Main page: Cisco Unified Presence, Release 7.x

Contents

Previous Topic

- Configuring Cisco Unified Presence Release 7.x for Interdomain Federation
- How to Exchange Certificates Using Self-Signed Certificates
- How to Exchange Certificates Using CA-Signed Certificates

How to Exchange Certificates Using Self-Signed Certificates

Note: In order identify each Cisco Unified Presence server, the servers are referred to as *Cisco Unified Presence server1* and *Cisco Unified Presence server2*.

Generating a New Certificate on Cisco Unified Presence Server1

Procedure

1. On Cisco Unified Presence server1, select **Cisco Unified Operating System Administration > Security > Certificate Management**.
2. Click **Generate New**.
3. Select **sipproxy** for the certificate name.
4. Click on **sipproxy.pem** in the certificate list.
   The certificate configuration displays. The `Issuer CN' and the `Subject CN' should be the FQDN of the Cisco Unified Presence server1.
5. Click **Download**, and save the certificate locally as **sipproxy.pem.**

Related Topics

- Getting More Information

What To Do Next

Importing the Certificate onto Cisco Unified Presence Server2

Importing the Certificate onto Cisco Unified Presence Server2

Before You Begin

Generate a new certificate on Cisco Unified Presence Server1.

Procedure

1. On Cisco Unified Presence server2, select **Cisco Unified Operating System Administration > Security > Certificate Management**.
2. Click **Upload Certificate**.
3. Select **sipproxy-trust**. for the certificate name.
   Note: Leave the Root Name field blank.
4. Click **Browse**.
5. Locate the certificate (that you created in the previous procedure) on your local computer.
6. Click **Upload File**.

Troubleshooting Tips

When the certificate list is refreshes, the entry **sipproxy-trust** should be present. The .pem file, .der file and File Name of this entry should be the FQDN of Cisco Unified Presence server1.

Related Topics

- Getting More Information

What To Do Next

Generating a New Certificate on Cisco Unified Presence Server2

Generating a New Certificate on Cisco Unified Presence Server2

Before You Begin

Import the Certificate onto Cisco Unified Presence Server2.

Procedure

1. On Cisco Unified Presence server2, select **Cisco Unified Operating System Administration > Security > Certificate Management**.
2. Generate and download the **sipproxy.pem** file as described in Generating a New Certificate on Cisco Unified Presence Server1.

Troubleshooting Tips

In the certificate configuration, the `Issuer CN' and the `Subject CN' of the certificate should be the FQDN of the Cisco Unified Presence server2.

Related Topics

- Getting More Information

What To Do Next

Importing the New Certificate onto Cisco Unified Presence Server1

Importing the New Certificate onto Cisco Unified Presence Server1

Before You Begin

Generate a new certificate on Cisco Unified Presence Server2.

Procedure

1. On Cisco Unified Presence Server1, select **Cisco Unified Operating System Administration > Security > Certificate Management**.
2. Cisco Unified Presence, Release 7.x -- How to Configure Security Certificates for Cisco Unified Presence to Cisco Unified Presence Federation (with no Cisco Adaptive Security Appliance)
3. Importing the Certificate onto Cisco Unified Presence Server2|Importing the Certificate onto Cisco Unified Presence Server2]].

Troubleshooting Tips

When the certificate list refreshes, the entry **sipproxy-trust** should be present. The .pem file, .der file and File Name of this entry should be the FQDN of Cisco Unified Presence server2.

Related Topics

- Getting More Information

How to Exchange Certificates Using CA-Signed Certificates

Note: You need to perform the procedures described in this section on **both** Cisco Unified Presence servers.

Downloading the Root Certificate for Interdomain Federation

Procedure

1. Click **Start > Run**.
2. Type **http://<name of your Issuing CA Server>/certsrv**.
3. Click **OK**.
4. Click **Download a CA certificate, certificate chain, or CRL** from Select a task.
5. Click **Base 64**.
6. Click **Download CA certificate**.

Related Topics

- Getting More Information

What To Do Next

Uploading the Root Certificate onto Cisco Unified Presence for Interdomain Federation

Uploading the Root Certificate onto Cisco Unified Presence for Interdomain Federation

Before You Begin

Download the root certificate.

Procedure

1. Select **Cisco Unified Operating System Administration > Security > Certificate Management**.
2. Click **Upload Certificate**.
3. Select **sipproxy-trust** for the certificate name.
   Note: Leave the Root Name field blank.
4. Click **Browse**.
5. Locate the CA certificate file (that you created in the previous procedure) on your local computer.
6. Click **Upload File**.

Troubleshooting Tips

When the certificate list is refreshed, the entry **sipproxy-trust** should be present. The .pem file, .der file and File Name of this entry should be the name of the CA that you downloaded the CA certificate from.

Related Topics

- Getting More Information

What To Do Next

Generating the Certificate Signing Request on Cisco Unified Presence for Interdomain Federation

Generating the Certificate Signing Request on Cisco Unified Presence for Interdomain Federation

Procedure

1. Select **Cisco Unified Operating System Administration > Security > Certificate Management**.
2. Click **Generate New**.
3. Select **sipproxy** for the certificate name.
4. Click **Generate New**.
5. Click **Generate CSR** on the Certificate Management screen.
6. Select **sipproxy** for the certificate name.
7. Click **Generate CSR.**
8. Click **Download CSR** on the Certificate Management screen.
9. Select **sipproxy** for the certificate name.
10. Click **Download CSR**.
11. Select the location on your local machine where you wish to download the CSR file to.
12. Using a text editor, open the CSR file you downloaded to your local machine in the previous step.
13. Copy the contents of the CSR file.
    You must copy all information from and including
    -----BEGIN CERTIFICATE REQUEST
    to and including
    END CERTIFICATE REQUEST-----

14. On your internet browser, browse to your CA server at the URL **http://<name of your Issuing CA Server>/certsrv**.
15. Click **Request a certificate**.
16. Select **Advanced certificate request**.
17. 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**.
18. Paste the contents of the CSR file (that you copied in step 13) into the Saved Request field.
19. Click **Submit**.

Related Topics

- Getting More Information

What To Do Next

Downloading the Signed Certificate for Interdomain Federation

Downloading the Signed Certificate for Interdomain Federation

Before You Begin

Generate the Certificate Signing Request (CSR) on Cisco Unified Presence.

Procedure

1. On your internet browser, browse to your CA server at the URL **http://<name of your Issuing CA Server>/certsrv**.
2. Click **View the status of a pending certificate request**.
3. Click on the certificate request that you issued in the previous section.
4. Click **Base 64 encoded**.
5. Click **Download certificate**.
6. Save the certificate to your local machine:
    - ♦ Specifying a certificate file name **sipproxy.pem**.
    - ♦ Save the certificate as type `Security Certificate'.

Related Topics

- Getting More Information

What To Do Next

Uploading the Signed Certificate onto Cisco Unified Presence for Interdomain Federation

Uploading the Signed Certificate onto Cisco Unified Presence for Interdomain Federation

Before You Begin

Download the signed certificate for interdomain federation.

Procedure

1. Select **Cisco Unified Operating System Administration > Security > Certificate Management**.
2. Click **Upload Certificate**.
3. Select **sipproxy** for the certificate name.
4. For the root certificate, enter the name of the root certificate you generated previously.
5. Click **Browse**.
6. Select the **sipproxy.pem** file downloaded from the CA.
7. Click **Upload File**.
8. On Cisco Unified Presence, select **Cisco Unified Operating System Administration > Security > Certificate Management**.
9. Click on the **sipproxy.pem** entry.
10. Verify that the issuer of the certificate is the CA that you received the certificate from, and the subject of the certificate is the FQDN of the Cisco Unified Presence server.

Related Topics

- Getting More Information