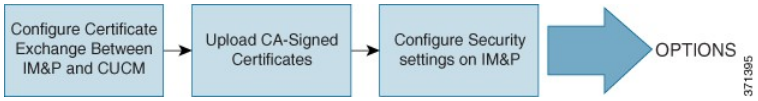
Security Configuration on IM and Presence Service

Security Setup Task List

The following workflow diagram shows the high-level steps to configure security on the IM and Presence Service node deployment.

Figure 1: Security Setup Workflow



The following table lists the tasks to perform to set up security on the IM and Presence Service node deployment. For detailed instructions, see the procedures that are related to the tasks outlined in the workflow.

Note Optionally, you can create a banner that users acknowledge as part of their login to any IM and Presence Service interface.

Table 1: Task List for Security Setup on IM and Presence Service

Task	Description
Configure Certificate Exchange Between IM and Presence Service and Cisco Unified Communications Manager	Perform the following tasks: • Import Cisco Unified Communications Manager certificate to IM and Presence Service node, and then restart the SIP proxy service. **Tip** You can import the certificate using either the Certificate Import Tool or manually using Cisco Unified IM and Presence OS Administration from **Security** > **Certificate Management**. • Download the certificate from IM and Presence Service, and then upload the certificate to Callmanager-trust on Cisco Unified Communications Manager. • Restart the Cisco Unified Communications Manager service. **Note** You must configure a SIP security profile and SIP trunk for IM and Presence Service before you can configure the certificate exchange between Cisco Unified Communications Manager and IM and Presence Service.
Upload CA-Signed Certificates	Upload the Certificate Authority (CA) signed certificates to IM and Presence Service for your deployment, which can be either a single-server or a multi-server deployment. Service restarts are required. See the related tasks for details. • tomcat certificate • cup-xmpp certificate • cup-xmpp-s2s certificate **Tip** You can upload these certificates on any IM and Presence Service node in the cluster. When this is done, the certificate and the associated signing certificates are automatically distributed to all the other IM and Presence Service nodes in the cluster.
Configure Security Settings on IM and Presence Service	When you import an IM and Presence Service certificate, IM and Presence Service automatically attempts to add the TLS peer subject to the TLS peer subject list, and to the TLS context list. Verify the TLS peer subject and TLS context configuration is set up to your requirements. IM and Presence Service provides increased security for XMPP-based configurations. You can configure the XMPP secure modes on IM and Presence Service using Cisco Unified CM IM and Presence Administration from **System** > **Security** > **Settings**.

Create Login Banner

You can create a banner that users acknowledge as part of their login to any IM and Presence Service interface. You create a .txt file using any text editor, include important notifications they want users to be made aware of, and upload it to the Cisco Unified IM and Presence OS Administration page. This banner will then appear on all IM and Presence Service interfaces notifying users of important information before they login, including

legal warnings and obligations. The following interfaces will display this banner before and after a user logs in: Cisco Unified CM IM and Presence Administration, Cisco Unified IM and Presence Operating System Administration, Cisco Unified IM and Presence Serviceability, Cisco Unified IM and Presence Reporting, and IM and Presence Disaster Recovery System.

Procedure

Step 1 Create a .txt file with the contents you want to display in the banner.

Step 2 Sign in to Cisco Unified IM and Presence Operating System Administration.

Step 3 Choose **Software Upgrades** > **Customized Logon Message**.

Step 4 Click **Browse** and locate the .txt file.

Step 5 Click **Upload File**.

The banner will appear before and after login on most IM and Presence Service interfaces.

Note The .txt file must be uploaded to each IM and Presence Service node separately.

Multi-Server Certificate Overview

IM and Presence Service supports multi-server SAN based certificates for the certificate purposes of tomcat, cup-xmpp, and cup-xmpp-s2s. You can select between a single-server or multi-server distribution to generate a Certificate Signing Request (CSR) for the certificate purposes which support multi-server certificates. The resulting signed multi-server certificate and its associated chain of signing certificates are automatically distributed to the other servers in the cluster on upload of the multi-server certificate to any of the individual servers in the cluster. For more information on multi-server certificates, see the New and Changed Features chapter of the *Release Notes for Cisco Unified Communications Manager, Release 10.5(1)*.

IM and Presence Service Certificate Types

This section describes the different certificates required for the clients and services on IM and Presence Service.

Table 2: Certificate Types and Services

Certificate Type	Service	Certificate Trust Store	Multi-Server Support	Notes
tomcat	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	Cisco SIP Proxy Cisco Presence Engine	cup-trust	No	

Certificate Type	Service	Certificate Trust Store	Multi-Server Support	Notes
cup-xmpp	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	Cisco XCP XMPP Federation Connection Manager	cup-xmpp-trust	Yes	Presented for XMPP interdomain federation when connecting to externally federated XMPP systems.

Related Topics

XMPP Security Settings Configuration on IM and Presence Service, on page 22
Configure Secure Connection Between IM and Presence Service and LDAP Directory

Certificate Exchange Configuration Between IM and Presence Service and Cisco Unified Communications Manager

This module describes the exchange of self-signed certificates between the Cisco Unified Communications Manager node and the IM and Presence Service node. You can use the Certificate Import Tool on IM and Presence Service to automatically import the Cisco Unified Communications Manager certificate to IM and Presence Service. However, you must manually upload the IM and Presence Service certificate to Cisco Unified Communications Manager.

Only perform these procedures if you require a secure connection between IM and Presence Service and Cisco Unified Communications Manager.

Prerequisites for Configuring Security

Configure the following items on Cisco Unified Communications Manager:

- Configure a SIP 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.

Related Topics

SIP Trunk Configuration on Cisco Unified Communications Manager

Import Cisco Unified Communications Manager Certificate to IM and Presence Service

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **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**.

What to do next

Proceed to restart the SIP proxy service.

Restart SIP Proxy Service

Before you begin

Import the Cisco Unified Communications Manager certificate to IM and Presence Service.

Procedure

Step 1 Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services** on IM and Presence Service,

Step 2 Choose **Cisco SIP Proxy**.

Step 3 Click **Restart**.

What to do next

Proceed to download the certificate from IM and Presence Service.

Download Certificate from IM and Presence Service

Procedure

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

Step 2 Click **Find**.

Step 3 Choose the **cup.pem** file.

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

Proceed to upload the IM and Presence Service certificate to Cisco Unified Communications Manager.

Upload IM and Presence Service Certificate to Cisco Unified Communications Manager

Before you begin

Download the certificate from IM and Presence Service.

Procedure

Step 1 Choose **Cisco Unified OS Administration** > **Security** > **Certificate Management** on Cisco Unified Communications Manager.

Step 2 Click **Upload Certificate**.

Step 3 Choose **Callmanager-trust** from the Certificate Name menu.

Step 4 Browse and choose the certificate (.pem file) previously downloaded from IM and Presence Service.

Step 5 Click **Upload File**.

What to do next

Proceed to restart the Cisco Unified Communications Manager CallManager service.

Restart Cisco Unified Communications Manager Service

Before you begin

Upload the IM and Presence Service certificate to Cisco Unified Communications Manager.

Procedure

Step 1 Choose **Cisco Unified Serviceability** > **Tools** > **Control Center - Feature Services** on Cisco Unified Communications Manager.

Step 2 Choose **Cisco CallManager**.

Step 3 Click **Restart**.

What to do next

Proceed to configure SIP security settings on IM and Presence Service.

Related Topics

SIP Security Settings Configuration on IM and Presence Service, on page 21

Multi-Server CA Signed Certificate Upload to IM and Presence Service

This section gives further information on uploading the following types of multi-server CA signed certificates:

- tomcat certificate
- cup-xmpp certificate
- cup-xmpp-s2s certificate

You can upload such certificates on any IM and Presence Service node in the cluster. When this is done the certificate and the associated signing certificates are automatically distributed to all the other IM and Presence Service nodes in the cluster. If a self-signed certificate already exists on any node, for the given certificate purpose (for example, tomcat, cup-xmpp, or cup-xmpp-s2s), it will be overwritten by the new multi-server certificate.

The IM and Presence Service nodes to which a given multi-server certificate and the associated signing certificates are distributed is dependent on the certificate purpose. The cup-xmpp and cup-xmpp-s2s multi-server certificates are distributed to all IM and Presence Service nodes in the cluster. The tomcat multi-server certificate is distributed to all IM and Presence Service nodes in the cluster and to all Cisco Unified Communications Manager nodes in the cluster. For more information on multi-server SAN certificates, see the New and Changed Features chapter of the *Release Notes for Cisco Unified Communications Manager, Release 10.5(1)*.

Single-Server CA Signed Certificate Upload to IM and Presence Service

This section describes how to upload the following types of CA signed certificates to an IM and Presence Service deployment:

- tomcat certificate
- cup-xmpp certificate
- cup-xmpp-s2s certificate

CA-Signed Tomcat Certificate Task List

The high-level steps to upload a CA signed Tomcat certificate to IM and Presence Service are:

1. Upload the Root Certificate and Intermediate Certificate of the signing Certificate Authority to IM and Presence Service.
2. Restart the Cisco Intercluster Sync Agent service.
3. Ensure that the CA certificates have been correctly synced to other clusters.

4. Upload the appropriate signed certificate to each IM and Presence Service node.
5. Restart the Cisco Tomcat service on all nodes.
6. Ensure that intercluster syncing is operating correctly.

Upload Root Certificate and Intermediate Certificate of the Signing Certificate Authority

When you upload the Root and Intermediate Certificates, you must upload each certificate in the certificate chain to IM and Presence Service from the Root Certificate down to the last Intermediate Certificate, as follows:

root > intermediate-1 > intermediate-2 > … > intermediate-N

With each certificate that you upload in the chain, you must specify which previously uploaded certificate signed it. For example:

- For intermediate-1, the root cert was used to sign it.
- For intermediate-2, the intermediate-1 cert was used to sign it.

You must upload the Root Certificate and the Intermediate Certificates, if any, to the trust store of the related leaf certificate on the IM and Presence database publisher node. Complete the following procedure to upload the Root Certificate and the Intermediate Certificate of the signing Certificate Authority (CA) to the IM and Presence Service deployment.

Procedure

Step 1 On the IM and Presence database publisher node, choose **Cisco Unified IM and Presence OS Administration** > **Security** > **Certificate Management**.

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

Step 3 From the Certificate Name drop-down list, choose **tomcat-trust**.

Step 4 Enter a description for the signed certificate.

Step 5 Click **Browse** to locate the file for the Root Certificate.

Step 6 Click **Upload File**.

Step 7 Upload each Intermediate Certificate in the same way using the **Upload Certificate/Certificate chain** window.

What to do next

Restart the Cisco Intercluster Sync Agent service.

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 service restart ensures that the CA certificates are synced immediately to all other clusters.

Procedure

Step 1 Log into the Admin CLI.

Step 2 Run the following command: **utils service restart Cisco Intercluster Sync Agent**

Note You can also restart the Cisco Intercluster Sync Agent service from the Cisco Unified Serviceability GUI.

What to do next

Verify that the CA certificates have synced to the other clusters.

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.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **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 Signed Certificate to Each IM and Presence Service Node

When the CA certificates have correctly synced to all clusters, you can upload the appropriate signed certificate 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.

Procedure

Step 1 Choose **Cisco Unified IM and Presence OS Administration** > **Security** > **Certificate Management**.

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

Step 3 From the Certificate Name drop-down list, choose **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.

For more information about certificate management, see the *Cisco Unified Communications Operating System Administration Guide*.

What to do next

Restart the Cisco Tomcat service.

Restart Cisco Tomcat Service

After you upload the tomcat certificate 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 Choose **Cisco Unified CM IM and Presence Administration** > **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.

CA-Signed cup-xmpp Certificate Upload

The high-level steps to upload a CA signed cup-xmpp certificate to IM and Presence Service are:

1. Upload the Root Certificate and Intermediate Certificate of the signing Certificate Authority to IM and Presence Service.
2. Restart the Cisco Intercluster Sync Agent service.
3. Ensure that the CA certificates have been correctly synced to other clusters.
4. Upload the appropriate signed certificate to each IM and Presence Service node.
5. Restart the Cisco XCP Router service on all nodes.

Upload Root Certificate and Intermediate Certificate of the Signing Certificate Authority

When you upload the Root and Intermediate Certificates, you must upload each certificate in the certificate chain to IM and Presence Service from the Root Certificate down to the last Intermediate Certificate, as follows:

root > intermediate-1 > intermediate-2 > … > intermediate-N

With each certificate that you upload in the chain, you must specify which previously uploaded certificate signed it. For example:

- For intermediate-1, the root cert was used to sign it.
- For intermediate-2, the intermediate-1 cert was used to sign it.

You must upload the Root Certificate and the Intermediate Certificates, if any, to the **cup-xmpp-trust** store on the IM and Presence database publisher node. Complete the following procedure to upload the Root Certificate and the Intermediate Certificate of the signing Certificate Authority (CA) to the IM and Presence Service deployment.

Procedure

Step 1 On the IM and Presence database publisher node, choose **Cisco Unified IM and Presence OS Administration** > **Security** > **Certificate Management**.

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

Step 3 From the Certificate Name drop-down list, choose **cup-xmpp-trust**.

Step 4 Enter a description for the signed certificate.

Step 5 Click **Browse** to locate the file for the Root Certificate.

Step 6 Click **Upload File**.

Step 7 Upload each Intermediate Certificate in the same way using the **Upload Certificate/Certificate chain** window.

What to do next

Restart the Cisco Intercluster Sync Agent service.

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 service restart ensures that the CA certificates are synced immediately to all other clusters.

Procedure

Step 1 Log into the Admin CLI.

Step 2 Run the following command: `utils service restart Cisco Intercluster Sync Agent`

Note You can also restart the Cisco Intercluster Sync Agent service from the Cisco Unified Serviceability GUI.

What to do next

Verify that the CA certificates have synced to the other clusters.

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.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **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 Signed Certificate to Each IM and Presence Service Node

When the CA certificates have correctly synced to all clusters, you can upload the appropriate signed cup-xmpp certificate to each IM and Presence Service node.

Note Cisco recommends that you sign all required cup-xmpp certificates for a cluster and upload them at the same time so that service impacts can be managed within a single maintenance window.

Procedure

Step 1 Choose **Cisco Unified IM and Presence OS Administration** > **Security** > **Certificate Management**.
Step 2 Click **Upload Certificate/Certificate chain**.
Step 3 From the Certificate Name drop-down list, choose **cup-xmpp**.
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.

For more information about certificate management, see the *Cisco Unified Communications Operating System Administration Guide* .

What to do next

Restart the Cisco XCP Router service on all nodes.

Restart Cisco XCP Router Service On All Nodes

Caution A restart of the Cisco XCP Router affects service.

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

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.

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

CA-Signed cup-xmpp-s2s Certificate Upload

The high-level steps to upload a CA signed cup-xmpp-s2s certificate to IM and Presence Service are:

1. Upload the Root Certificate and Intermediate Certificate of the signing Certificate Authority to IM and Presence Service.
2. Ensure that the CA certificates have been correctly synced to other clusters.

3. Upload the appropriate signed certificate to IM and Presence Service federation nodes (this certificate is not required on all IM and Presence Service nodes, only those used for federation).
4. Restart the Cisco XCP XMPP Federation Connection Manager service on all affected nodes.

Upload Root Certificate and Intermediate Certificate of Signing Certificate Authority

When you upload the Root and Intermediate Certificates, you must upload each certificate in the certificate chain to IM and Presence Service from the Root Certificate down to the last Intermediate Certificate, as follows:

root > intermediate-1 > intermediate-2 > … > intermediate-N

With each certificate that you upload in the chain, you must specify which previously uploaded certificate signed it. For example:

- For intermediate-1, the root cert was used to sign it.
- For intermediate-2, the intermediate-1 cert was used to sign it.

You must upload the Root Certificate and the Intermediate Certificates, if any, to the **cup-xmpp-trust** store on the IM and Presence database publisher node. Complete the following procedure to upload the Root Certificate and the Intermediate Certificate of the signing Certificate Authority (CA) to the IM and Presence Service deployment.

Procedure

Step 1 On the IM and Presence database publisher node, choose **Cisco Unified IM and Presence OS Administration** > **Security** > **Certificate Management**.

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

Step 3 From the Certificate Name drop-down list, choose **cup-xmpp-trust**.

Step 4 Enter a description for the signed certificate.

Step 5 Click **Browse** to locate the file for the Root Certificate.

Step 6 Click **Upload File**.

Step 7 Upload each Intermediate Certificate in the same way using the **Upload Certificate/Certificate chain** window.

What to do next

Verify that the CA certificates have synced to other clusters.

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.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **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 Signed Certificate to Federation Nodes

When the CA certificates have correctly synced to all clusters, you can upload the appropriate signed certificate to each IM and Presence Service federation node. You do not need to upload the certificate to all nodes, only nodes for federation.

Note Cisco recommends that you sign all required cup-xmpp-s2s certificates for a cluster and upload them at the same time.

Procedure

Step 1 Choose **Cisco Unified IM and Presence OS AdministrationSecurityCertificate Management**.

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

Step 3 From the Certificate Name drop-down list, choose **cup-xmpp**.

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 federation node.

For more information about certificate management, see the *Cisco Unified Communications Operating System Administration Guide*.

What to do next

Restart the Cisco XCP XMPP Federation Connection Manager service on the affected nodes.

Restart Cisco XCP XMPP Federation Connection Manager Service

After you upload the cup-xmpp-s2s 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.

Delete Self-Signed Trust Certificates

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

When CA-signed certificates are generated to replace the original self-signed trust certificates on either IM and Presence Service or Cisco Unified Communications Manager the original self-signed trust certificates persist in the service trust store of both nodes. If you want to delete the self-signed trust certificates, you must delete them on both the IM and Presence Service and Cisco Unified Communications Manager nodes.

Delete Self-Signed Trust Certificates from IM and Presence Service

Before you begin

Important You have configured the IM and Presence Service nodes with CA-signed certificates, and 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 Log in to the **Cisco Unified IM and Presence Operating System Administration** user interface, 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 — tomcat-trust
- Cup-xmpp — cup-xmpp-trust
- Cup-xmpp-s2s — cup-xmpp-trust
- Cup — 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 only appears for certificates you have the authority to delete.

What to do next

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.

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 20.

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.

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 Log in to the **Cisco Unified Operating System Administration** user interface, 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.

SIP Security Settings Configuration on IM and Presence Service

Configure TLS Peer Subject

When you import an IM and Presence Service certificate, IM and Presence Service automatically attempts to add the TLS peer subject to the TLS peer subject list, and to the TLS context list. Verify the TLS peer subject and TLS context configuration is set up to your requirements.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **System** > **Security** > **TLS Peer Subjects.**

Step 2 Click **Add New**.

Step 3 Perform one of the following actions for the Peer Subject Name:

a) Enter the subject CN of the certificate that the node presents.

b) Open the certificate, look for the CN and paste it here.

Step 4 Enter the name of the node in the Description field.

Step 5 Click **Save**.

What to do next

Proceed to configure the TLS context.

Configure TLS Context

When you import an IM and Presence Service certificate, IM and Presence Service automatically attempts to add the TLS peer subject to the TLS peer subject list, and to the TLS context list. Verify the TLS peer subject and TLS context configuration is set up to your requirements.

Before you begin

Configure a TLS peer subject on IM and Presence Service.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **System** > **Security** > **TLS Context Configuration**.

Step 2 Click **Find**.

Step 3 Choose **Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context**.

Step 4 From the list of available TLS peer subjects, choose the TLS peer subject that you configured.

Step 5 Move this TLS peer subject to Selected TLS Peer Subjects.

Step 6 Click **Save**.

Step 7 Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Service Activation**.

Step 8 Restart the Cisco SIP Proxy service.

Troubleshooting Tip

You must restart the SIP proxy service before any changes that you make to the TLS context take effect.

Related Topics

Restart SIP Proxy Service, on page 7

XMPP Security Settings Configuration on IM and Presence Service

XMPP Security Modes

IM and Presence Service provides increased security for XMPP-based configuration. The following table describes these XMPP security modes. To configure the XMPP security modes on IM and Presence Service, choose **Cisco Unified CM IM and Presence Administration** > **System** > **Security** > **Settings**.

Table 3: XMPP Secure Mode Descriptions

Secure Mode	Description
Enable XMPP Client To IM/P Service Secure Mode	If you turn on this setting, IM and Presence Service establishes a secure TLS connection between the IM and Presence Service nodes and XMPP client applications in a cluster. IM and Presence Service turns on this secure mode by default. We recommend that you do not turn off this secure mode unless the XMPP client application can protect the client login credentials in nonsecure mode. If you do turn off the secure mode, verify that you can secure the XMPP client-to-node communication in some other way.
Enable XMPP Router-to-Router Secure Mode	If you turn on this setting, IM and Presence Service establishes a secure TLS connection between XMPP routers in the same cluster, or in different clusters. IM and Presence Service automatically replicates the XMPP certificate within the cluster and across clusters as an XMPP trust certificate. An XMPP router will attempt to establish a TLS connection with any other XMPP router that is in the same cluster or a different cluster, and is available to establish a TLS connection.

Secure Mode	Description
Enable Web Client to IM/P Service Secure Mode	If you turn on this setting, IM and Presence Service establishes a secure TLS connection between the IM and Presence Service nodes and XMPP-based API client applications. If you turn on this setting, upload the certificates or signing certificates for the web client in the cup-xmpp-trust repository on IM and Presence Service. **Caution** If your network and IM and Presence Service node support IPv6, and you enable secure TLS connections to XMPP-based API client applications, you must enable the IPv6 enterprise parameter for the node and enable the IPv6 Ethernet IP setting for Eth0 on each IM and Presence Service node using Cisco Unified IM and Presence Operating System Administration; otherwise, the node attempts to use IPv4 for IP traffic. Any packets that are received from an XMPP-based API client application that has an IPv6 address will not be delivered. The node cannot revert to using IPv4 if the node is configured to use an IPv6 connection to an external database, LDAP server, or Exchange server, or if a federation deployment using IPv6 is configured for the node.

If you update the XMPP security settings, restart the services. Perform one of these actions:

- Restart the Cisco XCP Connection Manager if you edit **Enable XMPP Client To IM/P Service Secure Mode**. Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services** to restart this service.
- Restart the Cisco XCP Router if you edit the **Enable XMPP Router-to-Router Secure Mode**. Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Network Services** to restart this service.
- Restart the Cisco XCP Web Connection Manager if you edit **Enable Web Client To IM/P Service Secure Mode**. Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services** to restart this service.

Related Topics

Configure Secure Connection Between IM and Presence Service and XMPP Clients, on page 25

Configure Secure Connection Between IM and Presence Service and XMPP Clients

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **System** > **Security** > **Settings**.

Step 2 Perform one of the following tasks:

- To establish a secure TLS connection between IM and Presence Service and XMPP client applications in a cluster, choose **Enable XMPP Client To IM/P Service Secure Mode**.

  Cisco recommends that you do not turn off this secure mode unless the XMPP client application can protect the client login credentials in a nonsecure mode. If you do turn off the secure mode, verify that you can secure the XMPP client-to-node communication in some other way.

- To establish a secure TLS connection between IM and Presence Service and XMPP-based API client applications in a cluster, choose **Enable Web Client To IM/P Service Secure Mode**.

  If you turn on this setting, upload the certificates or signing certificates for the web client in the cup-xmpp-trust repository on IM and Presence.

  Caution If your network and IM and Presence Service node support IPv6, and you enable secure TLS connections to XMPP-based API client applications, you must enable the IPv6 enterprise parameter for the node and enable the IPv6 Ethernet IP setting for Eth0 on each IM and Presence Service node in the cluster. If the enterprise parameter and Eth0 are not configured for IPv6, the node attempts to use IPv4 for any IPv6 packets that are received from an XMPP-based API client application and those IPv6 packets are not delivered.

  The node cannot revert to using IPv4 if the node is configured to use an IPv6 connection to an external database, LDAP server, or an Exchange server, or if a federation deployment using IPv6 is configured for the node.

Step 3 Click **Save**.

If you update the XMPP security settings, restart the following service using one of the following actions:

- Restart the Cisco XCP Connection Manager if you edit **Enable XMPP Client To IM/P Service Secure Mode**. Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services** to restart this service.
- Restart the Cisco XCP Web Connection Manager if you edit **Enable Web Client To IM/P Service Secure Mode**. Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services** to restart this service.

What to do next

Proceed to turn on the services that support XMPP clients on the IM and Presence Service node.

Related Topics

Third-Party Client Integration

Turn On IM and Presence Service Services to Support XMPP Clients

Perform this procedure on each node in your IM and Presence Service cluster.

Procedure

Step 1 Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Service Activation**.

Step 2 Choose the IM and Presence Service node from the **Server** menu.

Step 3 Turn on the following services:

- Cisco XCP Connection Manager - Turn on this service if you are integrating XMPP clients, or XMPP-based API clients on IM and Presence Service.
- Cisco XCP Authentication Service - Turn on this service if you are integrating XMPP clients, or XMPP-based API clients, or XMPP-based API clients on IM and Presence Service.
- Cisco XCP Web Connection Manager - Optionally, turn on this service if you are integrating XMPP clients, or XMPP-based API clients on IM and Presence Service.

Step 4 Click **Save**.

Tip For XMPP clients to function correctly, make sure you turn on the Cisco XCP Router on all nodes in your cluster.

Related Topics

Third-Party Client Integration

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 certificate *cup-xmpp-s2s* 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”.

Tip To view the `cup-xmpp-s2s` certificate on any node, choose **Cisco Unified IM and Presence OS Administration** > **Security** > **Certificate Management** and click on the **cup-xmpp-s2s** link .

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.