Manage Certificates

Install Certificate Authority (CA) Certificate

To install or upload certificates on the Cisco Unified Intelligence Center server, perform the following steps:

Procedure

Step 1	Log in to Cisco Unified Operating System Administration.
Step 2	Navigate to **Security** > **Certificate Management**. The **Certificate List** window appears.
Step 3	Click **Generate CSR**. The **Generate Certificate Signing Request** dialog box opens.
Step 4	Select **tomcat** from the Certificate Purpose list.
Step 5	Click **Generate** to generate a certificate from a custom or third-party certificate authority.
Step 6	Click **Close**.
Step 7	Click **Download CSR**.
Step 8	In the **Download Certificate Signing Request** screen, click **Download CSR** to download the Certificate Signing Request to your computer.
Step 9	Use this CSR to obtain the Public certificate and Primary certificate from the Certificate Authority.
Step 10	Log in to OS platform again and navigate to **Security** > **Certificate Management**.
Step 11	Click **Upload Certificate/Certificate chain**. The **Upload Certificate/Certificate chain** dialog box opens.
Step 12	To upload the certificate chain, select **tomcat** from the **Certificate Purpose** list.
Step 13	Select the file to upload. Click the **Choose File** button and navigate to the file; then, click **Open**.
Step 14	Click **Upload**.
Step 15	After successfully uploading the certificate, navigate to **Security** > **Certificate Management**.
Step 16	Click **Find** to open the list of certificates.
Step 17	Click on the uploaded certificate to view **Certificate File Data**.
Step 18	Restart the node(s) using the CLI command *utils system restart*.

Note

- To upload a custom certificate with alternate hostname, set the alternate hostname using the CLI command *set web-security*. Configure the alternate hostname and use the procedure above to generate Certificate Signing Request (CSR) and to upload the certificates. You can access Cisco Unified Intelligence Center by using the alternate hostname as well.
- To avoid the certificate exception warning, you must access the servers using the Fully qualified domain name (FQDN) name. That is, leave the **Distribution** field in the CSR as the FQDN of the server.
- Ensure that the Certificate Authority (CA) certificate is RSA-signed.
- Cisco Unified Intelligence Center CSR certificates are signed with *sha1WithRSAEncryption* using a 2048-bit RSA public key.
- Cisco Unified Intelligence Center does not support wildcard certificates.

CUIC Server Certificates

Two server certificates — *intelligencecenter-jms* and *intelligencecenter-srvr*, even though available, are not used anymore. There is no impact even if these certificates expire, and it is not required to regenerate them.

Access Platform Web Applications using Chrome Browser

This section is applicable only if you are using Chrome based browsers (Google Chrome or Edge Chromium) to access the Platform web applications, such as Cisco Unified OS Administration, Cisco Unified Serviceability or Disaster Recovery System.

This section is also applicable for Cisco Unified Intelligence Center Administration web application on CUIC nodes.

If you are using self-signed certificates, add the certificates to the Client OS trust store to access the administrative web applications.

Note Chrome needs the self-signed certificate to have **Subject Alternative Name** extension to load the administrative web applications. If the self-signed certificate does not have **Subject Alternative Name**, regenerate the certificate from Cisco Unified OS Administration.

Download the Server Certificate from CUIC Node

This section provides instructions to download the server certificate from CUIC node.

Before you begin

Run the *show server tls cert_type* command on your server and identify the certificate type that your server uses. For more information see show tls server cert_type

Procedure

Step 1 Log in to the **Cisco Unified OS Administration** page using the URL: *https://<FQDN>:8443/cmplatform*

Step 2 Go to **Security** and select **Certificate Management**.
The **Certificate List** screen appears.

Step 3 In **Find Certificate List where** do the following:

a) Select **Common Name** in the first dropdown.
b) Select **begins with** in the second dropdown.
c) Enter the host name of the node in the search box.
d) Click **Find**.
The list of **Certificates** is displayed with their **Common Name** and **Key Type**. For ECDSA, the **Key Type** is **EC** and for RSA, the **Key Type** is **RSA**.

Step 4 Based on the certificate type required for your server, click the **Common Name** link of the **tomcat-trust** certificate in the search result.

Step 5 In the new window, click **Download .DER File** or **Download .PEM File** and save it.

Add Certificate to Trusted Root Certification Authorities on Windows Client System

To add the certificate to the Trusted Root Certification Authorities on Windows Client system, do the following:

Procedure

Step 1 In the **Control Panel** search for **Manage User Certificates** and click **Manage User Certificates**.
The **certmgr - [Certificates - Current User]** window appears.

Step 2 Select **Certificates - Current User** > **Trusted Root Certification Authorities** > **Certificates**.

Step 3 Right-click **Certificates** and click **All Tasks** > **Import** and then click **Next**.

Step 4 Browse and select the downloaded certificate file, click **Next** and then click **Finish**.

Step 5 In the **Security Warning** window, click **Yes**.

A window pops up to confirm that the import was successful.

Close the **Manage User Certificates** window and close all browser sessions.

Reopen the Chrome browser and clear the browser cache. Log in to the platform web application.

For example: *https://<FQDN>:8443/cmplatform*. The Chrome browser now shows the lock symbol to indicate that it is a trusted connection.

Add Certificate to Keychain Access in Mac Client Machine

This section is applicable for Mac OS Catalina version 10.15 and above. To add the certificate to Keychain Access in Mac Client machine, do the following:

Procedure

Step 1 On the Mac client machine, under **Applications** > **Utilities** select **Keychain Access**.

Step 2 In the left pane, select **System** and from the center pane, select the **Certificates** tab.

Step 3 Drag and drop the downloaded certificate on to the list of displayed certificates. (Provide the credentials for authentication, if prompted.)

Step 4 Double-click the newly imported certificate and click the expand icon beside **Trust**.

Step 5 In **When using this certificate** dropdown, select **Always trust** and close the window.