



# Configuring Access to Exchange E-Mails Through TTS

In this chapter, you configure Microsoft Exchange and Cisco Unity Connection so that licensed users can use text to speech (TTS) to listen to Exchange e-mails. (Note that access to Exchange e-mails by using TTS is a licensed feature, and that there is additional configuration when you create user accounts later.) When you are finished with this chapter, return to “[Overview of Mandatory Tasks for Installing a Cisco Unity Connection 1.x System](#).”



Note

The tasks in the list reference detailed instructions in the *Cisco Unity Connection Installation Guide* and in other Cisco Unity Connection documentation. Follow the documentation for a successful installation.

This chapter contains the following sections:

- [Enabling IMAP Access to Exchange, page 8-1](#)
- [Creating and Configuring a Service Account That Can Access Exchange E-Mails, page 8-2](#)
- [Creating and Installing SSL Certificates, page 8-3](#)
- [Configuring Exchange to Refuse Non-Secure IMAP Connections \(Optional\), page 8-7](#)
- [Configuring the Cisco Unity Connection Server to Trust Exchange Certificates, page 8-8](#)
- [Specifying the Exchange Servers on Which Connection Users Can Access E-Mails by Using TTS, page 8-9](#)

## Enabling IMAP Access to Exchange

Cisco Unity Connection uses the IMAP protocol to access e-mails 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 e-mails that you want licensed Connection users to be able to listen to by using TTS.

### Enabling IMAP Access to Exchange

- Step 1** On an Exchange server that contains e-mails that you want licensed Connection users to be able to listen to by using TTS, log on to Windows by using an account that is a member of the local Administrators group.
- Step 2** On the Windows Start menu, click **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, click **Start**.
  - Step 7** Click **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 e-mails that you want licensed Connection users to be able to listen to by using TTS.
- 

## Creating and Configuring a Service Account That Can Access Exchange E-Mails

Cisco Unity Connection needs a service account that it can use to access Exchange e-mails. Do the following procedure to create the account and give it Receive As permission.

### To Create and Configure a Service Account that Can Access Exchange E-Mails

---

- Step 1** On a computer on which Active Directory Users and Computers and Exchange System Manager are installed, log on to Windows by using an account that is a member of the Domain Administrators group.
- Step 2** On the Windows Start menu, click **Programs > Microsoft Exchange > Active Directory Users and Computers**.
- Step 3** In the left pane, expand <**Server name**>, right-click **Users**, and click **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, click **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 click **Properties**.
- Step 8** In the <Server name> Properties dialog box, click the **Security** tab.
- Step 9** Click **Add**.

**Step 10** Specify the service account name, depending on the Exchange version:

<b>Exchange 2003</b>	<p>a. 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 you created in <a href="#">Step 4</a>.</p> <p>b. Click <b>Check Names</b>.</p>
<b>Exchange 2000</b>	<p>a. In the Select Users, Computers, or Groups dialog box, in the Look In list, click the name of the domain in which you created the service account in <a href="#">Step 4</a>.</p> <p>b. In the list of users, computers, and groups, double-click the name of the service account.</p> <p>The Delegate Control dialog box reappears. The account you selected appears in the Group (Recommended) or User box.</p>

**Step 11** Click **OK** to close the dialog box.

**Step 12** In the <Server name> Properties dialog box, in the Group or User Names list, click the name of the service account.

**Step 13** In the Permissions For <Account name> list, set the permissions:

- a. For Full Control, check the **Deny** check box.
- b. For Receive As, check the **Allow** check box

**Step 14** Click **OK** to close the <Server name> Properties dialog box.

**Step 15** Repeat [Step 7](#) through [Step 14](#) for each additional Exchange server on which you want to access e-mails.

## Creating and Installing SSL Certificates

In this section, you create and install an SSL certificate on each Exchange server that contains e-mails that you want licensed Connection users to be able to listen to by using TTS. This prevents Cisco Unity Connection from sending the credentials of the service account that you created in the [“Creating and Configuring a Service Account That Can Access Exchange E-Mails”](#) section on page 8-2 over the network as unencrypted text. It also prevents Exchange from sending e-mail 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.

Do the following procedure on any server in the same domain as the Exchange servers that contain e-mails that you want licensed Connection users to be able to listen to by using TTS.

### To Install the Microsoft Certificate Services Component

**Step 1** Log on to Windows by using an account that is a member of the local Administrators group.

**Step 2** On the Windows Start menu, click **Settings > Control Panel > Add or Remove Programs**.

**Step 3** In the left pane of the Add or Remove Programs control panel, click **Add/Remove Windows Components**.

- Step 4** In the Windows Components dialog box, check the **Certificate Services** check box. Do not change any other items.
- Step 5** When the warning appears about not being able to rename the computer or to change domain membership, click **Yes**.
- Step 6** Click **Next**.
- Step 7** On the CA Type page, click **Stand-alone Root CA**, and click **Next**. (A stand-alone certification authority (CA) is a CA that does not require Active Directory.)
- Step 8** On the CA Identifying Information page, in the Common Name for This CA field, enter a name for the certification authority.
- Step 9** Accept the default value in the Distinguished Name Suffix field.
- Step 10** For Validity Period, accept the default value of **5 years**.
- Step 11** Click **Next**.
- Step 12** On the Certificate Database Settings page, click **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, click **Yes** to stop the services.
- Step 13** 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 14** In the Completing the Windows Components Wizard dialog box, click **Finish**.
- Step 15** Close the Add or Remove Programs dialog box.

---

Do the following procedure for each Exchange server that contains e-mails that you want licensed Connection users to be able to listen to by using TTS.

#### To Create a Certificate Signing Request

---

- Step 1** On a computer on which Exchange System Manager is installed, log on to Windows by using an account that is an Exchange Full Administrator.
- Step 2** On the Windows Start menu, click **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 e-mails that you want licensed Connection users to be able to listen to by using TTS.
- Step 4** Right-click **Default IMAP4 Virtual Server**, and click **Properties**.
- Step 5** In the Properties dialog box, click the **Access** tab.
- Step 6** Click **Certificate**.
- Step 7** On the Welcome to the Web Server Certificate Wizard page, click **Next**.
- Step 8** On the Server Certificate page, click **Create a New Certificate**.
- Step 9** Click **Next**.
- Step 10** On the Delayed or Immediate Request page, click **Prepare the Request Now But Send it Later**.
- Step 11** Click **Next**.

- Step 12** On the Name and Security Settings page, enter a name for the certificate. (For example, <Server name>\_Cert.)
- Step 13** Click **Next**.
- Step 14** On the Organization Information page, enter the applicable values.
- Step 15** Click **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** Click **Next**.
- Step 18** On the Geographical Information page, enter the applicable information.
- Step 19** Click **Next**.
- Step 20** On the Certificate Request File Name page, enter a path and file name, 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” procedure on page 8-3](#), try to choose a network location that you can access from the current server and from the server on which Microsoft Certificate Services is installed.
- Step 21** Click **Next**.
- Step 22** On the Request File Summary page, click **Next**.
- Step 23** On the Completing the Web Server Certificate Wizard page, click **Finish**.
- Step 24** Click **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 e-mails that you want licensed Connection users to be able to listen to by using TTS.
- 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 Certificate” procedure on page 8-6](#).
- 

Do the following procedure for each Exchange server that contains e-mails that you want licensed Connection users to be able to listen to by using TTS.

### To Issue the Certificate (Only When You Are Using Microsoft Certificate Services to Issue the Certificate)

---

- Step 1 On the server on which you installed Microsoft Certificate Services, log on to Windows by using an account that is a member of the Domain Admins group.
  - Step 2 On the Windows Start menu, click **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” procedure on page 8-3](#).
  - Step 4 Right-click the name of the certification authority, and click **All Tasks > Submit New Request**.
  - Step 5 Browse to the location of the first certificate signing request file that you created in the [“To Create a Certificate Signing Request” procedure on page 8-4](#), and double-click the file.
  - Step 6 In the left pane of Certification Authority, click **Pending Requests**.
  - Step 7 Right-click on the pending request that you submitted in [Step 5](#), and click **All Tasks > Issue**.
  - Step 8 In the left pane of Certification Authority, click **Issued Certificates**.
  - Step 9 Right-click the new certificate, and click **All Tasks > Export Binary Data**.
  - Step 10 In the Export Binary Data dialog box, in the Columns that Contain Binary Data list, click **Binary Certificate**.
  - Step 11 Click **Save Binary Data to a File**.
  - Step 12 Enter a path and file name, 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 choose a network location that you can access from the current server and from the server on which Microsoft Certificate Services is installed.
  - Step 13 Click **OK**.
  - Step 14 If you created more than one certificate signing request in the [“To Create a Certificate Signing Request” procedure on page 8-4](#), repeat [Step 9](#) through [Step 11](#) for each certificate signing request listed under Issued Certificates.
  - Step 15 Close Certification Authority.
  - Step 16 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 e-mails that you want licensed Connection users to be able to listen to by using TTS.

### To Install the Certificate

---

- Step 1 On a computer on which Exchange System Manager is installed, log on to Windows by using an account that is an Exchange Full Administrator.
- Step 2 On the Windows Start menu, click **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 e-mails that you want licensed Connection users to be able to listen to by using TTS.
- Step 4** Right-click **Default IMAP4 Virtual Server**, and click **Properties**.
- Step 5** Click the **Access** tab.
- Step 6** Click **Certificate**.
- Step 7** On the Welcome to the Web Server Certificate Wizard, click **Next**.
- Step 8** On the Pending Certificate Request page, click **Process the Pending Request and Install the Certificate**.
- Step 9** Click **Next**.
- Step 10** On the Process a Pending Request page, browse to the location where you saved the certificates, and specify the applicable file, depending on the CA that you used:

Sent the certificate request to an external CA	Specify the file that you got from the external CA.
Issued the certificate by using the Windows Certification Authority application	Specify the file that you created in <a href="#">Step 10</a> of the “ <a href="#">To Issue the Certificate (Only When You Are Using Microsoft Certificate Services to Issue the Certificate)</a> ” procedure on page 8-6.

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

- Step 11** Click **Next**.
- Step 12** On the Certificate Summary page, click **Next**.
- Step 13** On the Completing the Web Server Certificate Wizard page, click **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.

## Configuring Exchange to Refuse Non-Secure IMAP Connections (Optional)

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 Refuse Non-Secure IMAP Connections

- Step 1** On an Exchange server that contains e-mails that you want licensed Connection users to be able to listen to by using TTS, log on to Windows by using an account that is an Exchange Full Administrator.
- Step 2** On the Windows Start menu, click **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 click **Properties**.
  - Step 5 Click the **Communication** tab.
  - Step 6 Click **Require Secure Channel**.
  - Step 7 Click **OK**.
  - Step 8 Close the Properties dialog box.
  - Step 9 In the left pane, for the same server, expand **Servers > <Server name> > Protocols > IMAP4 > Default IMAP4 Virtual Server**.
  - Step 10 In the System Manager toolbar, click the **Stop** icon.
  - Step 11 Wait a few seconds.
  - Step 12 Click the **Play** icon.
  - Step 13 Repeat [Step 3](#) through [Step 12](#) for each additional Exchange server that contains e-mails that you want licensed Connection users to be able to listen to by using TTS.
- 

## Configuring the Cisco Unity Connection Server to Trust Exchange Certificates

To make the Cisco Unity Connection server trust the certificates for the Exchange servers, you need to add the certification authority's signing certificate to the root certificate store for the Connection server.

### To Configure the Cisco Unity Connection Server to Trust Exchange Certificates

---

- Step 1 On the server on which you installed certification authority, log on to Windows by using an account that is a member of the local Administrators group.
- Step 2 On the Windows Start menu, click **Programs > Administrative Tools > Certification Authority**.
- Step 3 In the left pane, expand **Certification Authority (Local)**.
- Step 4 Right-click the name of the certification authority, and click **Properties**.
- Step 5 In the <Certification authority name> Properties dialog box, click the **General** tab.
- Step 6 In the CA Certificates list, click the name of one of the certificates that you created for the Exchange servers.
- Step 7 Click **View Certificate**.
- Step 8 In the Certificate dialog box, click the **Details** tab.
- Step 9 Click **Copy to File**.
- Step 10 On the Welcome to the Certificate Export Wizard page, click **Next**.
- Step 11 On the Export File Format page, click **Base-64 Encoded X.509 (.CER)**.
- Step 12 Click **Next**.

- Step 13** On the File to Export page, enter a temporary path and file name of the certificate export file (for example, c:\cacert.cer). Write down the path and file name because you will need it later in this procedure.
- Step 14** Click **Next**.
- Step 15** On the Completing the Certificate Export Wizard page, click **Finish**.
- Step 16** Click **OK** to close the “Export successful” message box.
- Step 17** Click **OK** to close the Certificate dialog box.
- Step 18** Click **OK** to close the <Server name> Properties dialog box.
- Step 19** Close **Certification Authority**.
- Step 20** Copy the certificate export file that you specified in [Step 13](#) to the Cisco Unity Connection server and save it in the Utilities directory on the drive where Connection software is installed (usually drive G).
- Step 21** On the Windows Start menu, click **Programs > Accessories > Command Prompt**.
- Step 22** Change to the **Utilities** directory.
- Step 23** Run the following command, where <Certificate export file.cer> is the name of the certificate export file that you created in [Step 13](#):
- ```
certmgr /add /c <certificate export file.cer> /r localMachine /s root
```
- Note that the name of the application is certmgr, not CuCertMgr, which is in the same directory.
- 

## Specifying the Exchange Servers on Which Connection Users Can Access E-Mails by Using TTS

Do the following procedure to specify the Exchange servers that contain e-mails that you want licensed Cisco Unity Connection users to be able to listen to by using TTS.

### To Specify the Exchange Servers on Which Connection Users Can Access E-Mails by Using TTS

---

- Step 1** On the Cisco Unity Connection server, log on to Windows by using an account that is a member of the local Administrators group.
- Step 2** On the desktop, double-click the **Connection Administration** icon.
- Step 3** In Cisco Unity Connection Administration, expand **System Settings**, then click **External Services**.
- Step 4** Click **Add New**.
- Step 5** In the Type list, click **IMAP Service**.
- Step 6** For Display Name, enter a name that identifies this external service as being associated with one of the Exchange servers that contain e-mails that you want licensed Connection users to be able to listen to by using TTS.

The value that you enter here is also the value that you will choose when you enable TTS for Connection users.

- Step 7** For Server Address, enter the server name or the fully qualified domain name of one of the Exchange servers that contain e-mails that you want licensed Connection users to be able to listen to by using TTS. 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](#)” procedure on page 8-4.
- Step 8** For Service Login and Service Password, enter the domain-qualified name (for example, Domain1\UnitySvc) and the password of the account that you created in the “[To Create and Configure a Service Account that Can Access Exchange E-Mails](#)” procedure on page 8-2.
- Step 9** In the Security Transport list, click **SSL**.
- Step 10** Click **Save**.
- Step 11** Repeat [Step 4](#) through [Step 10](#) for each additional Exchange server that contains e-mails that you want licensed Connection users to be able to listen to by using TTS.
- Step 12** Close Cisco Unity Connection Administration.
-