Configure Certificates

Certificates Overview

Certificates are used to secure identities and to build a trust relationship between the IM and Presence Service and another system. You can use certificates to connect the IM and Presence Service to Cisco Unified Communications Manager, to Cisco Jabber clients, or to any external server. Without certificates, it would be impossible to know if a rogue DNS server was used, or if you were routed to another server.

There are two main classes of certificates that the IM and Presence Service can use:

- Self-signed Certificates—Self signed certificates are signed by the same server that issues the certificate. Within an enterprise, you may use self-signed certificates to connect with another internal system, provided none of those connections are travelling over an unsecure network. For example, the IM and Presence Service might generate self-signed certificates for an internal connection to Cisco Unified Communications Manager.
- CA-signed Certificates—These are certificates that are signed by a third-party Certificate Authority (CA). These can be signed by a public CA (such as Verisign, Entrust or Digicert) or a server (like Windows 2003, Linux, Unix, IOS) that controls the validity of the server/service certificate. CA-signed certificates are more secure than self-signed certificates and are typically used for any WAN connections. For example, a Federation connection with another enterprise or an intercluster peer configuration that uses WAN connections would require CA-signed certificates to build a trust relationship with the external system.

CA-signed certificates are more secure than self-signed certificates. In general, self-signed certificates are considered fine for internal connections, but for any WAN connections or connections that go across the public internet, you should use CA-signed certificates.

Multi-Server Certificates

The IM and Presence Service also supports multi-server SAN certificates for some system services. When you generate a Certificate Signing Request (CSR) for a multi-server certificate, the resulting multi-server certificate and its associated chain of signing certificates are distributed automatically to all cluster nodes once the certificate is uploaded to any cluster node.

Certificate Types in the IM and Presence Service

Within the IM and Presence Service, the different system components require different types of certificates. The following table describes the different certificates that are required for clients and services on the IM and Presence Service.

Note If the certificate name ends in -ECDSA, then the certificate/key type is Elliptic Curve (EC). Otherwise, it is RSA.

Table 1: Certificate Types and Services

Certificate Type	Service	Certificate Trust Store	Multi-Server Support	Notes
tomcat, tomcat-ECDSA	Cisco Client Profile Agent, Cisco AXL Web Service, Cisco Tomcat	tomcat- trust	Yes	Presented to a Cisco Jabber client as part of client authentication for IM and Presence Service. Presented to a web browser when navigating the Cisco Unified CM IM and Presence Administration user interface. The associated trust-store is used to verify connections made by IM and Presence Service for the purposes of authenticating user credentials with a configured LDAP server.
ipsec		ipsec-trust	No	Used when an IPSec policy is enabled.
cup, cup-ECDSA	Cisco SIP Proxy, Cisco Presence Engine	cup-trust	No	Presents the certificate to Expressway-C to get IM and Presence for SIP federated users. The IM and Presence proxy acts as both client and server. The Presence Engine uses these certificates for Exchange/Office 365 communication to get calendar presence. Presence Engine acts as a client only.

Certificate Type	Service	Certificate Trust Store	Multi-Server Support	Notes
cup-xmpp, cup-xmpp-ECDSA	Cisco XCP Connection Manager, Cisco XCP Web Connection Manager, Cisco XCP Directory service, Cisco XCP Router service	cup-xmpp-trust	Yes	Presented to a Cisco Jabber client, third-Party XMPP client, or a CAXL based application when the XMPP session is being created. The associated trust-store is used to verify connections made by Cisco XCP Directory service in performing LDAP search operations for third-party XMPP clients. The associated trust-store is used by the Cisco XCP Router service when establishing secure connections between IM and Presence Service servers if the Routing Communication Type is set to Router-to-Router.
cup-xmpp-s2s, cup-xmpp-s2s-ECDSA	Cisco XCP XMPP Federation Connection Manager	cup-xmpp-trust	Yes	Presented for XMPP interdomain federation when connecting to externally federated XMPP systems.

Certificates Prerequisites

Configure the following items on Cisco Unified Communications Manager:

- Configure a SIP trunk security profile for IM and Presence Service.
- Configure a SIP trunk for IM and Presence Service:
  - Associate the security profile with the SIP trunk.
  - Configure the SIP trunk with the subject Common Name (CN) of the IM and Presence Service certificate.

Certificate Exchange with Cisco Unified Communications Manager

Complete these tasks to exchange certificates with Cisco Unified Communications Manager.

Note The certificate exchange between Cisco Unified Communications Manager and the IM and Presence Service gets handled during the installation process automatically. However, complete these tasks if you need to complete the certificate exchange manually.

Procedure

	Command or Action	Purpose
Step 1	Import Cisco Unified Communications Manager Certificate to IM and Presence Service, on page 4	Import a certificate from Cisco Unified Communications Manager into the IM and Presence Service.
Step 2	Download Certificate from IM and Presence Service, on page 5	Download a certificate from the IM and Presence Service. The certificate will need to be imported into Cisco Unified Communications Manager.
Step 3	Import IM and Presence Certificate to Cisco Unified Communications Manager, on page 5	To complete the certificate exchange, import the IM and Presence Service certificate into the Callmanager-trust store of Cisco Unified Communications Manager.

Import Cisco Unified Communications Manager Certificate to IM and Presence Service

Use this procedure to import a certificate from Cisco Unified Communications Manager into the IM and Presence Service.

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **System** > **Security** > **Certificate Import Tool**.

Step 2 Choose **IM and Presence (IM/P) Service Trust** from the **Certificate Trust Store** menu.

Step 3 Enter the IP address, hostname or FQDN of the Cisco Unified Communications Manager node.

Step 4 Enter a port number to communicate with the Cisco Unified Communications Manager node.

Step 5 Click **Submit**.

Note After the Certificate Import Tool completes the import operation, it reports whether or not it successfully connected to Cisco Unified Communications Manager, and whether or not it successfully downloaded the certificate from Cisco Unified Communications Manager. If the Certificate Import Tool reports a failure, see the Online Help for a recommended action. You can also manually import the certificate by choosing **Cisco Unified IM and Presence OS Administration** > **Security** > **Certificate Management**.

Note Depending on the negotiated TLS cipher, the Certificate Import Tool will download either an RSA-based certificate or an ECDSA-based certificate.

Step 6 Restart the Cisco SIP Proxy service:

a) From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Feature Services** on IM and Presence Service.

b) From the **Server** drop-down list box, select an IM and Presence Service cluster node and click **Go**.

c) Choose **Cisco SIP Proxy** and click **Restart**.

What to do next

Download Certificate from IM and Presence Service, on page 5

Download Certificate from IM and Presence Service

Use this procedure to download a certificate from the IM and Presence Service. The certificate will need to be imported into Cisco Unified Communications Manager.

Procedure

Step 1 From **Cisco Unified IM and Presence OS Administration**, choose **Security** > **Certificate Management** on IM and Presence Service.

Step 2 Click **Find**.

Step 3 Choose the `cup.pem` file.

Note `cup-ECDSA.pem` is also an available option.

Step 4 Click **Download** and save the file to your local computer.

Tip Ignore any errors that IM and Presence Service displays regarding access to the cup.csr file; The CA (Certificate Authority) does not need to sign the certificate that you exchange with Cisco Unified Communications Manager.

What to do next

Import IM and Presence Certificate to Cisco Unified Communications Manager, on page 5

Import IM and Presence Certificate to Cisco Unified Communications Manager

To complete the certificate exchange, import the IM and Presence Service certificate into the Callmanager-trust store of Cisco Unified Communications Manager.

Before you begin

Download Certificate from IM and Presence Service, on page 5

Procedure

Step 1 Log into Cisco Unified OS Administration.

Step 2 Choose **Security** > **Certificate Management**

Step 3 Click **Upload Certificate**.

Step 4 From the Certificate Name menu, choose **Callmanager-trust**.

Step 5 **Browse** and select the certificate that you downloaded previously from the IM and Presence Service.

Step 6 Click **Upload File**.

Step 7 Restart the Cisco CallManager service:

a) From Cisco Unified Serviceability, choose **Tools** > **Control Center - Feature Services**.

b) From the **Server** drop-down list box, select a Cisco Unified Communications Manager node and click **Go**.

c) Select the **Cisco CallManager** service and click **Restart**.

Install Certificate Authority (CA) on IM and Presence Service

In order to use certificates signed by a third-party Certificate Authority (CA) in the IM and Presence Service, you must first install that CA's root certificate chain of trust on the IM and Presence Service.

Procedure

	Command or Action	Purpose
Step 1	Upload CA Root Certificate Chain, on page 6	Use this procedure to upload the CA root certificate chain from the third-party Certificate Authority to the IM and Presence Service.
Step 2	Restart Cisco Intercluster Sync Agent Service, on page 7	After you have uploaded certificates, restart the Cisco Intercluster Sync Agent service.
Step 3	Verify CA Certificates Have Synchronized to Other Clusters, on page 7	Verify that your CA certificate chain has replicated to all peer clusters.

Upload CA Root Certificate Chain

Use this procedure to upload the certificate chain from the signing Certificate Authority (CA) to the IM and Presence database publisher node. The chain may consist of multiple certificates in a chain, with each certificate signing the subsequent certificate:

- Root Certificate > Intermediate 1 Certificate > Intermediate 2 Certificate

Procedure

Step 1 On the IM and Presence database publisher node, log in to Cisco Unified IM and Presence OS Administration.

Step 2 Choose **Security** > **Certificate Management**.

Step 3 Click **Upload Certificate/Certificate chain**.

Step 4 From the **Certificate Name** drop-down list, choose one of the following:

- If you are uploading a CA-signed tomact certificate, choose **tomcat-trust**

- If you are uploading a CA-signed cup-xmpp certificate or a CA signed cup-xmpp-s2s, choose **cup-xmpp-trust**

Step 5 Enter a **Description** for the signed certificate.

Step 6 Click **Browse** to locate the file for the Root Certificate.

Step 7 Click **Click Upload File**.

Step 8 Upload each intermediate certificate in the same way using the **Upload Certificate/Certificate chain** window. For each intermediate certificate, you must enter the name of the preceding certificate in the chain.

What to do next

Restart Cisco Intercluster Sync Agent Service, on page 7

Restart Cisco Intercluster Sync Agent Service

After you upload the Root and Intermediate certificates to the IM and Presence database publisher node, you must restart the Cisco Intercluster Sync Agent service on that node. This restart ensures that the CA certificates are synced immediately to all other clusters.

Procedure

Step 1 From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Network Services**.

Step 2 From the **Server** drop-down list box, select the IM and Presence Service node on which you imported the certificate and click **Go**.

Note You can also restart the Cisco Intercluster Sync Agent service from the Command Line Interface with the `utils service restart Cisco Intercluster Sync Agent` command.

Step 3 Select the **Cisco Intercluster Sync Agent** service and click **Restart**.

What to do next

Verify Intercluster Syncing, on page 10

Verify CA Certificates Have Synchronized to Other Clusters

After the Cisco Intercluster Sync Agent service has restarted, you must ensure that the CA certificate(s) have been correctly synchronized to other clusters. Complete the following procedure on each of the other IM and Presence database publisher nodes.

Note The information in the following procedure also applies to certificates ending in `-ECDSA`.

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **Diagnostics** > **System Troubleshooter**.

Step 2 Under **Inter-clustering Troubleshooter**, find the test **Verify that each TLS-enabled inter-cluster peer has successfully exchanged security certificates** and verify that is has passed.

Step 3 If the test shows an error, note the intercluster peer IP address; it should reference the cluster on which you uploaded the CA certificate(s). Continue with the following steps to resolve the issue.

Step 4 Choose **Presence** > **Inter-Clustering** and click the link associated with the intercluster peer that was identified on the **System Troubleshooter** page.

Step 5 Click **Force Manual Sync**.

Step 6 Allow 60 seconds for the Inter-cluster Peer Status panel to auto-refresh.

Step 7 Verify that the **Certificate Status** field shows "Connection is secure".

Step 8 If the Certificate Status field does not show "Connection is secure", restart the Cisco Intercluster Sync Agent service on the IM and Presence database publisher node and then repeat steps 5 to 7.

- To restart the service from the admin CLI run the following command: utils service restart Cisco Intercluster Sync Agent
- Alternatively, you can restart this service from the Cisco Unified IM and Presence Serviceability GUI.

Step 9 Verify that the **Certificate Status** now shows "Connection is secure". This means that intercluster syncing is correctly established between the clusters and that the CA certificates that you uploaded are synced to the other clusters.

What to do next

Upload the signed certificate to each IM and Presence Service node.

Upload Certificates to IM and Presence Service

Complete these tasks to upload certificates to the IM and Presence Service. You can upload CA-signed certificates or self-signed certificates.

Before you begin

To use CA-signed certificates that are signed by a third-party Certificate Authority (CA), you must already have installed that CA's root certificate chain on the IM and Presence Service. For details, Install Certificate Authority (CA) on IM and Presence Service, on page 6.

Procedure

	Command or Action	Purpose
Step 1	Upload Certificates, on page 9	Upload signed certificates to the IM and Presence Service.
Step 2	Restart Cisco Tomcat Service, on page 10	(Tomcat certificates only). Restart the Cisco Tomcat Service.

	Command or Action	Purpose
Step 3	Verify Intercluster Syncing, on page 10	(Tomcat certificates only). After the Cisco Tomcat service has restarted for all affected nodes within the cluster, you must verify that intercluster syncing is operating correctly.
Step 4	Restart the Cisco XCP Router service on all nodes, on page 11	If you uploaded certificates to the cup-xmpp store, restart the Cisco XMP Router on all cluster nodes.
Step 5	Restart Cisco XCP XMPP Federation Connection Manager Service, on page 11	(XMPP Federation only). If you uploaded certificates to the cup-xmpp store for XMPP Federation, restart the Cisco XCPXMPP Federation Connection Manager Service.
Step 6	Enable Wildcards in XMPP Federation Security Certificates, on page 11	(XMPP Federation only). If you uploaded certificates to the cup-xmpp store for XMPP Federation over TLS, you must enable wildcards for XMPP security certificates. This is required for group chat.

Upload Certificates

Use this procedure to upload certificates to each IM and Presence Service node.

Note Cisco recommends that you sign all required tomcat certificates for a cluster and upload them at the same time. This process reduces the time to recover intercluster communications.

Note The information in the following procedure also applies to certificates ending in `-ECDSA`.

Before you begin

If the certificate is signed by a CA, you must have also installed that CA's root certificate chain or the CA-signed certificate will be untrusted. When the CA certificates have correctly synced to all clusters, you can upload the appropriate signed certificate to each IM and Presence Service node.

Procedure

Step 1 In **Cisco Unified IM and Presence OS Administration**, choose **Security** > **Certificate Management**.

Step 2 Click **Upload Certificate/Certificate chain**.

Step 3 Select the **Certificate Purpose**. For example, **tomcat**.

Step 4 Enter a Description for the signed certificate.

Step 5 Click **Browse** to locate the file to upload.

Step 6 Click **Upload File**.

Step 7 Repeat for each IM and Presence Service node.

What to do next

Restart the Cisco Tomcat service.

Restart Cisco Tomcat Service

After you upload tomcat certificates to each IM and Presence Service node, you must restart the Cisco Tomcat service on each node.

Procedure

Step 1 Log into the admin CLI.

Step 2 Run the following command: `utils service restart Cisco Tomcat.`

Step 3 Repeat for each node.

What to do next

Verify that intercluster syncing is operating correctly.

Verify Intercluster Syncing

After the Cisco Tomcat service has restarted for all affected nodes within the cluster, you must verify that intercluster syncing is operating correctly. Complete the following procedure on each IM and Presence database publisher node in the other clusters.

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **Diagnostics** > **System Troubleshooter**.

Step 2 Under **Inter-clustering Troubleshooter**, find the test **Verify that each TLS-enabled inter-cluster peer has successfully exchanged security certificates** test and verify that is has passed.

Step 3 If the test shows an error, note the intercluster peer IP address; it should reference the cluster on which you uploaded the CA certificate(s). Continue with the following steps to resolve the issue.

Step 4 Choose **Presence** > **Inter-Clustering** and click the link associated with the intercluster peer that was identified on the System Troubleshooter page.

Step 5 Click **Force Manual Sync**.

Step 6 Check the **Also resync peer's Tomcat certificates** checkbox and click **OK**.

Step 7 Allow 60 seconds for the Inter-cluster Peer Status panel to auto-refresh.

Step 8 Verify that the **Certificate Status** field shows "Connection is secure".

Step 9 If the **Certificate Status** field does not show "Connection is secure", restart the Cisco Intercluster Sync Agent service on the IM and Presence database publisher node and then repeat steps 5 to 8.

- To restart the service from the admin CLI run the following command: utils service restart Cisco Intercluster Sync Agent.
- Alternatively, you can restart this service from the Cisco Unified IM and Presence Serviceability GUI.

Step 10 Verify that the Certificate Status now shows "Connection is secure". This means that intercluster syncing is now re-established between this cluster and the cluster for which the certificates were uploaded.

Restart the Cisco XCP Router service on all nodes

After you upload a cup-xmpp and/or cup-xmpp-ECDSA certificate to each IM and Presence Service node, you must restart the Cisco XCP Router service on each node.

Note You can also restart the Cisco XCP Router service from the Cisco Unified IM and Presence Serviceability GUI.

Procedure

Step 1 Log into the admin CLI.

Step 2 Run the following command: utils service restart Cisco XCP Router.

Step 3 Repeat for each node.

Restart Cisco XCP XMPP Federation Connection Manager Service

After you upload the cup-xmpp-s2s and/or cup-xmpp-s2s-ECDSA certificate to each IM and Presence Service federation node, you must restart the Cisco XCP XMPP Federation Connection Manager service on each federation node.

Procedure

Step 1 Log into the admin CLI.

Step 2 Run the following command: utils service restart Cisco XCP XMPP Federation Connection Manager.

Step 3 Repeat for each federation node.

Enable Wildcards in XMPP Federation Security Certificates

To support group chat between XMPP federation partners over TLS, you must enable wildcards for XMPP security certificates.

By default, the XMPP federation security certificates `cup-xmpp-s2s` and `cup-xmpp-s2s-ECDSA` contains all domains hosted by the IM and Presence Service deployment. These are added as Subject Alternative Name (SAN) entries within the certificate. You must supply wildcards for all hosted domains within the same certificate. So instead of a SAN entry of "example.com", the XMPP security certificate must contain a SAN entry of "*.example.com". The wildcard is needed because the group chat server aliases are sub-domains of one of the hosted domains on the IM and Presence Service system. For example: "conference.example.com".

Note To view the `cup-xmpp-s2s` or `cup-xmpp-s2s-ECDSA` certificates on any node, choose **Cisco Unified IM and Presence OS Administration** > **Security** > **Certificate Management** and click on the **cup-xmpp-s2s** or **cup-xmpp-s2s-ECDSA** links.

Procedure

Step 1 Choose **System** > **Security Settings**.

Step 2 Check **Enable Wildcards in XMPP Federation Security Certificates**.

Step 3 Click **Save**.

What to do next

You must regenerate the XMPP federation security certificates on all nodes within the cluster where the Cisco XMPP Federation Connection Manager service is running and XMPP Federation is enabled. This security setting must be enabled on all IM and Presence Service clusters to support XMPP Federation Group Chat over TLS.

Generate a CSR

Use this procedure to generate a Certificate Signing Request (CSR). You will need the CSR to submit to the third-pary CA so that they can provide you with a CA-signed certificate.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Click the **Generate CSR** button. The **Generate Certificate Signing Request** popup displays.

Step 3 From the **Certificate Purpose** drop-down, select the type of certificate that you are generating.

Step 4 From the **Distribution** drop-down, select an IM and Presence server. For multi-server certificates, select **Multi-server (SAN)**.

Step 5 Enter the **Key Length** and **Hash Algorithm**.

Step 6 Complete any remaining fields and click **Generate**.

Step 7 Download the CSR to a local computer:

a) Click **Download CSR**.

b) Choose the certificate name from the **Certificate Purpose** drop-down list.

c) **Download CSR**

What to do next

Submit the CSR to the third-party Certificate Authority so that they can issue you a CA-signed certificate.

Certificate Signing Request Key Usage Extensions

The following tables display key usage extensions for Certificate Signing Requests (CSRs) for both Unified Communications Manager and the IM and Presence Service CA certificates.

Table 2: Cisco Unified Communications Manager CSR Key Usage Extensions

	Multi server	Extended Key Usage			Key Usage				
		Server Authentication (1.3.6.1.5.5.7.3.1)	Client Authentication (1.3.6.1.5.5.7.3.2)	IP security end system (1.3.6.1.5.5.7.3.5)	Digital Signature	Key Encipherment	Data Encipherment	Key Cert Sign	Key Agreement
CallManager CallManager-ECDSA	Y	Y	Y		Y	Y	Y		
CAPF (publisher only)	N	Y			Y	N		Y	
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		
TVS	N	Y	Y		Y	Y	Y		

Table 3: IM and Presence Service CSR Key Usage Extensions

	Multi server	Extended Key Usage			Key Usage				
		Server Authentication (1.3.6.1.5.5.7.3.1)	Client Authentication (1.3.6.1.5.5.7.3.2)	IP security end system (1.3.6.1.5.5.7.3.5)	Digital Signature	Key Encipherment	Data Encipherment	Key Cert Sign	Key Agreement
cup cup-ECDSA	N	Y	Y	Y	Y	Y	Y		
cup-xmpp cup-xmpp-ECDSA	Y	Y	Y	Y	Y	Y	Y		
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	Y	Y	Y	Y	Y	Y	Y		
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		

Note Ensure that 'Data Encipherment' bit is not changed or removed as part of the CA-signing certificate process.

Generate a Self-Signed Certificate

Use this procedure to generate a self-signed certificate.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.
Step 2 Click **Generate Self-Signed**. The **Generate New Self-Signed Certificate** popup displays.
Step 3 From the **Certificate Purpose** drop-down, select the type of certificate that you are generating.
Step 4 From the **Distribution** drop-down, enter the name of the server.
Step 5 Select the appropriate **Key Length**.
Step 6 From the **Hash Algorithm**, select the encryption algorithm. For example, SHA256.
Step 7 Click **Generate**.

Delete Self Signed Trust Certificates from IM and Presence Service

To support cross navigation for serviceability between nodes in the same cluster, the Cisco Tomcat service trust stores between the IM and Presence Service and Cisco Unified Communications Manager are synchronized automatically.

If you have replaced the original self-signed trust certificates with CA-signed certificates, the original self-signed trust certificates persist in the service trust store. You can use this procedure to delete the self-signed certificates on the IM and Presence Service and Cisco Unified Communications Manager nodes.

Before you begin

Important If you added CA-signed certificates, make sure that you have waited 30 minutes for the Cisco Intercluster Sync Agent Service to perform its periodic clean-up task on a given IM and Presence Service node.

Procedure

Step 1 From Cisco Unified IM and Presence Operating System Administration, choose**Security** > **Certificate Management**.
Step 2 Click **Find**.

The **Certificate List** appears.

Note The certificate name is composed of two parts, the service name and the certificate type. For example tomcat-trust where tomcat is the service and trust is the certificate type.

The self-signed trust certificates that you can delete are:

- Tomcat and Tomcat-ECDSA — tomcat-trust
- Cup-xmpp and Cup-xmpp-ECDSA — cup-xmpp-trust
- Cup-xmpp-s2s and Cup-xmpp-s2s-ECDSA — cup-xmpp-trust
- Cup and Cup-ECDSA — cup-trust
- Ipsec — ipsec-trust

Step 3 Click the link for the self-signed trust certificate you wish to delete.

Important Be certain that you have configured a CA-signed certificate for the service associated with the service trust store.

A new window appears that displays the certificate details.

Step 4 Click **Delete**.

Note The **Delete** button appears only if you have the authority to delete that certificate.

Step 5 Repeat the above procedure for each IM and Presence Service node in the cluster and on any intercluster peers to ensure complete removal of unnecessary self-signed trust certificates across the deployment.

What to do next

If the service is Tomcat, you must check for the IM and Presence Service node's self signed tomcat-trust certificate on the Cisco Unified Communications Manager node. See, Delete Self-Signed Tomcat-Trust Certificates from Cisco Unified Communications Manager, on page 15.

Delete Self-Signed Tomcat-Trust Certificates from Cisco Unified Communications Manager

There is a self-signed tomcat-trust certificate in the Cisco Unified Communications Manager service trust store for each node in the cluster. These are the only certificates that you delete from the Cisco Unified Communications Manager node.

Note The information in the following procedure also applies to `-EC` certificates.

Before you begin

Ensure that you have configured the cluster's IM and Presence Service nodes with CA-signed certificates, and you have waited for 30 minutes to allow the certificates to propagate to the Cisco Unified Communications Manager node.

Procedure

Step 1 In **Cisco Unified Operating System Administration**, choose **Security** > **Certificate Management**.

The **Certificate List** window appears.

Step 2 To filter the search results, choose **Certificate** and **begins with** from the drop-down lists and then enter tomcat-trust in the empty field. Click **Find**.

The **Certificate List** window expands with the tomcat-trust certificates listed.

Step 3 Identify the links that contain an IM and Presence Service node's hostname or FQDN in its name. These are self-signed certificates associated with this service and an IM and Presence Service node.

Step 4 Click the link to an IM and Presence Service node's self-signed tomcat-trust certificate.

A new window appears that shows the tomcat-trust certificate details.

Step 5 Confirm in the Certificate Details that this is a self-signed certificate by ensuring that the Issuer Name CN= and the Subject Name CN= values match.

Step 6 If you have confirmed that it is a self-signed certificate and you are certain that the CA-signed certificate has propagated to the Cisco Unified Communications Manager node, click **Delete**.

Note The **Delete** button only appears for certificates that you have the authority to delete.

Step 7 Repeat steps 4, 5, and 6 for each IM and Presence Service node in the cluster.

Certificate Monitoring Task Flow

Complete these tasks to configure the system to monitor certificate status and expiration automatically.

- Email you when certificates are approaching expiration.
- Revoke expired certificates.

Procedure

	Command or Action	Purpose
Step 1	Configure Certificate Monitor Notifications, on page 17	Configure automatic certificate monitoring. The system periodically checks certificate statuses and emails you when a certificate is approaching expiration.
Step 2	Configure Certificate Revocation via OCSP, on page 17	Configure the OCSP so that the system revokes expired certificates automatically.

Configure Certificate Monitor Notifications

Configure automated certificate monitoring for Unified Communications Manager or the IM and Presence Service. The system periodically checks the status of certificates and emails you when a certificate is approaching expiration.

Note The **Cisco Certificate Expiry Monitor** network service must be running. This service is enabled by default, but you can confirm the service is running in Cisco Unified Serviceability by choosing **Tools** > **Control Center - Network Services** and verifying that the **Cisco Certificate Expiry Monitor Service** status is **Running**.

Procedure

Step 1 Log in to Cisco Unified OS Administration (for Unified Communications Manager certificate monitoring) or Cisco Unified IM and Presence Administration (for IM and Presence Service certificate monitoring).

Step 2 Choose **Security** > **Certificate Monitor**.

Step 3 In the **Notification Start Time** field, enter a numeric value. This value represents the number of days before certificate expiration where the system starts to notify you of the upcoming expiration.

Step 4 In the **Notification Frequency** fields, enter the frequency of notifications.

Step 5 Optional. Check the **Enable E-mail notification** check box to have the system send email alerts of upcoming certificate expirations..

Step 6 Check the **Enable LSC Monitoring** check box to include LSC certificates in the certificate status checks.

Step 7 In the **E-mail IDs** field, enter the email addresses where you want the system to send notifications. You can enter multiple email addresses separated by a semicolon.

Step 8 Click **Save**.

Note The certificate monitor service runs once every 24 hours by default. When you restart the certificate monitor service, it starts the service and then calculates the next schedule to run only after 24 hours. The interval does not change even when the certificate is close to the expiry date of seven days. It runs every 1 hour when the certificate either has expired or is going to expire in one day.

What to do next

Configure the Online Certificate Status Protocol (OCSP) so that the system revokes expired certificates automatically. For details, seeConfigure Certificate Revocation via OCSP, on page 17

Configure Certificate Revocation via OCSP

Enable the Online Certificate Status Protocol (OCSP) to check certificate status regularly and to revoke expired certificates automatically.

Before you begin

Make sure that your system has the certificates that are required for OCSP checks. You can use Root or Intermediate CA certificates that are configured with the OCSP response attribute or you can use a designated OCSP signing certificate that has been uploaded to the tomcat-trust.

Procedure

Step 1 Log in to Cisco Unified OS Administration (for Unified Communications Manager certificate revocation) or Cisco Unified IM and Presence Administration (for IM and Presence Service certificate revocation).

Step 2 Choose **Security** > **Certificate Revocation**.

Step 3 Check the **Enable OCSP** check box, and perform one of the following tasks:

- If you want to specify an OCSP responder for OCSP checks, select the **Use configured OCSP URI** button and enter the URI of the responder in the **OCSP Configured URI** field.
- If the certificate is configured with an OCSP responder URI, select the **Use OCSP URI from Certificate** button.

Step 4 Check the **Enable Revocation Check** check box.

Step 5 Complete the **Check Every** field with the interval period for revocation checks.

Step 6 Click **Save**.

Step 7 Optional. If you have CTI, IPsec or LDAP links, you must also complete these steps in addition to the above steps to enable OCSP revocation support for those long-lived connections:

a) From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.
b) Under **Certificate Revocation and Expiry**, set the **Certificate Validity Check** parameter to **True**.
c) Configure a value for the **Validity Check Frequency** parameter.

Note The interval value of the **Enable Revocation Check** parameter in the **Certificate Revocation** window takes precedence over the value of the **Validity Check Frequency** enterprise parameter.

d) Click **Save**.