Manage Certificates

- Install Certificate Authority (CA) Certificate, on page 1

Install Certificate Authority (CA) Certificate

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. Do not change it to "Multi-server (SAN)" as Multi-Server SAN Certificates are not supported with Cisco Unified Intelligence Center.
- 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.