CHAPTER 40

Configuring Text-to-Speech Access to Exchange Emails in Cisco Unity Connection 9.x

See the following sections:

For information on configuring text-to-speech access to Exchange emails in Cisco Unity Connection, see the "Configuring Cisco Unity Connection 9.x and Later and Microsoft Exchange for Unified Messaging" chapter of the *Unified Messaging Guide for Cisco Unity Connection Release*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/unified_messaging/guide/9xcucumgx.html.

About Text-to-Speech Access to Exchange Emails in Cisco Unity Connection

When Cisco Unity Connection is configured to connect to an external message store (a message store other than Cisco Unity Connection), users can hear their emails read to them when they sign in to Cisco Unity Connection by phone. In this chapter, you configure Microsoft Exchange and Cisco Unity Connection so that licensed users can listen to emails.

Note Text-to-speech over Exchange 2007 and Exchange 2010 supports both the IPv4 and IPv6 addresses. However, the IPv6 address works only when Connection platform is configured in Dual (IPv4/IPv6) mode. For more information on Configuring IPv6 settings, see Adding or Changing the IPv6 Addresses of Cisco Unity Connection chapter of *Reconfiguration and Upgrade Guide for Cisco Unity Connection* guide at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/upgrade/guide/9xcucrug051.html.

Configuring Text-to-Speech Access to Exchange 2007 Emails in Cisco Unity Connection

If you configure Cisco Unity Connection to integrate with Exchange 2007, users can access emails in an Exchange 2007 message store.

See the following sections:

For information on configuring text-to-speech access to Exchange emails in Cisco Unity Connection, see the "Configuring Cisco Unity Connection 9.x and Later and Microsoft Exchange for Unified Messaging" chapter of the *Unified Messaging Guide for Cisco Unity Connection Release*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/unified_messaging/guide/9xcucumgx.html.

Task List for Configuring Text-to-Speech Access to Exchange 2007 Emails in Cisco Unity Connection

To enable users to access emails in an Exchange 2007 message store, complete the following tasks in the order presented.

1. Enable IMAP Access to Exchange. See the "Enabling IMAP Access to Exchange in Cisco Unity Connection" section on page 40-3.
2. Create and install an SSL server certificate on each Exchange server on which you want to access email messages. See the "Configuring Secure IMAP with SSL and Enabling the SSL Certificate in Cisco Unity Connection (Exchange 2007 Only)" section on page 40-3.
3. Create Connection external services. See the "Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access in Cisco Unity Connection" section on page 40-4.
4. Configure the users for the external services. See the "Configuring Users for the External Services in Cisco Unity Connection" section on page 40-5.
5. Associate users with a class of service that offers a license to access the TTS feature, and enables them to use it.
6. For each user, create an external service account in Connection that specifies the Exchange server on which the mailbox for the user is stored. This enables users to access their email when they sign in to Connection by phone.

Enabling IMAP Access to Exchange in Cisco Unity Connection

Cisco Unity Connection uses the IMAP protocol to access emails in Exchange so that the messages can be played by using TTS. By default, Exchange is not configured to allow IMAP access to messages. Do the following procedure to enable IMAP access on each Exchange server that contains emails that you want licensed Connection users to be able to access.

To Enable IMAP Access to Exchange in Cisco Unity Connection

Step 1 On an Exchange server that contains emails that you want licensed Connection users to be able to access, sign in to Windows by using an account that is a member of the local Administrators group.

Step 2 On the Windows Start menu, select **Administrative Tools > Services**.

Step 3 In the right pane, find the **Microsoft Exchange IMAP4** service.

Step 4 If the value of the Status column is **Started** and the value of the Startup Type column is **Automatic**, skip to Step 9.

If the values are different, double-click **Microsoft Exchange IMAP4**.

Step 5 In the Microsoft Exchange IMAP4 Properties dialog box, if Startup Type is not Automatic, change it to **Automatic**.

Step 6 If Service Status is not Started, select **Start**.

Step 7 Select **OK** to close the Microsoft Exchange IMAP4 Properties dialog box.

Step 8 Close the Services MMC.

Step 9 Repeat Step 1 through Step 8 on each Exchange server that contains emails that you want licensed Connection users to be able to access.

Configuring Secure IMAP with SSL and Enabling the SSL Certificate in Cisco Unity Connection (Exchange 2007 Only)

To Configure Secure IMAP with SSL and Enable the SSL Certificate in Cisco Unity Connection (Exchange 2007 Only)

Step 1 On the Exchange Server, open the **Exchange Management Shell** application.

Step 2 Enter the following command, where <Exchange server> is the IP address or host name of the Exchange server and <friendly name> is the friendly name that you select for the Exchange server:

new-exchangecertificate -generaterequest -domainname <Exchange server> -friendlyname <friendly name>-path c:\csr.txt

Caution The domain name for the Exchange server must be the IP address or the fully qualified DNS name (recommended) so that the Connection server can successfully ping the Exchange server. Otherwise, users may not be able to access their emails in the external message store.

Step 3 Press **Enter**. A Certificate Signing Request (CSR) file with the name Csr.txt is created in the root directory.

Step 4 Send the CSR file to a Certification Authority (CA), which will generate and send back a new certificate.

Note You must have a copy of the CA public root certificate or public root certificate chain. This certificate is needed for configuring Connection to trust the Exchange 2007 server.

Step 5 Enter the following command, where <path> is the location of the directory where the CA will save the new server certificate:

import-exchangecertificate -path <path>

Step 6 Press **Enter**.

Step 7 Enter the following command:

dir cert:\localmachine\my | fl

Step 8 Press **Enter**.

Step 9 Highlight the "thumbprint" property and press **Ctrl-C** to copy it to the clipboard.

Step 10 If Connection will be configured to use IMAP to access email from an external email server and use calendar data from Exchange 2007, enter the following command, where <thumbprint> is the "thumbprint" that you copied in Step 9:

enable-exchangecertificate -thumbprint <thumbprint> -services "IIS,IMAP"

If Connection will not be configured to use IMAP but will be configured to use calendar data from Exchange 2007, enter the following command, where <thumbprint> is the "thumbprint" that you copied in Step 9.

enable-exchangecertificate -thumbprint <thumbprint> -services "IIS"

Step 11 Press **Enter**.

Step 12 If you want data transmitted as clear text, skip the remaining steps in this procedure and continue with the "Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access in Cisco Unity Connection" section on page 40-4. Otherwise, open the **IIS Manager** application.

Step 13 Go to **IIS > <server name> > Web Sites > Default Web Site**.

Step 14 Right-click **Default Web Site** and select **Properties**.

Step 15 In the Properties dialog box, select the **Directory Security** tab.

Step 16 Under Secure Communications, select **Edit**.

Step 17 Check the **Require Secure Channel** check box.

Step 18 Select **OK**.

Step 19 In the Properties dialog box, select **OK**.

Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access in Cisco Unity Connection

In Cisco Unity Connection Administration, you create and configure one IMAP Service for each Exchange server that contains emails that you want licensed Connection users to be able to access.

To Specify the Exchange Servers on Which Cisco Unity Connection Users Can Access Emails in Cisco Unity Connection

Step 1 In Cisco Unity Connection Administration, expand **System Settings**, then select **External Services**.

Step 2 On the Search External Services page, select **Add New**.

Step 3 On the New External Service page, in the Type list, select **Exchange 2007 External Service Template**.

Step 4 Confirm that the **Enabled** check box is checked.

Step 5 In the Display Name field, enter a name that will help you identify the service when you configure Connection users to access their email. (For example, in the name of the service, you might include the name of the Exchange server that contains the email that users are accessing.)

Step 6 In the Server field, enter the server name or the fully qualified domain name of one of the Exchange servers that contain emails that you want licensed Connection users to be able to access.

The value that you enter must match the server name or the fully qualified domain name in the certificate for the Exchange server.

Step 7 In the Authentication Mode list, select **NTLM**.

Step 8 In the Security Transport Type list, if you created and installed SSL certificates, select **SSL**. Otherwise, select **None**.

Step 9 If you selected **SSL** in Step 8, check the **Validate Server Certificates** check box. Otherwise, skip to Step 10.

Self-signed certificates cannot be validated. If you selected **SSL** in Step 8 and you are using self-signed certificates, do not check the **Validate Server Certificates** check box, or Connection will not be able to access Exchange.

Step 10 Under Service Capabilities, check the **User Access to Email in Third-Party Message Store** check box.

Step 11 Select **Save**.

Step 12 Repeat Step 2 through Step 13 for each additional Exchange 2007 server that contains emails that you want licensed Connection users to access.

Step 13 Close Cisco Unity Connection Administration.

Configuring Users for the External Services in Cisco Unity Connection

Do the following procedure.

Note Exchange must have a user for each Connection user that you are configuring.

To Configure Users for the External Services in Cisco Unity Connection

Step 1 In Cisco Unity Connection Administration, expand **Users**, then select **Users**.

Step 2 On the Search Users page, select the alias of a user.

Step 3 On the Edit User Basics page, on the Edit menu, select **External Service Accounts**.

Step 4 On the External Service Accounts page, select **Add New**.

Step 5 On the New External Service Accounts page, in the External Service field, select the display name of the applicable external service that you created in the "Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access in Cisco Unity Connection" section on page 40-4.

Step 6 In the Email Address field, enter the email address for the user.

Step 7 In the Sign-In Type field, select the applicable option:

- **Use Connection Alias**—This option is useful when the User ID setting in Exchange 2007 is the same as the Connection user alias. Connection will sign in the user with the Connection user alias.
- **Use User ID Provided Below**—Enter the User ID setting from Exchange 2007 (useful when the User ID setting is different from the Connection user alias). Connection will sign in the user with the setting in this field.

Step 8 *(Only when the Use User ID Provided Below option is selected in Step 7)* In the User ID field, enter the User ID setting from Exchange.

Step 9 In the Password field, enter the password from Exchange. Connection will sign in the user with the setting in this field.

Step 10 Under Service Capabilities, check the **User Access to Email in Third-Party Message Store** check box.

Step 11 Select **Save**.

Step 12 To check the Exchange configuration for the user, select **Test**. The Task Execution Results window appears with the test results.

If any part of the test fails, verify the configuration for Exchange, Cisco Unity Connection, and the user.

Step 13 Repeat Step 2 through Step 12 for all remaining users.

Configuring Text-to-Speech Access to Exchange 2003 Emails in Cisco Unity Connection

If you configure Cisco Unity Connection to integrate with Exchange 2003, users can access emails in an Exchange 2003 message store.

See the following sections:

- Configuring Users for the External Services in Cisco Unity Connection, page 40-17

For information on configuring text-to-speech access to Exchange emails in Cisco Unity Connection, see the "Configuring Cisco Unity Connection 9.x and Later and Microsoft Exchange for Unified Messaging" chapter of the *Unified Messaging Guide for Cisco Unity Connection Release*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/unified_messaging/guide/9xcucumgx.html.

Task List for Configuring Text-to-Speech Access to Exchange 2003 Emails in Cisco Unity Connection

To enable users to emails on an Exchange 2003 message store, complete the following tasks in the order presented.

1. Enable IMAP access to Exchange 2003. See the "Enabling IMAP Access to Exchange in Cisco Unity Connection" section on page 40-7.
2. Create an Active Directory service account that Connection uses to access Exchange data, and grant the account the necessary permissions. See the "Creating and Configuring an Active Directory Service Account in Cisco Unity Connection (Exchange 2003 Only)" section on page 40-8.
3. Create and install an SSL server certificate on each Exchange server on which you want to access email messages. See the "Creating and Installing SSL Certificates in Cisco Unity Connection (Exchange 2003 Only)" section on page 40-9.
4. *(Optional but recommended)* Configure IIS to refuse unencrypted communications from web clients including Connection. See the "Requiring Secure Communication Between Cisco Unity Connection and Exchange in Cisco Unity Connection (Exchange 2003 Only)" section on page 40-14.
5. Configure Connection to trust the SSL certificates that you created and installed on the Exchange servers. See the "Configuring the Cisco Unity Connection Server to Trust Exchange Certificates in Cisco Unity Connection (Exchange 2003 Only)" section on page 40-14.
6. Create Connection external services. See the "Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access in Cisco Unity Connection" section on page 40-16.
7. Configure the users for the external services. See the "Configuring Users for the External Services in Cisco Unity Connection" section on page 40-17.
8. Associate users with a class of service that offers a license to access the TTS feature, and enables them to use it.
9. For each user, create an external service account in Connection that specifies the Exchange server on which the mailbox for the user is stored. This enables the user to access their email when they sign in to Connection by phone.

Enabling IMAP Access to Exchange in Cisco Unity Connection

Cisco Unity Connection uses the IMAP protocol to access emails in Exchange so the messages can be played by using TTS. By default, Exchange is not configured to allow IMAP access to messages. Do the following procedure to enable IMAP access on each Exchange server that contains emails that you want licensed Connection users to be able to listen to by using TTS.

To Enable IMAP Access to Exchange in Cisco Unity Connection

Step 1 On an Exchange server that contains emails that you want licensed Connection users to be able to access, sign in to Windows by using an account that is a member of the local Administrators group.

Step 2 On the Windows Start menu, select **Administrative Tools > Services**.

Step 3 In the right pane, find the **Microsoft Exchange IMAP4** service.

Step 4 If the value of the Status column is **Started** and the value of the Startup Type column is **Automatic**, skip to Step 9.

If the values are different, double-click **Microsoft Exchange IMAP4**.

Step 5 In the Microsoft Exchange IMAP4 Properties dialog box, if Startup Type is not Automatic, change it to **Automatic**.

Step 6 If Service Status is not Started, select **Start**.

Step 7 Select **OK** to close the Microsoft Exchange IMAP4 Properties dialog box.

Step 8 Close the Services MMC.

Step 9 Repeat Step 1 through Step 8 on each Exchange server that contains emails that you want licensed Connection users to be able to access.

Creating and Configuring an Active Directory Service Account in Cisco Unity Connection (Exchange 2003 Only)

Cisco Unity Connection accesses Exchange 2003 email by using an Active Directory account that acts as a proxy for Connection. Do the following procedure to create the service account and give it the necessary permissions.

To Create and Configure a Service Account That Can Access Exchange Emails in Cisco Unity Connection

Step 1 On a computer on which Active Directory Users and Computers and Exchange System Manager are installed, sign in to Windows by using an account that is a member of the Domain Administrators group.

Step 2 On the Windows Start menu, select **Programs > Microsoft Exchange > Active Directory Users and Computers**.

Step 3 In the left pane, expand **<Server name>**, right-click **Users**, and select **New > User**.

Step 4 Follow the on-screen prompts to create a domain user account. Do not create a mailbox.

Step 5 On the Windows Start menu, select **Programs > Microsoft Exchange > System Manager**.

Step 6 In the left pane, expand **Servers**.

Step 7 Right-click the name of the Exchange server that contains mailboxes that will be accessed by Cisco Unity Connection, and select **Properties**.

Step 8 In the <Server name> Properties dialog box, select the **Security** tab.

Step 9 Select **Add**.

Step 10 In the Select Users, Computers, or Groups dialog box, in the Enter the Object Names to Select field, enter the name of the service account that you created in Step 4.

Step 11 Select **Check Names**.

Step 12 Select **OK** to close the dialog box.

Step 13 In the <Server name> Properties dialog box, in the Group or User Names list, select the name of the service account.

Step 14 In the Permissions For <Account name> list, set the permissions:

a. For Full Control, check the **Deny** check box.

Note Ensure that the List Contents and the Read Properties are set to **Allow** on the Exchange Servers Security tab.

b. For Receive As, check the **Allow** check box

Caution If Exchange server 2003 is configured for Single Inbox, Step 14a. will break Single Inbox permission requirements. Single Inbox needs Receive As, the Send As, and the Administer Information Store permissions to be set to **Allow**.

Step 15 Select **OK** to close the <Server name> Properties dialog box.

Step 16 Repeat Step 7 through Step 15 for each additional Exchange server on which you want to access emails.

Creating and Installing SSL Certificates in Cisco Unity Connection (Exchange 2003 Only)

In this section, you create and install an SSL certificate on each Exchange server that contains emails that you want licensed Connection users to be able to access. This prevents Cisco Unity Connection from sending the credentials of the service account that you created in the "Creating and Configuring an Active Directory Service Account in Cisco Unity Connection (Exchange 2003 Only)" section on page 40-8 over the network as unencrypted text. It also prevents Exchange from sending email content over the network in unencrypted text.

If you use another method to create and install certificates, use the applicable documentation.

This section contains four procedures. Do them in the order listed, as applicable.

If you want to issue SSL certificates by using:

- Microsoft Certificate Services—do the following procedure on any server in the same domain as the Exchange servers that contain emails that you want licensed Connection users to be able to access.
- Another application—see the documentation for that application for installation instructions. Then skip to the "To Create a Certificate Signing Request in Cisco Unity Connection" procedure on page 40-10.
- An external certification authority—skip to the "To Create a Certificate Signing Request in Cisco Unity Connection" procedure on page 40-10.

To Install the Microsoft Certificate Services Component in Cisco Unity Connection

Step 1 Locate a Windows Server 2003 disc, which you may be prompted to use to complete the installation of the Microsoft Certificate Services component.

Step 2 Sign in to Windows by using an account that is a member of the local Administrators group.

Step 3 On the Windows Start menu, select **Settings > Control Panel > Add or Remove Programs**.

Step 4 In the left pane of the Add or Remove Programs control panel, select **Add/Remove Windows Components**.

Step 5 In the Windows Components dialog box, check the **Certificate Services** check box. Do not change any other items.

Step 6 When the warning appears about not being able to rename the computer or to change domain membership, select **Yes**.

Step 7 Select **Next**.

Step 8 On the CA Type page, select **Stand-alone Root CA**, and select **Next**. (A standalone certification authority (CA) is a CA that does not require Active Directory.)

Step 9 On the CA Identifying Information page, in the Common Name for This CA field, enter a name for the certification authority.

Step 10 Accept the default value in the Distinguished Name Suffix field.

Step 11 For Validity Period, accept the default value of **5 Years**.

Step 12 Select **Next**.

Step 13 On the Certificate Database Settings page, select **Next** to accept the default values.

If a message appears indicating that Internet Information Services is running on the computer and must be stopped before proceeding, select **Yes** to stop the services.

Step 14 If you are prompted to insert the Windows Server 2003 disc into the drive, insert either the Cisco Unity Connection disc, which contains the same required software, or a Windows Server 2003 disc.

Step 15 In the Completing the Windows Components Wizard dialog box, select **Finish**.

Step 16 Close the Add or Remove Programs dialog box.

Do the following procedure for each Exchange server that contains emails that you want licensed Connection users to be able to access.

To Create a Certificate Signing Request in Cisco Unity Connection

---

Step 1 On a server on which Exchange System Manager is installed, sign in to Windows by using an account that is an Exchange Full Administrator.

Step 2 On the Windows Start menu, select **Programs > Microsoft Exchange > System Manager**.

Step 3 In the left pane, expand **<Organization> > Administrative Groups > <Administrative group> > Servers > <Server name> > Protocols > IMAP4**, where <Administrative group> and <Server name> identify the first Exchange server that contains emails that you want licensed Connection users to be able to access.

Step 4 Right-click **Default IMAP4 Virtual Server**, and select **Properties**.

Step 5 In the Properties dialog box, select the **Access** tab.

Step 6 Select **Certificate**.

Step 7 On the Welcome to the Web Server Certificate Wizard page, select **Next**.

Step 8 On the Server Certificate page, select **Create a New Certificate**.

Step 9 Select **Next**.

Step 10 On the Delayed or Immediate Request page, select **Prepare the Request Now But Send It Later**.

Step 11 Select **Next**.

Step 12 On the Name and Security Settings page, enter a name for the certificate (for example, <Server name>_Cert).

Step 13 Select **Next**.

Step 14 On the Organization Information page, enter the applicable values.

Step 15 Select **Next**.

Step 16 On the Your Site's Common Name page, enter the computer name of the Exchange server or the fully qualified domain name.

Remember whether you specified the computer name or the fully qualified domain name. You will need this information in a later procedure.

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

Step 17 Select **Next**.

Step 18 On the Geographical Information page, enter the applicable information.

Step 19 Select **Next**.

Step 20 On the Certificate Request File Name page, enter a path and filename, and write down the information. You will need it in a later procedure.

If this is not the server on which you installed Microsoft Certificate Services in the "To Install the Microsoft Certificate Services Component in Cisco Unity Connection" procedure on page 40-9, try to select a network location that you can access from the current server and from the server on which Microsoft Certificate Services is installed.

Step 21 Select **Next**.

Step 22 On the Request File Summary page, select **Next**.

Step 23 On the Completing the Web Server Certificate Wizard page, select **Finish**.

Step 24 Select **OK** to close the Default IMAP4 Virtual Server Properties dialog box.

Step 25 Repeat Step 3 through Step 24 to create a certificate signing request for each additional Exchange server that contains emails that you want licensed Connection users to be able to access.

Step 26 Close Exchange System Manager.

Step 27 If Microsoft Certificate Services is on another server and you were not able to save the certificate request files in a network location accessible to that server, copy the certificate request files to a removable medium (diskette, CD, or DVD).

Step 28 If you are not using an external certification authority, you are finished with this procedure.

If you are using an external certification authority, send the certificate request file that you specified in Step 20 to the CA. When the certificate returns from the CA, skip to the "To Install the Server Certificate in Cisco Unity Connection" procedure on page 40-13.

Issue certificates or have them issued for each of the certificate signing requests that you created in the "To Create a Certificate Signing Request in Cisco Unity Connection" procedure on page 40-10:

- If you are using Microsoft Certificate Services to issue certificates, do the following procedure.
- If you are using an application other than Microsoft Certificate Services, see the documentation for the application for information on issuing server certificates and exporting a trust certificate. When you export the trust certificate, which is uploaded to the Cisco Unity Connection server later in this chapter, export it in base-64 encoded X.509 format with a .pem filename extension. Then continue with the "To Install the Server Certificate in Cisco Unity Connection" procedure on page 40-13.
- If you are using an external certification authority (CA) to issue certificates, send the certificate signing requests to the CA. Request that the CA provide the trust certificate, which is uploaded to the Cisco Unity Connection server later in this chapter, in base-64 encoded X.509 format with a .pem filename extension. When the certificates are returned, continue with the "To Install the Server Certificate in Cisco Unity Connection" procedure on page 40-13.

To Issue the Server Certificate in Cisco Unity Connection (Only When You Are Using Microsoft Certificate Services to Issue the Certificate)

Step 1 On the server on which you installed Microsoft Certificate Services, sign in to Windows by using an account that is a member of the Domain Admins group.

Step 2 On the Windows Start menu, select **Programs > Administrative Tools > Certification Authority**.

Step 3 In the left pane, expand **Certification Authority (Local) > <Certification authority name>**, where <Certification authority name> is the name that you gave to the certification authority when you installed Microsoft Certificate Services in the "To Install the Microsoft Certificate Services Component in Cisco Unity Connection" procedure on page 40-9.

Step 4 Right-click the name of the certification authority, and select **All Tasks > Submit New Request**.

Step 5 In the Open Request File dialog box, browse to the location of the first certificate signing request file that you created in the "To Create a Certificate Signing Request in Cisco Unity Connection" procedure on page 40-10, and double-click the file.

Step 6 In the left pane of Certification Authority, select **Pending Requests**.

Step 7 Right-click on the pending request that you submitted in Step 5, and select **All Tasks > Issue**.

Step 8 In the left pane of Certification Authority, select **Issued Certificates**.

Step 9 Right-click the new certificate, and select **All Tasks > Export Binary Data**.

Step 10 In the Export Binary Data dialog box, in the Columns that Contain Binary Data list, select **Binary Certificate**.

Step 11 Select **Save Binary Data to a File**.

Step 12 Select **OK**.

Step 13 In the Save Binary Data dialog box, enter a path and filename, and write down the information. You will need it in a later procedure.

If this is not a server on which Exchange System Manager is installed, try to select a network location that you can access from the current server and from the server on which Microsoft Certificate Services is installed.

Step 14 Select **OK**.

Step 15 If you created more than one certificate signing request in the "To Create a Certificate Signing Request in Cisco Unity Connection" procedure on page 40-10, repeat Step 9 through Step 11 for each certificate signing request listed under Issued Certificates.

Step 16 Close Certification Authority.

Step 17 If Exchange System Manager is on another server, and if you were not able to save the certificate request files in a network location accessible to that server, copy the certificate request files to a removable medium (diskette, CD, or DVD).

Do the following procedure for each Exchange server that contains emails that you want licensed Connection users to be able to access.

To Install the Server Certificate in Cisco Unity Connection

Step 1 On a computer on which Exchange System Manager is installed, sign in to Windows by using an account that is an Exchange Full Administrator.

Step 2 On the Windows Start menu, select **Programs > Microsoft Exchange > System Manager**.

Step 3 In the left pane, expand **<Organization name> > Administrative Groups > <Administrative group> > Servers > <Server name> > Protocols > IMAP4**, where <Administrative group> and <Server name> identify the first Exchange server that contains emails that you want licensed Connection users to be able to access.

Step 4 Right-click **Default IMAP4 Virtual Server**, and select **Properties**.

Step 5 Select the **Access** tab.

Step 6 Select **Certificate**.

Step 7 On the Welcome to the Web Server Certificate Wizard, select **Next**.

Step 8 On the Pending Certificate Request page, select **Process the Pending Request and Install the Certificate**.

Step 9 Select **Next**.

Step 10 On the Process a Pending Request page, browse to the location where you saved the certificates, and specify the server certificate that you created using Microsoft Certificate Services or another application, or that you got from an external CA.

You may have to change the value of the Files of Type list to All Files (*.*) to see the certificates.

Step 11 Select **Next**.

Step 12 On the Certificate Summary page, select **Next**.

Step 13 On the Completing the Web Server Certificate Wizard page, select **Finish**.

Step 14 Close the Default IMAP4 Virtual Server Properties dialog box.

Step 15 Repeat Step 3 through Step 14 for each certificate that you want to install.

Step 16 Close Exchange System Manager.

Requiring Secure Communication Between Cisco Unity Connection and Exchange in Cisco Unity Connection (Exchange 2003 Only)

Earlier in this chapter, you enabled IMAP access to Exchange, and you secured the IMAP connections between the Cisco Unity Connection server and one or more Exchange servers. To prevent Exchange from allowing access through unsecured IMAP connections, do the following procedure on each Exchange server that you are allowing Cisco Unity Connection to access.

To Configure Exchange to Require Secure Communication with Cisco Unity Connection (Optional But Recommended)

Step 1 On an Exchange server that contains emails that you want licensed Connection users to be able to access, sign in to Windows by using an account that is an Exchange Full Administrator.

Step 2 On the Windows Start menu, select **Programs > Microsoft Exchange > System Manager**.

Step 3 In the left pane, expand **Servers > <Server name> > Protocols > IMAP4 > Default IMAP4 Virtual Server**.

Step 4 Right-click **Default IMAP4 Virtual Server**, and select **Properties**.

Step 5 Select the **Access** tab.

Step 6 Select **Communication**.

Step 7 Select **Require Secure Channel**.

Step 8 Select **OK**.

Step 9 Close the Properties dialog box.

Step 10 In the left pane, for the same server, expand **Servers > <Server name> > Protocols > IMAP4 > Default IMAP4 Virtual Server**.

Step 11 In the System Manager toolbar, select the **Stop** icon.

Step 12 Wait a few seconds.

Step 13 Select the **Play** icon.

Step 14 Repeat Step 1 through Step 13 for each additional Exchange server that contains emails that you want licensed Connection users to be able to access.

Configuring the Cisco Unity Connection Server to Trust Exchange Certificates in Cisco Unity Connection (Exchange 2003 Only)

To make the Cisco Unity Connection server trust the certificates for the Exchange servers, you need to upload, to the root certificate store on the Connection server, a trust certificate for each certification authority that issued certificates. Typically, you will use the same certification authority (for example, Microsoft Certificate Services or VeriSign) to issue all certificates.

To Configure the Cisco Unity Connection Server to Trust Exchange Certificates

Step 1 If you used Microsoft Certificate Services to issue the certificates, continue with Step 2.

If you used another application or an external certification authority to issue the certificates, skip to Step 21 to upload the trust certificates, in base-64-encoded X.509 format, to the root certificate store on the Connection server.

Step 2 On the server on which you installed Microsoft Certificate Services, sign in to Windows by using an account that is a member of the local Administrators group.

Step 3 On the Windows Start menu, select **Programs > Administrative Tools > Certification Authority**.

Step 4 In the left pane, expand **Certification Authority (Local)**.

Step 5 Right-click the name of the certification authority, and select **Properties**.

Step 6 In the <Certification authority name> Properties dialog box, on the **General** tab, in the CA Certificates list, select the name of one of the certificates that you issued for the Exchange servers.

Step 7 Select **View Certificate.**

Step 8 In the Certificate dialog box, select the **Details** tab.

Step 9 Select **Copy to File**.

Step 10 On the Welcome to the Certificate Export Wizard page, select **Next**.

Step 11 On the Export File Format page, select **Base-64 Encoded X.509 (.CER)**.

Step 12 Select **Next**.

Step 13 On the File to Export page, enter a temporary path and filename for the trust certificate (for example, c:\cacert.pem). Use the filename extension **.pem**.

Caution The trust certificate must have a .pem filename extension or you will not be able to upload it on the Connection server.

Step 14 Write down the path and filename because you will need it later in this procedure.

Step 15 Select **Next**.

Step 16 On the Completing the Certificate Export Wizard page, select **Finish**.

Step 17 Select **OK** to close the “Export successful” message box.

Step 18 Select **OK** to close the Certificate dialog box.

Step 19 Select **OK** to close the <Server name> Properties dialog box.

Step 20 Close **Certification Authority**.

Step 21 Copy the trust certificate to a network location that is accessible to the Connection server.

Step 22 On the Connection server, sign in to Cisco Unified Operating System Administration.

Step 23 On the Security menu, select **Certificate Management**.

Step 24 On the Certificate List page, select **Upload Certificate**.

Step 25 On the Upload Certificate page, in the Certificate Name list, select **Connection-trust**.

Step 26 In the Root Certificate field, enter the name of the certificate file that you issued using Microsoft Certificate Services or another certification authority, or that you got from a CA.

Step 27 Select **Browse**.

Step 28 In the Choose File dialog box, browse to the location of the certificate file, select the name of the file, and select **Open**.

Step 29 On the Upload Certificate page, select **Upload File**.

Step 30 When the Status area reports that the upload succeeded, select **Close**.

Step 31 If you issued certificates or had them issued by more than one certification authority, repeat Step 24 through Step 30 for each trust certificate.

Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access in Cisco Unity Connection

In Cisco Unity Connection Administration, you create and configure one IMAP Service for each Exchange server that contains emails that you want licensed Connection users to be able to access.

To Specify the Exchange Servers on Which Cisco Unity Connection Users Can Access Emails in Cisco Unity Connection

Step 1 In Cisco Unity Connection Administration, expand **System Settings**, then select **External Services**.

Step 2 On the Search External Services page, select **Add New**.

Step 3 On the New External Service page, in the Type list, select **Exchange 2003 External Service Template**.

Step 4 Confirm that the **Enabled** check box is checked.

Step 5 In the Display Name field, enter a name that will help you identify the service when you configure Connection users to access their email. (For example, in the name of the service, you might include the name of the Exchange server that contains the email that users are accessing.)

Step 6 In the Server field, enter the server name or the fully qualified domain name of one of the Exchange servers that contain emails that you want licensed Connection users to be able to access.

The value that you enter must match the server name or the fully qualified domain name in the certificate for the Exchange server, which you specified in Step 16 of the "To Create a Certificate Signing Request in Cisco Unity Connection" procedure on page 40-10.

Step 7 In the Authentication Mode list, select **NTLM**.

Step 8 In the Security Transport Type list, if you created and installed SSL certificates, select **SSL**. Otherwise, select **None**.

Step 9 If you selected SSL in Step 8, check the **Validate Server Certificates** check box. Otherwise, continue to Step 10.

Self-signed certificates cannot be validated. If you selected **SSL** in Step 8 and you are using self-signed certificates, do not check the **Validate Server Certificates** check box, or Connection will not be able to access Exchange.

Step 10 Under Service Credentials, in the Alias field, enter the Active Directory user sign-in name of the service account that you created in the "To Create and Configure a Service Account That Can Access Exchange Emails in Cisco Unity Connection" procedure on page 40-8. Use the format **<Domain name>\<Account name>**.

Step 11 In the Password field, enter the password for the service account.

Step 12 Under Service Capabilities, check the **User Access to Email in Third-Party Message Store** check box.

Step 13 Select **Save**.

Step 14 Repeat Step 2 through Step 13 for each additional Exchange server that contains emails that you want licensed Connection users to be able to access.

Step 15 Close Cisco Unity Connection Administration.

Configuring Users for the External Services in Cisco Unity Connection

Do the following procedure.

Note Exchange must have a user for each Connection user that you are configuring.

To Configure Users for the External Services in Cisco Unity Connection

Step 1 In Cisco Unity Connection Administration, expand **Users**, then select **Users**.

Step 2 On the Search Users page, select the alias of a user.

Step 3 On the Edit User Basics page, on the Edit menu, select **External Service Accounts**.

Step 4 On the External Service Accounts page, select **Add New**.

Step 5 On the New External Service Accounts page, in the External Service field, select the display name of the applicable external service that you created in the "Creating Cisco Unity Connection External Services to Specify the Exchange Servers That Users Can Access in Cisco Unity Connection" section on page 40-16.

Step 6 In the Email Address field, enter the email address for the user.

Step 7 In the Sign-In Type field, select the applicable option:

- **Use Connection Alias**—This option is useful when the User ID setting in Exchange 2003 is the same as the Connection user alias. Connection will sign in the user with the Connection user alias.
- **Use User ID Provided Below**—Enter the User ID setting from Exchange 2003 (useful when the User ID setting is different from the Connection user alias). Connection will sign in the user with the setting in this field.

Step 8 *(Only when the Use User ID Provided Below option is selected in Step 7)* In the User ID field, enter the User ID setting from Exchange.

Step 9 Under Service Capabilities, check the **User Access to Email in Third-Party Message Store** check box.

Step 10 Select **Save**.

Step 11 To check the Exchange configuration for the user, select **Test**. The Task Execution Results window appears with the test results.

If any part of the test fails, verify the configuration for Exchange, Cisco Unity Connection, and the user.

Step 12 Repeat Step 2 through Step 11 for all remaining users.