b> check box, and click <b>Finish</b>. Cisco Unity software is now upgraded.</p>
<p><b>If the server contains Intel Dialogic D/120JCT-EURO or D/240PCI-T1 voice cards</b></p>	<p>a. Uncheck the <b>Yes, I Want to Restart My Computer Now</b> check box, and click <b>Finish</b>.</p> <p> <b>Caution</b> 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 <a href="#">Appendix A, “Voice Cards.”</a></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.

If you are installing license files for a Cisco Unity system without failover or on the primary server for a Cisco Unity system with failover, do the first procedure, [“To Install the License Files.”](#)

If you are installing the secondary Cisco Unity server now, do the second procedure, [“To Install the Default License File on the Secondary Cisco Unity Server.”](#)

### To Install the License Files

- 
- 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 screen, 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 2-1.)

- 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**.
- 

Do the following procedure if you are installing the secondary server now for a Cisco Unity system with failover. Otherwise, do the first procedure, "[To Install the License Files](#)."

#### To Install the Default License File on the Secondary Cisco Unity 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 screen, click **Next**.
- Step 4** Click **Add**.
- Step 5** Install the default license file:
- Browse to the **CommServer\Licenses** directory.
  - Double-click **CiscoUnity40.lic**.
- Click **Next**.
- Step 6** In the Licenses list, confirm that the license information is correct.
- Step 7** Click **Next**.
- Step 8** Click **Finish**.
- 

## Setting New Default Passwords

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

#### 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.

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

- You are configuring Cisco Unity as Voice Messaging.
- Subscribers will only access messages using the phone.

- Subscribers will not have access to Cisco Personal Communications Assistant.
- You will be creating Cisco Unity subscribers using the Cisco Unity Administrator.

When a subscriber is created 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**

Anyone who knows the password for the Active Directory account, knows the alias for a subscriber, and knows which Exchange server the voice messages for that subscriber are stored on can access those messages.

- Step 3** When the Password Hardening wizard finishes, the Integrate the Phone System with Cisco Unity screen appears in the main window.

## Configuring Services

From the Cisco Unity Installation and Configuration Assistant, you run the Cisco Unity Services Configuration wizard fourth 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 screen, click **Next**.
- Step 3** Choose the message store type of the partner Exchange server that you chose in the [“Determining the Partner Exchange Server”](#) section on page 6-2.
- Step 4** Click **Next**.
- Step 5** Follow the on-screen prompts to complete the configuration.

## Configuring Cisco Unity for the Message Store

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

This section contains procedures for configuring Cisco Unity when the partner Exchange server is an Exchange 2003 or Exchange 2000 server, and when it is an Exchange 5.5 server. (You chose the partner Exchange server in the [“Determining the Partner Exchange Server”](#) section on page 6-2. Note that for the Voice Messaging configuration with Exchange 2000 installed on the Cisco Unity server, the Cisco Unity server is the partner Exchange server.)

Do the applicable procedure, depending on the Exchange version on the partner server:

- [Exchange 2003 or Exchange 2000, page 8-9](#)
- [Exchange 5.5, page 8-10](#)

## Exchange 2003 or Exchange 2000

### To Configure Cisco Unity for the Message Store (Exchange 2003 or Exchange 2000)

- 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 server where you want to create new mailboxes. 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 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:
- Click **Change**.
  - 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 2000** or **Microsoft Exchange 2003**, depending on the version of Exchange installed on the partner Exchange server, and click **Next**.
- Step 8** 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 9** 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.
- Step 10** 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:

<b>Create New Accounts or Import Existing Accounts</b>	Click if administrators will create subscriber accounts either by adding a new user to Exchange or by importing existing user data from Exchange.
<b>Import Existing Accounts Only</b>	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**.
- 

## Exchange 5.5

### To Configure Cisco Unity for the Message Store (Exchange 5.5)

---

- 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 server where you want to create new mailboxes. If Exchange is not running, configuring the message store on the Cisco Unity server will fail.
- Step 3** On the Welcome screen, click **Next**.
- Step 4** Enter the password for the installation account, and click **Next**.
- Step 5** In the Select Partner Message Store dialog box, click **Microsoft Exchange 5.5**, and click **Next**.
- Step 6** In the Server Name field, specify the name of the partner Exchange server.
- Step 7** Enter the LDAP port number for the Exchange server that you made note of in the procedure [“To Change the LDAP Port Number of the Exchange 5.5 Server \(When Active Directory Is Installed\)”](#) in the [“Installing Exchange 5.5 Administration Software: Unified Messaging with Exchange on a Separate Server”](#) section on page 6-6.



**Note** When Active Directory and Exchange 5.5 are installed on the same server, the Exchange LDAP port number must be reset from the default of 389, because Active Directory reserves port 389 for LDAP. If you do not know the LDAP port number of the Exchange server, consult the Exchange administrator.

---

- Step 8** Click **Next**.
- Step 9** 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 10**. When installation is complete, you will log on to the Cisco Unity Administrator 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 10** Click **Next**.
- Step 11** Click **OK** to stop Cisco Unity services.

- Step 12** In the Select How Subscribers Will Be Created dialog box, set how administrators will create Cisco Unity subscriber accounts in the Cisco Unity Administrator:

<b>Create New Accounts or Import Existing Accounts</b>	Click if administrators will create subscriber accounts either by adding a new user to Exchange or by importing existing user data from Exchange.
<b>Import Existing Accounts Only</b>	Click if administrators will create subscriber accounts only by importing existing user data from Exchange.

- Step 13** Click **Next**.
- Step 14** By default, the account that you created for Cisco Unity directory and message store services appears. If you want to choose a different account, click **Change**.
- Step 15** Specify a password for the account, and click **Next**.
- Step 16** When message store configuration is complete, click **Finish**.

## 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.

If you are integrating the phone system for a Cisco Unity system without failover or on the primary server for a Cisco Unity system with failover, do the first procedure, “[To Integrate the Phone System with Cisco Unity](#).”

If you are integrating the phone system on the secondary server now, do the second procedure, “[To Integrate the Phone System with Cisco Unity on the Secondary Server](#).”

### To Integrate the Phone System with Cisco Unity

- 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/prod\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_configuration_guides_list.html).)
- When the integration is complete, the Set Up the Cisco Personal Communications Assistant to Use SSL screen appears in the main window.

Do the following procedure if you are integrating the phone system on the secondary Cisco Unity server now for a system with failover. Otherwise, do the first procedure, “[To Integrate the Phone System with Cisco Unity](#).”

### 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 server, with the exception of the Cisco CallManager Device Name Prefix field value for a Cisco CallManager 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 CallManager 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 server.
- When the integration is complete, the Set Up the Cisco Personal Communications Assistant to Use SSL screen 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.

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 8-12](#).

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 8-13](#)
- [Setting Up the Cisco PCA to Use SSL by Using a Certificate Authority, page 8-14](#)

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.

## 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** 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** In the Cisco Unity Installation and Configuration Assistant, 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 running Windows Server 2003, expand **Web Sites**. If not, skip to [Step 5](#)
- 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** In the Web Server Certificate wizard Welcome window, 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 site's common name, enter either the Cisco Unity server's system name or the fully qualified domain name.
-  **Caution** The name must exactly match the host portion of any URL that will access this system 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 close 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 running Windows Server 2003, expand **Web Sites**. If not, skip to [Step 28](#)
  - 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** In the Web Server Certificate wizard Welcome window, 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 enter 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 close 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** In the Cisco Unity Installation and Configuration Assistant, 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 running Windows Server 2003, expand **Web Sites**. If not, skip to [Step 5](#).

- 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** In the Web Server Certificate wizard Welcome window, 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 site's common name, enter either the Cisco Unity server's system name or the fully qualified domain name.
-   
**Caution** The name must exactly match the host portion of any URL that will access this system 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 close 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** In the Certificate Export wizard Welcome window, 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** In Internet Services Manager, expand the name of the Cisco Unity server.
  - Step 5** If the Cisco Unity server is running Windows Server 2003, expand **Web Sites**. If not, skip to [Step 6](#).
  - Step 6** Right-click **Default Web Site**, and click **Properties**.
  - Step 7** In the 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 screen, 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 close the Web Server Certificate wizard window.
  - 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** Close the Cisco Unity Installation and Configuration Assistant.
- 

## Installing the Latest Cisco Unity 4.0(4) Service Release, If Any

Periodically, a number of Cisco Unity engineering specials are rolled up into a Cisco Unity service release. To determine whether a Cisco Unity 4.0(4) service release is available and, if so, to get download and installation instructions, refer to *Release Notes for Cisco Unity 4.0(4) Service Release <x>* at [http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html).

## Testing the Phone System Integration

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

If you are setting up failover, test only the integration with the primary server now. You test the integration with the secondary server after you set up failover. The *Cisco Unity Failover Configuration and Administration Guide* 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 from Virus Scanning the Directory in Which Cisco Unity Is Installed

**Note**

---

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

---

You exclude from scanning the directory in which Cisco Unity is installed, as well as all subdirectories, so that the Cisco Unity Administrator and the Cisco Unity Assistant will work properly.

### To Exclude from Virus Scanning the Directory in Which Cisco Unity Is Installed

- 
- Step 1** Refer to the virus-scanning software Help for instructions on excluding directories from scanning.
- Step 2** Exclude from virus scanning the directory in which Cisco Unity is installed (the default directory is CommServer) and all subdirectories under the directory.
- 

## 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 running Windows Server 2003, expand **Web Sites**. If not, skip to [Step 4](#).
- 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.
- 

## 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 voice 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 for 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**. Information on the Example Administrator appears in the Cisco Unity 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 Administrator.
  - The password does not spell Example Administrator, 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 Log Files

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

As you do the following procedure, if applicable, refer to the drive locations you made note of in the [“Determining the Drive Locations for Files on the Cisco Unity System”](#) section on page 2-5.

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

## To Move the SQL or MSDE Databases and Transaction Log Files

- 
- 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** Stop the Cisco Unity services, and stop and restart the SQL Server or MSDE service:
- On the Windows Start menu, click **Run**.
  - Run **cmd**.
  - Change to the directory in which Cisco Unity is installed (CommServer is the default).
  - Run the command **kill -f av\*** to stop all Cisco Unity services, including the Windows tray icon. (The tray icon may continue to appear in the Windows taskbar, but if you move the mouse cursor over it, it disappears.)
  - Close the Command Prompt window.
  - On the Windows Start menu, click **Programs > Administrative Tools > Services**.
  - Stop and restart the MSSQLSERVER service.
  - Close the Services MMC.
- Step 3** On the Windows Start menu, click **Run**.
- Step 4** Run **cmd**.
- Step 5** Start OSQL by entering **OSQL -E** on the command line.




---

**Caution** OSQL commands are case-sensitive. Enter the instructions exactly as they appear in the procedure.

---

- Step 6** Detach the databases from the data store application by entering the following instructions on the command line:
- Enter **use master** and press **Enter**.
  - Enter **go** and press **Enter**.
  - Enter **EXEC sp\_detach\_db 'UnityDb'** and press **Enter**.

- d. Enter  
**go**  
and press **Enter**.
- e. Enter  
**EXEC sp\_detach\_db 'ReportDb'**  
and press **Enter**.
- f. Enter  
**go**  
and press **Enter**.

**Step 7** In Windows Explorer, create the new database and log destination directories on the drive locations you made note of in the “[Determining the Drive Locations for Files on the Cisco Unity System](#)” section on page 2-5. Use directory names that are easy to remember, for example:

<b>UnityDb.mdf and ReportDb.mdf</b>	<Database destination drive>\<Path>\Unity Data
<b>UnityDb_log.ldf and ReportDb_log.ldf</b>	<Log file destination drive>\<Path>\Unity Logs

- Step 8** In Windows Explorer, copy the databases **UnityDb.mdf** and **ReportDb.mdf** from Program Files\Microsoft SQL Server\MSSQL\Data to the new database destination(s).
- Step 9** In Windows Explorer, copy the transaction log files **UnityDb\_log.ldf** and **ReportDb\_log.ldf** from Program Files\Microsoft SQL Server\MSSQL\Data to the new log file destination(s).
- Step 10** In OSQL, reattach the databases and log files to the data store application by entering the following instructions on the command line:
- a. Enter  
**use master**  
and press **Enter**.
  - b. Enter  
**go**  
and press **Enter**.
  - c. 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**.
  - d. Enter  
**go**  
and press **Enter**.
  - e. 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**.
  - f. Enter  
**go**  
and press **Enter**.

- Step 11** In OSQL, verify the change in the file locations by entering the following instructions on the command line:
- Enter **use UnityDb** and press **Enter**.
  - Enter **go** and press **Enter**.
  - Enter **sp\_helpfile** and press **Enter**.
  - Enter **go** and press **Enter**.
  - The directories in the output should match the directories to which you moved UnityDb.mdf in [Step 8](#) and UnityDb\_log.ldf in [Step 9](#).
  - Repeat Step [a.](#) through Step [d.](#) for ReportDb.
- Step 12** Enter **exit** and press **Enter** to close OSQL.
- Step 13** *Optional:* In Windows Explorer, rename each of the databases and log files in the old locations **<Original file name and extension>.old**. (For example, in its original location, rename UnityDb.mdf to UnityDb.mdf.old.)
- Step 14** On the Windows Start menu, click **Programs > Startup > AvCsTrayStatus** to restart the Cisco Unity tray icon.
- Step 15** When the tray icon appears in the Windows taskbar, use it to restart Cisco Unity.
- 

## 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.

- b. On the General tab, in the Startup Type list, click **Automatic** to re-enable the service.
- c. Click **Start** to start the service.
- d. Click **OK** to close the Properties dialog box.

**Step 4** When the services have been re-enabled, close the Services MMC.

---

## Hardening the Cisco Unity Server



### Note

If the Cisco Unity server is not connected to the corporate network, skip this section.

---

When the Cisco Unity server is connected to the corporate network, we strongly recommend that you harden the server. Refer to *White Paper: Security Best Practices for Cisco Unity 4.0 (With Microsoft Exchange)* at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/whitapr/secure40.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/whitapr/secure40.htm).

