Using SSL to Secure Client/Server Connections

Using SSL to Secure Client/Server Connections

Introduction

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.

Related Documentation

This chapter contains several instances where a user needs to create, generate, download and upload the Certificate Signing Request (CSR) using Multi-Server certificates or Single-Server Certificate. For more information see the chapter 'Security' of *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 15* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/os_administration/guide/b_15cucosagx.html .

Deciding the Installation of a SSL Certificate to Secure Cisco PCA, Unity Connection SRSV, and IMAP Email Client Access to Unity Connection

When you install 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.

For information on managing security alerts, see the "Managing Security Alerts Using Self-Signed Certificates with SSL Connections" section in "Setting Up Access to the Cisco Personal Communications Assistant" chapter of *User Workstation Setup Guide for Cisco Unity Connection Release 15* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/user_setup/guide/b_15cucuwsx.html.

For more information on self-signed certificate, refer to the "Security in Cisco Unity Connection Survivable Remote Site Voicemail" chapter of *Complete Reference Guide for Cisco Unity Connection Survivable Remote Site Voicemail (SRSV), Release 15* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/srsv/guide/b_15cucsrsvx.html.

Securing Connection Administration, Cisco PCA, Unity Connection SRSV, and IMAP Email Client Access to 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.
2. If you are using another application to issue certificates, install the application. See the manufacturer documentation for installation instructions. Then skip to Task 3.

   If you are using an external certification authority to issue certificates, skip to Task 3.

Note If you already have installed Microsoft Certificate Services or another application that can create certificate signing requests, skip to Task 3.

3. If a Unity Connection cluster is configured, run the `set web-security` CLI command or generate a Multi-server SAN certificate (for SIP integration only) for both Unity Connection servers in the cluster and assign both servers the same alternate name. The alternate name is 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 https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.
4. If a Unity Connection cluster is configured, configure a DNS A record that contains the alternate name that you assigned in Task 3. 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 using the same Unity Connection server name.
5. 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.

If a Unity Connection cluster is configured with Single-server certificate signing request, do this task for both servers in the Unity Connection cluster.

6. If you are using Microsoft Certificate Services to export the root certificate and to issue the server certificate, see

   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 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 using freely available utilities like OpenSSL.

   If a Unity Connection cluster is configured with Single-server certificate signing request, do this task for both servers in the Unity Connection cluster

7. Upload the root certificate and the server certificate to the Unity Connection server.

   If a Unity Connection cluster is configured with Single-server certificate signing request, 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 Restarting the Connection IMAP Server Service.

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

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

   Import the server certificate that you uploaded to the Unity Connection server in Task 7 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 7 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.

Restarting the 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.

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 https://www.cisco.com/c/en/us/support/conferencing/unified-meetingplace/products-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:
4. 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.

   - 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 using freely available utilities like OpenSSL.
   - The root certificate filename must not contain any spaces.

Securing Communication between Unity Connection and Cisco Unity Gateway Servers

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 Unity Connection when networking is configured on 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 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 is automatically 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/c/en/us/support/unified-communications/unity-connection/products-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 using the same Unity Connection server name.

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

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

4. 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)".

   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 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).

5. Upload the root certificate and the server certificate to the Unity Connection server.

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

6. Restart the Unity Connection IMAP Server service so that Unity Connection and the IMAP email clients use the new SSL certificates. Do the "Restarting the IMAP Server Service".

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

7. Upload the root certificate and the server certificate to the Cisco Unity server.

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

Creating and Downloading 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 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.

Restarting 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.

Uploading the Root and Server Certificate 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 2008)

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.

Step 1 Open Server Manager, click Add Roles, click Next, and click Active Directory Certificate Services. Click Next two times.

Step 2 On the Select Role Services page, click Certification Authority. Click Next.

Step 3 On the Specify Setup Type page, click Standalone or Enterprise. Click Next.

Note You must have a network connection to a domain controller in order to install an enterprise CA.

Step 4 On the Specify CA Type page, click Root CA. Click Next.

Step 5 On the Set Up Private Key page, click Create a new private key. Click Next.

Step 6 On the Configure Cryptography page, select a cryptographic service provider, key length, and hash algorithm. Click Next.

Step 7 On the Configure CA Name page, create a unique name to identify the CA. Click Next.

Step 8 On the Set Validity Period page, specify the number of years or months that the root CA certificate is valid. Click Next.

Step 9 On the Configure Certificate Database page, accept the default locations unless you want to specify a custom location for the certificate database and certificate database log. Click Next.

Step 10 On the Confirm Installation Options page, review all of the configuration settings that you have selected. If you want to accept all of these options, click Install and wait until the setup process has finished.

Step 11 Right click the Active Directory Certificate Authority. Select Add Role Services and select the check box for Certificate Authority Web Enrollment, Online Responder, Network Device Enrollment Service and install these services.

Step 12 Go to Server Manager -> Add Role -> Next-> check the Web Server (IIS) box and install it.

Step 13 Right click the Web Server (IIS). Select Add Role Services and check all the role services and install them.

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

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 in the Installing Microsoft Certificate Services (Windows Server 2008).

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 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 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 need it in a later procedure.

k) Select **OK**.

Step 6 Close Certification Authority.