Configuring Security Certificates for XMPP Federation

June 18, 2013

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

1. Configure the domain for the XMPP certificate, see Configuring the Domain for XMPP Certificate, page 12-1
2. Create the certificate once using one of the following procedures:
   - Using a Self-signed Certificate for XMPP Federation, page 12-2
   - Using a CA-signed Certificate for XMPP Federation, page 12-3
3. Import the root CA certificate, see Importing the Root CA Certificate for XMPP Federation, page 12-5. 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.

Configuring the Domain for XMPP Certificate

For XMPP Federation, the Subject Common Name (CN) for the certificate must contain the domain of the Cisco Unified Presence server. For Cisco Unified Presence Release 8.6(5) and later, the Subject Alternative Name (SAN) for the certificate must contain the domain of the Cisco Unified Presence server.

Procedure

Step 1 Select **Cisco Unified Presence Administration > System > Security > Settings**.

Step 2 In **Domain name for XMPP Server-to-Server certificate Subject Common name**, enter the domain name of the Cisco Unified Presence server.

For Cisco Unified Presence Release 8.6(5) and later, the Subject Alternative Name (SAN) for the certificate must contain the domain of the Cisco Unified Presence server.

Tip You can configure a wildcard domain here, for example, '*.example.net' if you deploy the Chat feature on Cisco Unified Presence, and the chat component is a subdomain of the parent domain.

Step 3 If you want the general XMPP certificate to use the same Domain Name as the XMPP server-to-server certificate, check **Use Domain Name for XMPP Certificate Subject Common Name**.

For Cisco Unified Presence Release 8.6(5) and later, the Subject Alternative Name (SAN) for the certificate must contain the domain of the Cisco Unified Presence server

Step 4 Select **Save**.

What To Do Next

Create the certificate once using one of the following procedures:

- Using a Self-signed Certificate for XMPP Federation, page 12-2
- Using a CA-signed Certificate for XMPP Federation, page 12-3

Troubleshooting Tips

- If you make any changes to this configuration, you must restart the Cisco UP XCP Router service. Select **Cisco Unified Serviceability > Tools > Control Center - Network Services** to restart this service.
- If you change server-to-server domain name value, you must regenerate affected XMPP S2S certificates before you restart the Cisco UP XCP Router service.

Using 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 Using a CA-signed Certificate for XMPP Federation, page 12-3.

Procedure

Step 1 Select **Cisco Unified Operating System Administration > Security > Certificate Management**.

Step 2 Select **Generate New**.

Step 3 Select **cup-xmpp-s2s** from the Certificate Name drop-down list and select **Generate**.

Step 4 Restart the Cisco UP XCP Router service. Select **Cisco Unified Serviceability > 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 Cisco Unified Presence server or another XMPP server.

What To Do Next

Importing the Root CA Certificate for XMPP Federation, page 12-5

Using 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 Using a Self-signed Certificate for XMPP Federation, page 12-2.

- Generating a Certificate Signing Request for XMPP Federation, page 12-3
- Uploading the CA-Signed Certificate for XMPP Federation, page 12-4

Generating 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, see Configuring the Domain for XMPP Certificate, page 12-1

Procedure

Step 1 Select **Cisco Unified Operating System Administration > Security > Certificate Management** on Cisco Unified Presence.

Step 2 To generate the CSR, perform these steps:

a. Select **Generate CSR**.

b. Select **cup-xmpp-s2s** for the certificate name.

c. Select **Generate CSR**.

d. Select Close, and return to the main certificate window.

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

a. Select **Download CSR**.

b. Select the **cup-xmpp-s2s.csr** file in the menu on the Download Certificate Signing Request window.

c. Select **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 Select **Request a certificate**.

Step 8 Select **Advanced certificate request**.

Step 9 Select **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 Select **Submit**.

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

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

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

Step 15 Select **Base 64 encoded**.

Step 16 Select **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

Uploading the CA-Signed Certificate for XMPP Federation, page 12-4

Troubleshooting Tips

- If you make any changes to this configuration, you must restart the Cisco UP XCP Router service. Select **Cisco Unified Serviceability > Tools > Control Center - Network Services** to restart this service.
- If you change server-to-server domain name value, you must regenerate affected XMPP S2S certificates before you restart the Cisco UP XCP Router service.

Uploading the CA-Signed Certificate for XMPP Federation

Before You Begin

Complete the steps in Generating a Certificate Signing Request for XMPP Federation, page 12-3.

Procedure

Step 1 Select **Cisco Unified Operating System Administration > Security > Certificate Management** on Cisco Unified Presence.

Step 2 Select **Upload Certificate**.

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

Step 4 Specify the name of the root certificate in the Root Certificate Field.

Step 5 Select **Upload File**.

Step 6 Browse to the location of the CA-signed certificate that you saved to your local machine.

Step 7 Select **Upload File**.

Step 8 Restart the Cisco UP XCP Router service. Select **Cisco Unified Serviceability > Tools > Control Center - Network Services** to restart this service.

What To Do Next

Importing the Root CA Certificate for XMPP Federation, page 12-5

Importing the Root CA Certificate for XMPP Federation

Note This section describes how to manually upload the XMPP S2S trust certificates to Cisco Unified Presence. You can also use the Certificate Import Tool to automatically upload XMPP S2S trust certificates. To access the Certificate Import Tool, select **Cisco Unified Presence Administration > System > Security > Certificate Import Tool**, and see the Online Help for instructions on how to use this tool.

If Cisco Unified Presence 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 Cisco Unified Presence server.

If Cisco Unified Presence 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 Select **Cisco Unified Operating System Administration > Security > Certificate Management** on Cisco Unified Presence.

Step 2 Select **Upload Certificate**.

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

Note Leave the Root Name field blank.

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

Step 5 Select **Upload File** to upload the certificate to the Cisco Unified Presence server.

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.