



CHAPTER 22

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

This chapter contains information on creating a certificate signing request, issuing an SSL certificate (or having it issued by an external certification authority), and installing the certificate on the Cisco Unity Connection server to secure Cisco Personal Communications Assistant (Cisco PCA) and IMAP e-mail client access to Cisco Unity Connection.

See the following sections:

- [Deciding Whether to Create and Install an SSL Certificate, page 22-1](#)
- [Creating and Installing an SSL Server Certificate, page 22-2](#)

Deciding Whether to Create and Install an SSL Certificate

When you install Cisco Unity Connection, a local certificate is automatically created and installed 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. However, if you want to reduce the risk of man-in-the-middle attacks, do the procedures in this chapter.

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, we recommend that you also consider adding the certification authority's trust certificate to the Trusted Root Store on user workstations. Without the addition, the web browser will display security alerts for users who access the Cisco PCA and for users who access 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 *User Workstation Setup Guide for Cisco Unity Connection*, available at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.)

Creating and Installing an SSL Server Certificate

Do the following tasks to create and install an SSL server certificate to secure Cisco Personal Communications Assistant and IMAP e-mail client access to Cisco Unity Connection:

1. If you are using Microsoft Certificate Services to issue certificates, install Microsoft Certificate Services. Do the [“To Install the Microsoft Certificate Services Component” procedure on page 22-2](#).

If you are using another application to issue certificates, install the application. See the manufacturer documentation for installation instructions. Then skip to Step 2.

If you are using an external certification authority to issue certificates, skip to Step 2.



Note If you already have installed Microsoft Certificate Services or another application that can create certificate signing requests, skip this procedure.

2. Create a certificate signing request. Then download the certificate signing request to the server on which you installed Microsoft Certificate Services or another application that issues certificates, or download the request to a server that you can use to send the certificate signing request to an external certification authority (CA). Do the [“To Create and Download a Certificate Signing Request” procedure on page 22-3](#).

3. If you are using Microsoft Certificate Services to issue the server certificate, do the [“To Issue the Server Certificate \(Only When You Are Using Microsoft Certificate Services to Issue the Certificate\)” procedure on page 22-3](#).

If you are using another application to issue the certificate, see the documentation for the application for information on issuing certificates.

If you are using an external CA to issue the certificate, send the certificate signing request to the external CA. When the external CA returns the certificate, continue with Step 4.

4. Install the server certificate on the Cisco Unity Connection server. Do the [“To Install the Certificate” procedure on page 22-4](#).

To Install the Microsoft Certificate Services Component

- Step 1** On any server whose DNS name (FQDN) or 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, 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 and Download a Certificate Signing Request

- Step 1** Log on to Cisco Unified Operating System Administration.
- Step 2** On the Security menu, click **Certificate Management**.
- Step 3** On the Certificate List page, click **Generate CSR**.
- Step 4** On the Generate Certificate Signing Request page, in the **Certificate Name** list, click **tomcat**.
- Step 5** Click **Generate CSR**.
- Step 6** When the Status area displays a message that the CSR was successfully generated, click **Close**.
- Step 7** On the Certificate List page, click **Download CSR**.
- Step 8** On the Download Certificate Signing Request page, in the **Certificate Name** list, click **tomcat**.
- Step 9** Click **Download CSR**.
- Step 10** In the File Download dialog box, click **Save**.
- Step 11** In the Save As dialog box, in the **Save As Type** list, click **All Files**.
- Step 12** Save the file **tomcat.csr** to a location on the server on which you installed Microsoft Certificate Services or on a server that you can use to send the CSR to an external certification authority.
- Step 13** On the Download Certificate Signing Request page, click **Close**.
-

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 22-2](#).
- 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 and Download a Certificate Signing Request” procedure on page 22-3](#), 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** 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.
- Choose a network location that you can access from the Cisco Unity Connection server.
- Step 14** Click **OK**.
- Step 15** Close Certification Authority.
-

To Install the Certificate

- Step 1** Log on to Cisco Unified Operating System Administration.
- Step 2** On the Security menu, click **Certificate Management**.
- Step 3** On the Certificate List page, click **Upload Certificate**.
- Step 4** On the Upload Certificate page, in the **Certificate Name** list, click **tomcat-trust**.
- Step 5** In the Root Certificate field, enter the name of the certificate file that you either issued using Microsoft Certificate Services or another application, or that you got from an external CA.
- Step 6** Click **Browse**.
- Step 7** In the Choose File dialog box, browse to the location of the certificate file, click the name of the file, and click **Open**.
- Step 8** On the Upload Certificate page, click **Upload File**.
- Step 9** When the Status area reports that the upload succeeded, click **Close**.
-