



## CHAPTER 32

# Configuring Access to Exchange E-Mails Through TTS

---

Text to Speech (TTS) allows users to hear their Exchange e-mails read to them when they log on to Cisco Unity Connection by phone. 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.

See the following sections:

- [Task List for Offering TTS Access to Exchange E-Mail, page 32-1](#)
- [Enabling IMAP Access to Exchange, page 32-2](#)
- [Creating and Configuring an Active Directory Service Account \(Exchange 2000 and Exchange 2003 Only\), page 32-3](#)
- [Creating and Installing SSL Certificates \(Exchange 2000 and Exchange 2003 Only\), page 32-4](#)
- [Requiring Secure Communication Between Connection and Exchange \(Exchange 2000 and Exchange 2003 Only\), page 32-8](#)
- [Configuring the Connection Server to Trust Exchange Certificates \(Exchange 2000 and Exchange 2003 Only\), page 32-9](#)
- [Creating Connection External Services to Specify the Exchange Servers That Users Can Access by Using TTS, page 32-10](#)

## Task List for Offering TTS Access to Exchange E-Mail

To enable users to use TTS, complete the following tasks in the order presented.



### Caution

---

Using TTS to access Exchange 2007 e-mail is supported. However, creating and installing an SSL server certificate on Exchange 2007 servers to secure TTS access to Exchange e-mail is currently not supported. When support is added, a tech note will be posted on Cisco.com.

---

1. Configure access to Exchange mailboxes:
  - a. If all of the Exchange mailboxes that users want to access are in Exchange 2007, skip to Step e. If any of the Exchange mailboxes that users want to access are in Exchange 2000 or Exchange 2003, 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 \(Exchange 2000 and Exchange 2003 Only\)”](#) section on page 32-3.

- b. Create and install an SSL server certificate on each Exchange server on which you want to access e-mail messages. See the “[Creating and Installing SSL Certificates \(Exchange 2000 and Exchange 2003 Only\)](#)” section on page 32-4.
  - c. *Optional but recommended:* Configure IIS not to accept unencrypted communications from web clients including Connection. See the “[Requiring Secure Communication Between Connection and Exchange \(Exchange 2000 and Exchange 2003 Only\)](#)” section on page 32-8.
  - d. Configure Connection to trust the SSL certificates that you created and installed on the Exchange servers. See the “[Configuring the Connection Server to Trust Exchange Certificates \(Exchange 2000 and Exchange 2003 Only\)](#)” section on page 32-9.
  - e. Create Connection external services. See the “[Creating Connection External Services to Specify the Exchange Servers That Users Can Access by Using TTS](#)” section on page 32-10.
2. Associate users with a class of service that offers a license to access the TTS feature, and enables them to use it. See the “[Text to Speech Access to Exchange E-Mail](#)” section in the “[Setting Up Features and Functionality That Are Controlled by Class of Service](#)” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*, available at [http://www.cisco.com/en/US/products/ps6509/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html).
  3. 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 e-mail when they log on to Connection by phone.
  4. If you have users who access their e-mail messages on a Microsoft Exchange server by using Outlook (with MAPI) or Outlook Web Access and will also use Connection to manage e-mail messages, make sure that they understand how each application handles deleted messages. See the “[Potential User Concerns and Misconceptions](#)” section in the “[Operator and Support Desk Orientation](#)” chapter of the *User Workstation Setup Guide for Cisco Unity Connection*, available at [http://www.cisco.com/en/US/products/ps6509/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html).

## 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 an Active Directory Service Account (Exchange 2000 and Exchange 2003 Only)

Cisco Unity Connection accesses Exchange 2000 and Exchange 2003 e-mail 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 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><b>a.</b> 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 <a href="#">Step 4</a>.</p> <p><b>b.</b> Click <b>Check Names</b>.</p>
<b>Exchange 2000</b>	<p><b>a.</b> 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>b.</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:
- For Full Control, check the **Deny** check box.
  - 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 (Exchange 2000 and Exchange 2003 Only)

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 an Active Directory Service Account \(Exchange 2000 and Exchange 2003 Only\)”](#) section on page 32-3 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, 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 e-mails that you want licensed Connection users to be able to listen to by using TTS.
- Another application—see the documentation for that application for installation instructions. Then skip to the [“To Create a Certificate Signing Request”](#) procedure on page 32-5.
- An external certification authority—skip to the [“To Create a Certificate Signing Request”](#) procedure on page 32-5.

### To Install the Microsoft Certificate Services Component

---

- 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** Log on to Windows by using an account that is a member of the local Administrators group.
- Step 3** On the Windows Start menu, click **Settings > Control Panel > Add or Remove Programs**.
- Step 4** In the left pane of the Add or Remove Programs control panel, click **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, click **Yes**.
- Step 7** Click **Next**.

- Step 8** 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 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** Click **Next**.
- Step 13** 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 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, click **Finish**.
- Step 16** 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 server 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 32-4](#), 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 Server Certificate” procedure on page 32-8](#).

---

Issue certificates or have them issued for each of the certificate signing requests that you created in the [“To Create a Certificate Signing Request” procedure on page 32-5](#):

- 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” procedure on page 32-8](#).

- 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” procedure on page 32-8](#).

#### To Issue the Server 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 32-4](#).
- Step 4** Right-click the name of the certification authority, and click **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” procedure on page 32-5](#), 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** Click **OK**.
- Step 13** In the Save Binary Data dialog box, 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 14** Click **OK**.
- Step 15** If you created more than one certificate signing request in the [“To Create a Certificate Signing Request” procedure on page 32-5](#), 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 e-mails that you want licensed Connection users to be able to listen to by using TTS.

### To Install the Server 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 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** 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.
- 

## Requiring Secure Communication Between Connection and Exchange (Exchange 2000 and 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 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 **Access** tab.
  - Step 6** Click **Communication**.
  - Step 7** Click **Require Secure Channel**.
  - Step 8** Click **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, click the **Stop** icon.
  - Step 12** Wait a few seconds.
  - Step 13** Click the **Play** icon.
  - Step 14** Repeat [Step 1](#) through [Step 13](#) 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 Connection Server to Trust Exchange Certificates (Exchange 2000 and 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, log on to Windows by using an account that is a member of the local Administrators group.
- Step 3** On the Windows Start menu, click **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 click **Properties**.
- Step 6** In the <Certification authority name> Properties dialog box, on the **General** tab, in the CA Certificates list, click the name of one of the certificates that you issued 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 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 file name because you will need it later in this procedure.
- Step 15** Click **Next**.
- Step 16** On the Completing the Certificate Export Wizard page, click **Finish**.
- Step 17** Click **OK** to close the “Export successful” message box.
- Step 18** Click **OK** to close the Certificate dialog box.
- Step 19** Click **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, log on to Cisco Unified Operating System Administration.
- Step 23** On the Security menu, click **Certificate Management**.
- Step 24** On the Certificate List page, click **Upload Certificate**.
- Step 25** On the Upload Certificate page, in the Certificate Name list, click **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** Click **Browse**.
- Step 28** In the Choose File dialog box, browse to the location of the certificate file, click the name of the file, and click **Open**.
- Step 29** On the Upload Certificate page, click **Upload File**.
- Step 30** When the Status area reports that the upload succeeded, click **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 Connection External Services to Specify the Exchange Servers That Users Can Access by Using TTS

In Cisco Unity Connection Administration, you create and configure one IMAP Service for each Exchange server that contains e-mails that you want licensed 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** In Cisco Unity Connection Administration, expand **System Settings**, then click **External Services**.
- Step 2** Click **Add New**.
- Step 3** In the Type list, click **IMAP**.
- Step 4** In the Display Name field, enter a name that will help you identify the service when you configure Connection users to access their e-mail. (For example, in the name of the service, you might include the name of the Exchange server that contains the e-mail that users are accessing.)
- Step 5** In the DNS Address of Server field, 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 32-5.
- Step 6** Confirm that the **Access Enabled** check box is checked.
- Step 7** If you are accessing an Exchange 2007 server:
- Uncheck the Use Service Credentials check box.
  - Leave the Service Login and Service Password fields blank.
  - In the Security Transport list, click **None**.
  - Skip to [Step 8](#).
- If you are accessing an Exchange 2000 or Exchange 2003 server:
- Check the Use Service Credentials check box.
  - In the Service Login field, enter the Active Directory user logon name of the service account that you created in the “[To Create and Configure a Service Account that Can Access Exchange E-Mails](#)” procedure on page 32-3. Use the format <**Domain name**>\<**Account name**>.
  - In the Service Password field, enter the password for the service account.
  - In the Security Transport list, if you created and installed SSL certificates, click **SSL**. Otherwise, click **None**.
- Step 8** Click **Save**.
- Step 9** Repeat [Step 2](#) through [Step 8](#) 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 10** Close Cisco Unity Connection Administration.
-

