CHAPTER 25

Securing Cisco PCA and IMAP Email 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 email client access to Cisco Unity Connection.

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

See the following sections:

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 email 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 email 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.

If you decide to install an SSL certificate, we recommend that you also consider adding the trust certificate of the certification authority to the Trusted Root Store on user workstations. Without the addition, the web browser displays security alerts for users who access the Cisco PCA and for users who access Connection voice messages with some IMAP email clients.

(For information on managing security alerts, see the "Managing Security Alerts When Using Self-Signed Certificates with SSL Connections" section in the "Setting Up Access to the Cisco Personal Communications Assistant" chapter of the *User Workstation Setup Guide for Cisco Unity Connection*. For information on configuring supported IMAP email clients, see the "Configuring an Email Account to Access Cisco Unity Connection Voice Messages" chapter of the same guide.)

Creating and Installing an SSL Server Certificate

Revised May 2009

Do the following tasks to create and install an SSL server certificate to secure Cisco Personal Communications Assistant and IMAP email 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 25-3.

   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 to Step 2.

2. If a Connection cluster is configured, run the `set web-security` CLI command on both Connection servers in the cluster and assign both servers the same alternate name. The alternate name will automatically be included in the certificate signing request and in the certificate. For information on the `set web-security` CLI command, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.
3. If a Connection cluster is configured, configure a DNS A record that contains the alternate name that you assigned in Step 2. List the publisher server first. This allows all IMAP email applications and the Cisco Personal Communications Assistant to access Connection voice messages by using the same Connection server name.
4. 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 CA. Do the "To Create and Download a Certificate Signing Request" procedure on page 25-3.

   If a Connection cluster is configured, do this step for both servers in the Connection cluster.
5. If you are using Microsoft Certificate Services to export the issuer certificate and to issue the server certificate, do the "To Export the Issuer Certificate and to Issue the Server Certificate (Only When You Are Using Microsoft Certificate Services to Issue the Certificate)" procedure on page 25-4.

   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 6.

   If a Connection cluster is configured, do this step for both servers in the Connection cluster.
6. Upload the issuer certificate and the server certificate to the Connection server. Do the "To Upload the Issuer and Server Certificates to the Cisco Unity Connection Server" procedure on page 25-5.

   If a Connection cluster is configured, do this step for both servers in the Connection cluster.
7. Restart the Connection IMAP Server service so that Connection and the IMAP email clients use the new SSL certificates. Do the "To Restart the Connection IMAP Server Service" procedure on page 25-6.

   If a Connection cluster is configured, do this step for both servers in the Connection cluster.

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 use the Cisco PCA or that will use an IMAP client to access Cisco Unity 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, do so.

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 On the Cisco Unity Connection server, 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 Export the Issuer Certificate and 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 25-3.

Step 4 Export the issuer certificate:

a. Right-click the name of the certification authority, and click **Properties**.

b. On the General tab, click **View Certificate**.

c. Click the **Details** tab.

d. Click **Copy to File**.

e. On the Welcome to the Certificate Export Wizard page, click **Next**.

f. On the Export File Format page, click **Next** to accept the default value of **DER Encoded Binary X.509 (.CER)**.

g. On the File to Export page, enter a path and file name for the .cer file. Choose a network location that you can access from the Connection server.

Write down the path and file name. You will need it in a later procedure.

h. Follow the onscreen prompts until the wizard has finished the export.

i. Click **OK** to close the Certificate dialog box, and click **OK** again to close the Properties dialog box.

Step 5 Issue the server certificate:

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

b. 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 25-3, and double-click the file.

c. In the left pane of Certification Authority, click **Pending Requests**.

d. Right-click the pending request that you submitted in b., and click **All Tasks > Issue**.

e. In the left pane of Certification Authority, click **Issued Certificates**.

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

g. In the Export Binary Data dialog box, in the Columns that Contain Binary Data list, click **Binary Certificate**.

h. Click **Save Binary Data to a File**.

i. Click **OK**.

j. In the Save Binary Data dialog box, enter a path and file name. Choose a network location that you can access from the Cisco Unity Connection server.

   Write down the path and file name. You will need it in a later procedure.

k. Click **OK**.

Step 6 Close Certification Authority.

To Upload the Issuer and Server Certificates to the Cisco Unity Connection Server

Step 1 On the Cisco Unity Connection server on which you created the certificate signing request, log on to Cisco Unified Operating System Administration.

Step 2 On the Security menu, click **Certificate Management**.

Note If you click **Find** and display a list of the certificates currently installed on the server, you will see an existing, automatically generated, self-signed certificate for Tomcat. That certificate is unrelated to the Tomcat certificates that you upload in this procedure.

Step 3 Upload the issuer certificate:

a. On the Certificate List page, click **Upload Certificate**.

b. On the Upload Certificate page, in the Certificate Name list, click **tomcat-trust**.

c. Leave the Root Certificate field blank.

d. Click **Browse**, and browse to the location of the issuer CA certificate.

   If you used Microsoft Certificate Services to issue the certificate, this is the location of the issuer certificate that you exported in the "To Export the Issuer Certificate and to Issue the Server Certificate (Only When You Are Using Microsoft Certificate Services to Issue the Certificate)" procedure on page 25-4.

   If you used an external certification authority to issue the certificate, this is the location of the issuer CA certificate that you received from the external certification authority.

e. Click the name of the file.

f. Click **Open**.

g. On the Upload Certificate page, click **Upload File**.

h. When the Status area reports that the upload succeeded, click **Close**.

Step 4 Upload the server certificate:

a. On the Certificate List page, click **Upload Certificate**.

b. On the Upload Certificate page, in the Certificate Name list, click **tomcat**.

c. In the Root Certificate field, enter the filename of the issuer certificate that you uploaded in Step 3.

d. Click **Browse**, and browse to the location of the server certificate.

   If you used Microsoft Certificate Services to issue the certificate, this is the location of the server certificate that you issued in the "To Export the Issuer Certificate and to Issue the Server Certificate (Only When You Are Using Microsoft Certificate Services to Issue the Certificate)" procedure on page 25-4.

If you used an external certification authority to issue the certificate, this is the location of the server certificate that you received from the external certification authority.

e. Click the name of the file.

f. Click **Open**.

g. On the Upload Certificate page, click **Upload File**.

h. When the Status area reports that the upload succeeded, click **Close**.

Step 5 Restart the Tomcat service (the service cannot be restarted from Cisco Unified Serviceability):

a. Log on to the Connection server by using an SSH application.

b. Run the following CLI command to restart the Tomcat service:

```
utils service restart Cisco Tomcat
```

To Restart the Connection IMAP Server Service

Step 1 Log on to Cisco Unity Connection Serviceability.

Step 2 On the Tools menu, click **Service Management**.

Step 3 In the Optional Services section, for the Connection IMAP Server service, click **Stop**.

Step 4 When the Status area displays a message that the Connection IMAP Server service was successfully stopped, click **Start** for the service.