



## Configuring SSL in Cisco Unity Connection 10.x

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 Unity Connection Administration, Cisco Personal Communications Assistant (Cisco PCA) and IMAP email client access to 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**

IMAP client access to Unity Connection voice messages is a licensed feature.

## 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 Unity Connection, and between IMAP email clients and Unity Connection. This means that all network traffic (including usernames, passwords, other text data, and voice messages) between the Cisco PCA and Unity Connection is automatically encrypted, and network traffic between IMAP email clients and Unity 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 Unity 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 in Cisco Unity Connection 10.x” section in the “Setting Up Access to the Cisco Personal Communications Assistant in Cisco Unity Connection 10.x” chapter of the *User Workstation Setup Guide for Cisco Unity Connection Release 10.x*, available at [http://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/connection/10x/user\\_setup/guide/10xcucuwx/10xcucuwx010.html](http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/user_setup/guide/10xcucuwx/10xcucuwx010.html).

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

Revised April 30, 2014

Do the following tasks to create and install an SSL server certificate to secure Cisco Unity 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 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](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 and the Cisco Personal Communications Assistant to access Unity Connection voice messages 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 30-3.

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 issuer certificate and to issue the server certificate, do the procedure in the “[Exporting Issuer Certificate and Issuing the Server Certificate \(Microsoft Certificate Services Only\)](#)” section on page 30-5.

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.

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

6. Upload the issuer certificate and the server certificate to the Unity Connection server. Do the “[Steps to Upload the Issuer and Server Certificates to the Unity Connection Server](#)” procedure on page 30-3.

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 “[Steps to Restart the Connection IMAP Server Service](#)” procedure on page 30-5.

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

8. Restart the Connection Jetty service so that the Connection Jetty and comet notification client use new SSL certificates. Do the “[Steps to Restart the Connection Jetty Service](#)” procedure on [page 30-5](#).

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



**Note** You need to restart the Connection Jetty service, if comet notification over SSL mode is enabled.

9. To prevent users from seeing a security alert whenever they access Unity Connection using Connection Administration, the 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.

### Steps 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**.

### Steps to Upload the Issuer and Server Certificates to the 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 issuer 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 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 “[Steps to Export the Issuer Certificate and to Issue the Server Certificate](#)” procedure on page 30-5.

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. 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 issuer 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 “[Steps to Export the Issuer Certificate and to Issue the Server Certificate](#)” procedure on page 30-5.

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 using an SSH application.
- b. Run the following CLI command to restart the Tomcat service:

```
utils service restart Cisco Tomcat
```

---

**Steps to Restart the 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 **Connection IMAP Server** service, select **Stop**.
  - Step 4** When the **Status** area displays a message that the **Connection IMAP Server** service was successfully stopped, select **Start** for the service.
- 

---

**Steps to Restart the Connection Jetty 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 **Connection Jetty** service, select **Stop**.
  - Step 4** When the **Status** area displays a message that the **Connection Jetty** service was successfully stopped, select **Start** for the service.
- 

## Exporting Issuer Certificate and Issuing the Server Certificate (Microsoft Certificate Services Only)

---

**Steps to Export the Issuer Certificate and to Issue the Server Certificate**

---

- Step 1** On the server on which you installed Microsoft Certificate Services, sign in to Windows 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.
- Step 4** Export the issuer 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 30-3, 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**.

---