APPENDIX C

Configuring Security Certificates for Cisco Unified Presence to Cisco Unified Presence Federation (with no Cisco Adaptive Security Appliance)

January 26, 2009

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

Step 1 On Cisco Unified Presence server1, select **Cisco Unified Operating System Administration > Security > Certificate Management**.

Step 2 Click **Generate New**.

Step 3 Select **sipproxy** for the certificate name.

Step 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.

Step 5 Click **Download**, and save the certificate locally as **sipproxy.pem.**

What To Do Next

Importing the Certificate onto Cisco Unified Presence Server2, page C-2

Importing the Certificate onto Cisco Unified Presence Server2

Before You Begin

Complete the steps in Generating a New Certificate on Cisco Unified Presence Server1, page C-1

Procedure

Step 1 On Cisco Unified Presence server2, select **Cisco Unified Operating System Administration > Security > Certificate Management**.

Step 2 Click **Upload Certificate**.

Step 3 Select **sipproxy-trust**. for the certificate name.

Note Leave the Root Name field blank.

Step 4 Click **Browse**.

Step 5 Locate the certificate (that you created in the previous procedure) on your local computer.

Step 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.

What To Do Next

Generating a New Certificate on Cisco Unified Presence Server2, page C-2

Generating a New Certificate on Cisco Unified Presence Server2

Before You Begin

Complete the steps Importing the Certificate onto Cisco Unified Presence Server2, page C-2

Procedure

Step 1 On Cisco Unified Presence server2, select **Cisco Unified Operating System Administration > Security > Certificate Management**.

Step 2 Generate and download the **sipproxy.pem** file as described in Generating a New Certificate on Cisco Unified Presence Server1, page C-1.

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.

What To Do Next

Importing the New Certificate onto Cisco Unified Presence Server1, page C-3

Importing the New Certificate onto Cisco Unified Presence Server1

Before You Begin

Complete the steps in Generating a New Certificate on Cisco Unified Presence Server2, page C-2

Procedure

Step 1 On Cisco Unified Presence Server1, select **Cisco Unified Operating System Administration > Security > Certificate Management**.

Step 2 Upload the certificate as described in Importing the Certificate onto Cisco Unified Presence Server2, page C-2.

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.

What To Do Next

Importing the New Certificate onto Cisco Unified Presence Server1, page C-3

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

Procedure

Step 1 Click **Start > Run**.

Step 2 Type **http://<name of your Issuing CA Server>/certsrv**.

Step 3 Click **OK**.

Step 4 Click **Download a CA certificate, certificate chain, or CRL** from Select a task.

Step 5 Click **Base 64**.

Step 6 Click **Download CA certificate**.

What To Do Next

Uploading the Root Certificate onto Cisco Unified Presence, page C-4

Uploading the Root Certificate onto Cisco Unified Presence

Before You Begin

Complete the steps in Downloading the Root Certificate, page C-4

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

Step 2 Click **Upload Certificate**.

Step 3 Select **sipproxy-trust** for the certificate name.

Note Leave the Root Name field blank.

Step 4 Click **Browse**.

Step 5 Locate the CA certificate file (that you created in the previous procedure) on your local computer.

Step 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.

What To Do Next

Generating the Certificate Signing Request on Cisco Unified Presence, page C-4

Generating the Certificate Signing Request on Cisco Unified Presence

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

Step 2 Click **Generate New**.

Step 3 Select **sipproxy** for the certificate name.

Step 4 Click **Generate New**.

Step 5 Click **Generate CSR** on the Certificate Management screen.

Step 6 Select **sipproxy** for the certificate name.

Step 7 Click **Generate CSR.**

Step 8 Click **Download CSR** on the Certificate Management screen.

Step 9 Select **sipproxy** for the certificate name.

Step 10 Click **Download CSR**.

Step 11 Select the location on your local machine where you wish to download the CSR file to.

Step 12 Using a text editor, open the CSR file you downloaded to your local machine in the previous step.

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-----

Step 14 On your internet browser, browse to your CA server at the URL **http://<name of your Issuing CA Server>/certsrv**.

Step 15 Click **Request a certificate**.

Step 16 Select **Advanced certificate request**.

Step 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**.

Step 18 Paste the contents of the CSR file (that you copied in step 13) into the Saved Request field.

Step 19 Click **Submit**.

What To Do Next

Downloading the Signed Certificate, page C-5

Downloading the Signed Certificate

Before You Begin

Complete the steps in Generating the Certificate Signing Request on Cisco Unified Presence, page C-4

Step 1 On your internet browser, browse to your CA server at the URL **http://<name of your Issuing CA Server>/certsrv**.

Step 2 Click **View the status of a pending certificate request**.

Step 3 Click on the certificate request that you issued in the previous section.

Step 4 Click **Base 64 encoded**.

Step 5 Click **Download certificate**.

Step 6 Save the certificate to your local machine:

- Specifying a certificate file name **sipproxy.pem**.
- Save the certificate as type 'Security Certificate'.

What To Do Next

Uploading the Signed Certificate onto Cisco Unified Presence, page C-6

Uploading the Signed Certificate onto Cisco Unified Presence

Before You Begin

Complete the steps in Downloading the Signed Certificate, page C-5

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

Step 2 Click **Upload Certificate**.

Step 3 Select **sipproxy** for the certificate name.

Step 4 For the root certificate, enter the name of the root certificate you generated previously.

Step 5 Click **Browse**.

Step 6 Select the **sipproxy.pem** file downloaded from the CA.

Step 7 Click **Upload File**.

Step 8 On Cisco Unified Presence, select **Cisco Unified Operating System Administration > Security > Certificate Management**.

Step 9 Click on the **sipproxy.pem** entry.

Step 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

Uploading the Root Certificate onto Cisco Unified Presence, page C-4