



## Securing Cisco PCA and IMAP E-Mail Client Access to Cisco Unity Connection

In this chapter, you create and install an SSL certificate on the Cisco Unity Connection server by using Microsoft Certificate Services. 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.

The chapter contains the following sections:

- [Deciding Whether to Create and Install an SSL Certificate, page 7-1](#)
- [Creating and Installing an SSL Certificate, page 7-2](#)

## Deciding Whether to Create and Install an SSL Certificate

Cisco Unity Connection automatically creates and installs a local certificate to secure communication between the Cisco PCA and Connection, and between IMAP e-mail clients and Connection. This means that all network traffic (including user names, passwords, other text data, and voice messages) between the Cisco PCA and Connection is automatically encrypted, and network traffic between IMAP e-mail clients and Connection is automatically encrypted if you enable encryption in the IMAP clients.



### Note

If you are using the Connection secure-messaging feature, which encrypts voice messages before they are stored on the Connection server, you cannot use either the Cisco PCA or IMAP e-mail clients to listen to Connection voice messages.

If you want to reduce the risk of man-in-the-middle attacks, do the procedures in this chapter to create a certificate signing request, issue the certificate by using Microsoft Certificate Services or have it issued by another certification authority, and install the certificate on the Cisco Unity Connection server.

The Cisco PCA website provides access to the web tools that users use to manage messages and personal preferences with Cisco Unity Connection. Note that IMAP client access to Connection voice messages is a licensed feature.

If you decide to install an SSL certificate, consider adding the certificate to the Trusted Root Store on user workstations. Without the addition, the web browser will display security alerts for users accessing the Cisco PCA and for users accessing Connection voice messages with some IMAP e-mail clients.

(Information on managing security alerts and configuring supported IMAP e-mail clients is provided in the *Cisco Unity Connection User Setup Guide, Release 1.x* 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). The “Overview of Mandatory Tasks for Installing a Cisco Unity Connection 1.x System” in this guide alerts you when to do the tasks.)

## Creating and Installing an SSL Certificate

In this section you create and install a certificate by using Microsoft Certificate Services. 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 whose IP address can be resolved by all client computers that will be using the Cisco PCA or that will be using an IMAP client to access Connection voice messages.

### 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.
-

### To Create a Certificate Signing Request

---

- 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 Windows Start menu, click **Programs > Accessories > Command Prompt**.
- Step 3** Change to the **CiscoUnityConnection\Utilities\CuCert** directory on the drive where Connection software is installed.
- Step 4** Enter the command **cucert -c** and press **Enter**.  
Cucert displays the following text:  
Certificate signing request created: G:\CiscoUnityConnection\Utilities\CuCert\cunewcert.csr
- Step 5** Close the Command Prompt window.
- Step 6** If you are using Microsoft Certificate Services to issue the certificate, and if Certificate Services is on another server, copy **Cunewcert.csr** to a network location accessible to that server, or copy it to a removable medium (diskette, CD, or DVD).
- Step 7** 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, **Cunewcert.csr**, to the CA. When the certificate returns from the CA, skip to the [“To Install the Certificate” procedure on page 7-4](#).
- 

### 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 7-2](#).
- 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 certificate signing request file that you created in the [“To Create a Certificate Signing Request” procedure on page 7-3](#), and double-click the file.
- Step 6** In the left pane of Certification Authority, click **Pending Requests**.
- Step 7** Right-click 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 the Cisco Unity Connection server, 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** Close Certification Authority.
- Step 15** If this is not the Cisco Unity Connection 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).
- 

#### To Install the Certificate

---

- 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** Copy the certificate that you issued by using Microsoft Certificate Services or that a CA issued to the **Utilities\CuCert** directory on the drive where Connection software is installed.
- Step 3** On the Windows Start menu, click **Programs > Accessories > Command Prompt**.
- Step 4** Change to the **Utilities\CuCert** directory on the drive where Connection software is installed.
- Step 5** Enter the command **cucert -i <certificate file name>** and press **Enter**.
- Step 6** Close the Command Prompt window.
- Step 7** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
- Step 8** In the right pane, right-click **Apache Tomcat**, and click **Stop**.
- Step 9** Right-click **Apache Tomcat** again, and click **Start**.
- Step 10** If Cisco Unity Connection users are using an IMAP client to access voice messages, repeat [Step 8](#) and [Step 9](#) for the **CuIMAPsvr** service.
- Step 11** Close Services.
-