Using SSL to Secure Client/Server Connections in 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 Unity Connection. Note that IMAP client access to Unity Connection voice messages is a licensed feature.

See the following sections:

Deciding Whether to Install an SSL Certificate to Secure Cisco PCA, Cisco Unity Connection SRSV, and IMAP Email Client Access to Cisco Unity Connection

When you install Cisco Unity Connection, a local self-signed certificate is automatically created and installed to secure communication between the Cisco PCA and Unity Connection, communication between IMAP email clients and Unity Connection, and communication between Unity Connection SRSV and the central Unity Connection server. This means that all the network traffic (including usernames, passwords, other text data, and voice messages) between the Cisco PCA and Unity

Connection is automatically encrypted, the network traffic between IMAP email clients and Unity Connection is automatically encrypted if you enable encryption in the IMAP clients, and the network traffic between Unity Connection SRSV and the central Unity Connection server is automatically encrypted. 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 Unity Connection voice messages with some IMAP email clients.

"Managing Security Alerts When Using Self-Signed Certificates with SSL Connections in Cisco Unity Connection"For more information on self-signed certificate, refer to the "Securing Connections in Cisco Unity Connection Survivable Remote Site Voicemail 10.x" chapter of the Complete Reference Guide for Cisco Unity Connection Survivable Remote Site Voicemail (SRSV) guide at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/srsv/guide/10xcucsrsvx.html.

Securing Connection Administration, Cisco PCA, Cisco Unity Connection SRSV, and IMAP Email Client Access to Cisco Unity Connection

Do the following tasks to create and install an SSL server certificate to secure Cisco Unity Connection Administration, Cisco Personal Communications Assistant, Unity Connection SRSV, and IMAP email client access to Cisco Unity Connection:

1. If you are using Microsoft Certificate Services to issue certificates, install Microsoft Certificate Services. For information on installing Microsoft Certificate Services on a server running Windows Server 2003, see the "Installing Microsoft Certificate Services (Windows Server 2003 Only)" section on page 10-11. For information on installing Microsoft Certificate Services on a server running a later version of Windows Server, refer to Microsoft documentation.

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

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

Note If you already have installed Microsoft Certificate Services or another application that can create certificate signing requests, skip to Task 2.

2. If a Unity Connection cluster is configured, run the `set web-security` CLI command on both Unity 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 Unity Connection cluster is configured, configure a DNS A record that contains the alternate name that you assigned in Task 2. List the publisher server first. This allows all IMAP email applications, Cisco Personal Communications Assistant, and Unity Connection SRSV to access Unity Connection voice messages by using the same Unity 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 10-3.

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

5. If you are using Microsoft Certificate Services to export the root certificate and to issue the server certificate, do the procedure in the "Exporting the Root Certificate and Issuing the Server Certificate (Microsoft Certificate Services Only)" section on page 10-12.

   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 Task 6.

   Only PEM-formatted (also known as Base-64 encoded DER) certificates can be uploaded to Unity Connection. The certificate must have a .pem filename extension. If the certificate is not in this format, you can usually convert what you have to PEM format by using freely available utilities like OpenSSL.

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

6. Upload the root certificate and the server certificate to the Unity Connection server. Do the "To Upload the Root and Server Certificates to the Cisco Unity Connection Server" procedure on page 10-4.

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

7. Restart the Unity Connection IMAP Server service so that Unity Connection and the IMAP email clients use the new SSL certificates. Do the "To Restart the Unity Connection IMAP Server Service" procedure on page 10-5.

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

8. To prevent users from seeing a security alert whenever they access Unity Connection by using the Connection Administration, Cisco PCA, or an IMAP email client, do the following tasks on all computers from which users will access Unity Connection:

   - Import the server certificate that you uploaded to the Unity Connection server in Task 6. into the certificate store. The procedure differs based on the browser or IMAP email client. For more information, see the documentation for the browser or IMAP email client.
   - Import the server certificate that you uploaded to the Unity Connection server in Task 6. into the Java store. The procedure differs based on the operating system running on the client computer. For more information, see the operating system documentation and the Java Runtime Environment documentation.

To Create and Download a Certificate Signing Request

Step 1 On the Cisco Unity Connection server, sign in to Cisco Unified Operating System Administration.

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

Step 3 On the Certificate List page, select **Generate CSR**.

Step 4 On the Generate Certificate Signing Request page, in the **Certificate Name** list, select **tomcat**.

Step 5 Select **Generate CSR**.

Step 6 When the Status area displays a message that the CSR was successfully generated, select **Close**.

Step 7 On the Certificate List page, select **Download CSR**.

Step 8 On the Download Certificate Signing Request page, in the **Certificate Name** list, select **tomcat**.

Step 9 Select **Download CSR**.

Step 10 In the File Download dialog box, select **Save**.

Step 11 In the Save As dialog box, in the **Save As Type** list, select **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, select **Close**.

To Upload the Root 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, sign in to Cisco Unified Operating System Administration.

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

Note If you select **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 root certificate:

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

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

c. Leave the Root Certificate field blank.

d. Select **Browse**, and browse to the location of the root CA certificate.

If you used Microsoft Certificate Services to issue the certificate, this is the location of the root certificate that you exported in the "To Export the Root Certificate and to Issue the Server Certificate" procedure on page 10-12.

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

e. Select the name of the file.

f. Select **Open**.

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

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

Step 4 Upload the server certificate:

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

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

c. Select **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 Root Certificate and to Issue the Server Certificate" procedure on page 10-12.

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.

d. Select the name of the file.

e. Select **Open**.

f. On the Upload Certificate page, select **Upload File**.

g. When the Status area reports that the upload succeeded, select **Close**.

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

a. Sign in to the Unity 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 Unity Connection IMAP Server Service

Step 1 Sign in to Cisco Unity Connection Serviceability.

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

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

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

Securing Access to Exchange Calendars, Contacts, and Emails

Securing Access to Cisco Unified MeetingPlace

To secure access to MeetingPlace, do the following tasks.

1. Configure SSL for MeetingPlace. For more information, see the "Configuring SSL for the Cisco Unified MeetingPlace Application Server" chapter of the *Administration Documentation for Cisco Unified MeetingPlace Release 8.0* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_maintenance_guides_list.html.
2. Integrate Unity Connection with MeetingPlace. When you configure Unity Connection for the MeetingPlace calendar integration, specify SSL for the security transport.
3. On the Unity Connection server, upload the root certificate of the certification authority from which you got the server certificate that you installed on the MeetingPlace server in Task 1. Note the following:

- The root certificate is not the same thing as the certificate that was installed on the MeetingPlace server. The root certificate for the certification authority contains a public key that can be used to verify the authenticity of the certificate uploaded to the MeetingPlace server.
- Only PEM-formatted (also known as Base-64 encoded DER) certificates can be uploaded to Unity Connection. The certificate must have a .pem filename extension. If the certificate is not in this format, you can usually convert what you have to PEM format by using freely available utilities like OpenSSL.
- The root certificate filename must not contain any spaces.

To Upload the Root Certificate to the Unity Connection Server

Step 1 Sign in to Cisco Unified Operating System Administration by using the administrator account and password.

The administrator account, which you created during Unity Connection installation, is different from the accounts and passwords that you use to sign in to Connection Administration.

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

Step 3 Select **Upload Certificate**.

Step 4 In the Certificate Name list, select **Connection-trust**.

Step 5 Select **Browse**, and find the file that contains the root certificate for the certification authority that issued the certificate for MeetingPlace.

Step 6 Select **Upload File**.

Securing Access to an LDAP Directory

Securing Communication Between Unity Connection and Cisco Unity Gateway Servers When Unity Connection Networking Is Configured

Do the following tasks to create and install an SSL server certificate to secure Connection Administration, 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. For information on installing Microsoft Certificate Services on a server running Windows Server 2003, see the "Installing Microsoft Certificate Services (Windows Server 2003 Only)" section on page 10-11. For information on installing Microsoft Certificate Services on a server running a later version of Windows Server, refer to Microsoft documentation.

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

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

Note If you already have installed Microsoft Certificate Services or another application that can create certificate signing requests, skip to Task 2.

2. If a Unity Connection cluster is configured for the Unity Connection gateway server, run the `set web-security` CLI command on both Unity 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 Unity Connection cluster is configured for the Unity Connection gateway server, configure a DNS A record that contains the alternate name that you assigned in Task 2. List the publisher server first. This allows Cisco Unity to access Unity Connection voice messages by using the same Unity Connection server name.
4. On the Unity Connection gateway server, 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 on a Unity Connection Gateway Server" procedure on page 10-8.

   If a Unity Connection cluster is configured, do this task for both servers in the Unity Connection cluster.
5. On the Cisco Unity gateway server, 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 on a Cisco Unity Gateway Server" procedure on page 10-8.

   If Cisco Unity failover is configured, do this task for the primary and secondary servers.
6. If you are using Microsoft Certificate Services to export the root certificates and to issue the server certificates, do the procedure in the "Exporting the Root Certificate and Issuing the Server Certificate (Microsoft Certificate Services Only)" section on page 10-12.

   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 certificates, send the certificate signing request to the external CA. When the external CA returns the certificates, continue with Task 7.

   Only PEM-formatted (also known as Base-64 encoded DER) certificates can be uploaded to Unity Connection. The certificate must have a .pem filename extension. If the certificate is not in this format, you can usually convert what you have to PEM format by using freely available utilities like OpenSSL.

   Do this task for the Unity Connection server (both servers if a Unity Connection cluster is configured) and for the Cisco Unity server (both servers if failover is configured).
7. Upload the root certificate and the server certificate to the Unity Connection server. Do the "To Upload the Root and Server Certificates to the Cisco Unity Connection Server" procedure on page 10-4.

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

8. Restart the Unity Connection IMAP Server service so that Unity Connection and the IMAP email clients use the new SSL certificates. Do the "To Restart the Unity Connection IMAP Server Service" procedure on page 10-5.

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

9. Upload the root certificate and the server certificate to the Cisco Unity server. Do the "To Upload the Root and Server Certificates to the Cisco Unity Server" procedure on page 10-10.

   If failover is configured, do this task for the primary and secondary servers.

To Create and Download a Certificate Signing Request on a Unity Connection Gateway Server

Step 1 On the Cisco Unity Connection server, sign in to Cisco Unified Operating System Administration.

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

Step 3 On the Certificate List page, select **Generate CSR**.

Step 4 On the Generate Certificate Signing Request page, in the **Certificate Name** list, select **tomcat**.

Step 5 Select **Generate CSR**.

Step 6 When the Status area displays a message that the CSR was successfully generated, select **Close**.

Step 7 On the Certificate List page, select **Download CSR**.

Step 8 On the Download Certificate Signing Request page, in the **Certificate Name** list, select **tomcat**.

Step 9 Select **Download CSR**.

Step 10 In the File Download dialog box, select **Save**.

Step 11 In the Save As dialog box, in the **Save As Type** list, select **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, select **Close**.

To Create and Download a Certificate Signing Request on a Cisco Unity Gateway Server

Step 1 On the Windows Start menu, select **Programs > Administrative Tools > Internet Information Services (IIS) Manager**.

Step 2 Expand the name of the Cisco Unity server.

Step 3 Expand **Web Sites**.

Step 4 Right-click **Default Web Site**, and select **Properties**.

Step 5 In the Default Web Site Properties dialog box, select the **Directory Security** tab.

Step 6 Under Secure Communications, select **Server Certificate**.

Step 7 In the Web Server Certificate Wizard:

a. Select **Next**.

b. Select **Create a New Certificate**, and select **Next**.

c. Select **Prepare the Request Now, But Send It Later**, and select **Next**.

d. Enter a name and a bit length for the certificate.

We strongly recommend that you choose a bit length of 512. Greater bit lengths may decrease performance.

e. Select **Next**.

f. Enter the organization information, and select **Next**.

g. For the common name of the site, enter either the system name of the Cisco Unity server or the fully qualified domain name.

Caution The name must exactly match the name that the Unity Connection site gateway server uses to construct a URL to access the Cisco Unity server. This name is the value of the Hostname field in Connection Administration on the Networking > Links > Intersite Links page.

h. Select **Next**.

i. Enter the geographical information, and select **Next**.

j. Specify the certificate request filename and location, and write down the filename and location because you will need the information in the next procedure.

k. Save the file to a disk or to a directory that the certificate authority (CA) server can access.

l. Select **Next**.

m. Verify the request file information, and select **Next**.

n. Select **Finish** to exit the Web Server Certificate wizard.

Step 8 Select **OK** to close the Default Web Site Properties dialog box.

Step 9 Close the Internet Information Services Manager window.

To Upload the Root 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, sign in to Cisco Unified Operating System Administration.

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

Note If you select **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 root certificate:

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

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

c. Leave the Root Certificate field blank.

d. Select **Browse**, and browse to the location of the root CA certificate.

If you used Microsoft Certificate Services to issue the certificate, this is the location of the root certificate that you exported in the "To Export the Root Certificate and to Issue the Server Certificate" procedure on page 10-12.

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

e. Select the name of the file.

f. Select **Open**.

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

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

Step 4 Upload the server certificate:

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

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

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

d. Select **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 Root Certificate and to Issue the Server Certificate" procedure on page 10-12.

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. Select the name of the file.

f. Select **Open**.

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

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

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

a. Sign in to the Unity 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 Unity Connection IMAP Server Service

Step 1 Sign in to Cisco Unity Connection Serviceability.

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

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

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

To Upload the Root and Server Certificates to the Cisco Unity Server

Step 1 On the Cisco Unity server, install the Certificates MMC for the computer account.

Step 2 Upload the certificates. For more information, refer to Microsoft documentation.

Installing Microsoft Certificate Services (Windows Server 2003 Only)

If you want to use a third-party certificate authority to issue SSL certificates, or if Microsoft Certificate Services is already installed, skip this section.

Do the procedure in this section if you want to use Microsoft Certificate Services to issue your own certificate and if you want to install the application on a server running Windows Server 2003.

If you want to install a root certification authority (the generic term for Microsoft Certificate Services) on a Windows Server 2008 server, refer to the Windows Server 2008 online help.

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, sign in to Windows by using an account that is a member of the local Administrators group.

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

Step 3 In the left pane of the Add or Remove Programs control panel, select **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, select **Yes**.

Step 6 Select **Next**.

Step 7 On the CA Type page, select **Stand-alone Root CA**, and select **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 Select **Next**.

Step 12 On the Certificate Database Settings page, select **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, select **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, select **Finish**.

Step 15 Close the Add or Remove Programs dialog box.

Exporting the Root Certificate and Issuing the Server Certificate (Microsoft Certificate Services Only)

Do the following procedure only when you are using Microsoft Certificate Services to issue the certificate.

To Export the Root Certificate and to Issue the Server Certificate

Step 1 On the server on which you installed Microsoft Certificate Services, sign in to Windows by using an account that is a member of the Domain Admins group.

Step 2 On the Windows Start menu, select **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 10-11.

Step 4 Export the root certificate:

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

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

c. Select the **Details** tab.

d. Select **Copy to File**.

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

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

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

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

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

i. Select **OK** to close the Certificate dialog box, and select **OK** again to close the Properties dialog box.

Step 5 Issue the server certificate:

a. Right-click the name of the certification authority, and select **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 10-3, and double-click the file.

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

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

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

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

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

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

i. Select **OK**.

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

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

k. Select **OK**.

Step 6 Close Certification Authority.