Security Certificate Configuration for XMPP Federation

This section provides information on the Security Certificate Configuration for XMPP Federation.

Security Certificate Configuration for XMPP Federation

To configure security for XMPP federation, you must complete the following procedures:

1. Verify that all local domains are created and configured on the system and, if necessary, manually create any missing local domains before you generate the cup-xmpp-s2s certificate.
2. Create the certificate once using one of the following types of certificates:
   - Self-signed single server certificate for XMPP federation
   - CA-signed single-server or multiple server certificate for XMPP federation
3. Import the root CA certificate.

   You must repeat this procedure every time you federate with a new enterprise whose CA you do not already trust. Likewise, you should follow this procedure if the new enterprise uses self-signed certificates, where the self-signed certificates are uploaded instead of the root CA certificate.

Local Domain Validation for XMPP Federation

All local domains must be included in the generated cup-xmpp-s2s certificate. Before you generate the cup-xmpp-s2s certificate, validate that all local domains are configured and appear in the Domains window. Manually add any domains that are planned for, but that don't yet appear in the list of local domains. For

example, a domain that does not currently have any users assigned normally does not appear in the list of domains.

Log in to the **Cisco Unified CM IM and Presence Administration** user interface, choose **Presence** > **Domains**.

After you have validated that all domains are created in the system, you can proceed to create the cup-xmpp-s2s certificate once using either a self-signed certificate or a CA-signed certificate for XMPP federation. If email address for federation is enabled, all email domains must also be included in the certificate.

If you add, update, or delete any local domains and regenerate the cup-xmpp-s2s certificate, you must restart the Cisco XCP XMPP Federation Connection Manager service. To restart this service, log in to the **Cisco Unified IM and Presence Serviceability** user interface and choose **Tools** > **Control Center - Feature Services**.

Related Topics

Add or Update Email Domain
Use a Self-Signed Certificate for XMPP Federation, on page 2
Use of a CA Signed Certificate for XMPP Federation, on page 3
View Email Domains

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 the appropriate Certificate Signing Request (CSR). The resulting signed multi-server certificate and its associated chain of signing certificates is 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)*.

Use a Self-Signed Certificate for XMPP Federation

This section describes how to use a self-signed certificate for XMPP federation. For information about using a CA-signed certificate, see Use of a CA Signed Certificate for XMPP Federation, on page 3.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Operating System Administration** user interface. Choose **Security** > **Certificate Management**.

Step 2 Click **Generate Self-signed**.

Step 3 From the Certificate Purpose drop-down list, choose **cup-xmpp-s2s** and click **Generate**.

Step 4 Restart the Cisco XCP XMPP Federation Connection Manager service. Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools** > **Control Center - Network Services** to restart this service.

Step 5 Download and send the certificate to another enterprise so that it can be added as a trusted certificate on their XMPP server. This can be a IM and Presence Service node or another XMPP server.

What to do next

Use of a CA Signed Certificate for XMPP Federation, on page 3

Use of a CA Signed Certificate for XMPP Federation

This section describes how to use a CA signed certificate. For information about using a self-signed certificate, see Use a Self-Signed Certificate for XMPP Federation, on page 2.

Generate a Certificate Signing Request for XMPP Federation

This procedure describes how to generate a Certificate Signing Request (CSR) for a Microsoft Certificate Services CA.

Note While this procedure is to generate a CSR for signing a Microsoft Certificate Services CA, the steps to generate the CSR (steps 1 to 3) apply when requesting a certificate from any Certificate Authority.

Before you begin

Configure the domain for the XMPP certificate.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Operating System Administration** user interface. Choose **Security** > **Certificate Management**.

Step 2 To generate the CSR, perform these steps:

a) Click **Generate CSR**.

b) From the Certificate Purpose drop-down list, choose **cup-xmpp-s2s** for the certificate name.

c) For the distribution select the FQDN of the local server to generate a single-signed certificate or **Multi-server(SAN)** to generate a multi-server certificate.

Note For both distribution options all presence domains, email domains, and Group Chat Server aliases configured on the Cisco Unified IM and Presence Administration user interface will be automatically included in the CSR that is generated. If you choose the **Multi-server(SAN)** option, the hostname or FQDN of each IM and Presence Service node(s) is also added to the CSR that is generated. 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)*.

d) Click **Generate**.

Note If you have selected **Multi-server(SAN)** the CSR will be copied to the file-system on all other IM and Presence Service nodes in the cluster.

e) Click **Close**, and return to the main certificate window.

Step 3 To download the `.csr` file to your local machine:

a) Click **Download CSR**.
b) Choose **cup-xmpp-s2s** from the Certificate Purpose drop-down menu.
c) Click **Download CSR** to download this file to your local machine.

Step 4 Using a text editor, open the `cup-xmpp-s2s.csr` file.

Step 5 Copy the contents of the CSR file.

You must copy all information from and including

- BEGIN CERTIFICATE REQUEST

to and including

END CERTIFICATE REQUEST -

Step 6 On your internet browser, browse to your CA server, for example: `http://<name of your Issuing CA Server>/certsrv`.

Step 7 Click **Request a certificate**.

Step 8 Click **Advanced certificate request**.

Step 9 Click **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file,** or submit a renewal request by using a base-64-encoded PKCS #7 file.

Step 10 Paste the contents of the CSR file (that you copied in step 5) into the Saved Request field.

Step 11 Click **Submit**.

Step 12 On your internet browser, return to the URL: `http://<name of your Issuing CA Server>/certsrv`.

Step 13 Click **View the status of a pending certificate request**.

Step 14 Click on the certificate request that you issued in the previous section.

Step 15 Click **Base 64 encoded**.

Step 16 Click **Download certificate**.

Step 17 Save the certificate to your local machine:

a) Specify a certificate file name `cup-xmpp-s2s.pem`.
b) Save the certificate as type **Security Certificate**.

What to do next

Upload a CA-Signed Certificate for XMPP Federation, on page 5

Troubleshooting Tips

- If the list of supported domains on IM and Presence Service changes, then the cup-xmpp-s2s certificate must be regenerated to reflect the new domain list.

Upload a CA-Signed Certificate for XMPP Federation

Before you begin

Complete the steps in Generate a Certificate Signing Request for XMPP Federation, on page 3.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Operating System Administration** user interface. Choose **Security** > **Certificate Management**.

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

Step 3 Choose **cup-xmpp-s2s** for Certificate Name.

Step 4 Browse to the location of the CA-signed certificate that you saved to your local machine.

Step 5 Click **Upload File**.

Note If you have generated a multi-server SAN based certificate, you can upload this to any IM and Presence Service node in the cluster. When this is done 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. If a self-signed certificate already exists on any of the nodes, it will be overwritten by the new multiple server certificate. 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)*.

Step 6 Restart the Cisco XMPP Federation Connection Manager service. Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools** > **Control Center - Network Services** to restart this service.

Note If you upload a multi-server certificate you must restart the XCP Router service on **all** IM and Presence Service nodes in the cluster.

What to do next

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 certificates persist in the node's service trust store. Leaving the original self-signed certificates in the service trust store is not an issue because no service presents them. However, you can delete these certificates, but if you do, you must delete them on the IM and Presence Service and Cisco Unified Communications Manager,

See the section Delete Self-Signed Trust Certificates in Part II, Chapter 9 — Security Configuration on IM and Presence Service, in the appropriate release of the *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Import a Root CA Certificate for XMPP Federation

Note This section describes how to manually upload the cup-xmpp-s2s trust certificates to IM and Presence Service. You can also use the Certificate Import Tool to automatically upload cup-xmpp-s2s trust certificates. To access the Certificate Import Tool, log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **System** > **Security** > **Certificate Import Tool**, and see the Online Help for instructions on how to use this tool.

If IM and Presence Service federates with an enterprise, and a commonly trusted Certificate Authority (CA) signs the certificate of that enterprise, you must upload the root certificate from the CA to an IM and Presence Service node.

If IM and Presence Service federates with an enterprise that uses a self-signed certificate rather than a certificate signed by a commonly trusted CA, you can upload the self-signed certificate using this procedure.

Before you begin

Download the root CA certificate and save it to your local machine.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Operating System Administration** user interface. Choose **Security** > **Certificate Management** on IM and Presence Service.

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

Step 3 Choose **cup-xmpp-trust** for Certificate Name.

Note Leave the Root Name field blank.

Step 4 Click **Browse**, and browse to the location of the root CA certificate that you previously downloaded and saved to you local machine.

Step 5 Click **Upload File** to upload the certificate to the IM and Presence Service node.

Note You must repeat this procedure every time you federate with a new enterprise whose CA you do not already trust. Likewise, you should follow this procedure if the new enterprise uses self-signed certificates, where the self-signed certificates are uploaded instead of the Root CA certificate.

Troubleshooting Tip

If your trust certificate is self-signed, you cannot turn on the **Require client side certificates** parameter in the XMPP federation security settings window.