Main page: Cisco Unified Presence, Release 7.x

Contents

Previous Topic

- Configuring Cisco Unified Presence Release 7.x with Microsoft OCS for Remote Call Control

This module is only applicable if you require a secure connection between Cisco Unified Presence and Microsoft OCS.

Note: SIP Proxy certificates (own and trust) should be X.509 version 3 compliant.

Configuring the Standalone Root Certificate Authority (CA) for Remote Call Control

Procedure

1. Sign in to the CA server with Domain Administrator privileges.
2. Insert the Windows Server 2003 CD.
3. Select **Start > Settings > Control Panel**.
4. Double-click **Add or Remove Programs**.
5. Select **Add/Remove Windows Components**.
6. Select **Application Server**.
7. Select **Internet Information Services (IIS)**.
8. Complete the installation procedure.
9. Select **Add/Remove Windows Components**.
10. Select **Certificate Services**.
11. Select **Next**.
12. Select **Standalone root CA**.
13. Select **Next**.
14. Type the name of the CA root. This name can be a friendly name for the CA root in the forest root.
15. Change the time to the number of years required for this certificate.
16. Select **Next** to begin installation.
17. Select the location for the certificate database and the certificate database files.
18. Select **Next**.
19. Select **Yes** when prompted to stop IIS.
20. Select **Yes** when prompted with a message regarding Active Server Pages.
21. Select **Finish**.

What To Do Next

Downloading the Root Certificate from the CA Server for Remote Call Control.

Downloading the Root Certificate from the CA Server for Remote Call Control

Before You Begin

Configure the Standalone Root Certificate Authority.

Procedure

1. Sign in to your CA server and open a web browser.
2. Open the URL **http://<ca_server_IP_address>/certsrv**.
3. Select **Download a CA certificate, certificate chain, or CRL**.
4. Select **Base 64** for the Encoding Method.
5. Select **Download CA Certificate**.
6. Save the certificate file certnew.cer to the local disk.

Troubleshooting Tips

If you do not know the Subject Common Name (CN) of the root certificate, you can use an external certificate management tool to find out. On Windows operating system, you can right-click the certificate file with a .cer extension and open the certificate properties.

What To Do Next

Uploading the Root Certificate onto Cisco Unified Presence for Remote Call Control

Uploading the Root Certificate onto Cisco Unified Presence for Remote Call Control

Before You Begin

Download the Root Certificate from the CA Server.

Procedure

1. Copy the certnew.cer file to the local computer that you use to administer the Cisco Unified Presence server.

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

3. Select **Upload Certificate**.

4. Select **sipproxy-trust** from the Certificate Name menu.

    Note: Leave the Root Name field blank.

5. Select **Browse**.

6. Locate the certnew.cer file on your local computer.

    Note: You may need to change the certificate file to a .pem extension.

7. Select **Upload File**.

Tip: Make a note of the new CA certificate filename you have uploaded to the sipproxy-trust using the Certificate Management Find screen. This certificate filename (without the .pem or .der extension) is the value you enter in the 'Root CA' field when uploading the CA-signed SIP proxy certificate.

What To Do Next

Generating a Certificate Signing Request for Cisco Unified Presence for Remote Call Control

Generating a Certificate Signing Request for Cisco Unified Presence for Remote Call Control

Before You Begin

Upload the Root Certificate onto Cisco Unified Presence.

Procedure

1. Select **Cisco Unified Operating System Administration > Security > Certificate Management**.
2. Select **Generate CSR**.
3. Select **sipproxy** from the Certificate Name menu.

4. Select **Generate CSR**.

What To Do Next

Downloading the Certificate Signing Request from Cisco Unified Presence for Remote Call Control

Downloading the Certificate Signing Request from Cisco Unified Presence for Remote Call Control

Before You Begin

Generate a Certificate Signing Request for Cisco Unified Presence.

Procedure

1. Select **Cisco Unified Operating System Administration > Security > Certificate Management**.
2. Select **Download CSR**.
3. Select **sipproxy** from the Certificate Name menu.
4. Select **Download CSR**.
5. Select Save to save the sipproxy.csr file to your local computer.

What To Do Next

Submitting the Certificate Signing Request on the CA Server for Remote Call Control

Submitting the Certificate Signing Request on the CA Server for Remote Call Control

Before You Begin

Download the Certificate Signing Request from Cisco Unified Presence.

Procedure

1. Copy the certificate request file sipproxy.csr to your CA server.

2. Open the URL **http://local-server/certserv or http://127.0.0.1/certsrv**.

3. Select **Request a certificate**.

4. Select **Advanced certificate request**.

5. 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.

6. Using a text editor like Notepad, open the sipproxy self-certificate that you generated.

7. Copy all information from and including

   -----BEGIN CERTIFICATE REQUEST
   to and including
   END CERTIFICATE REQUEST-----

8. Paste the content of the certificate request into the Certificate Request text box.

9. Select **Submit**.

   The Request ID number displays.

10. Open Certificate Authority in Administrative Tools.

    The Certificate Authority window displays the request you just submitted under Pending Requests.

11. Right-click on your certificate request.

12. Select **All Tasks > Issue**.

13. Select Issued certificates and verify that your certificate has been issued.

What To Do Next

Downloading the Signed Certificate from the CA Server for Remote Call Control

Downloading the Signed Certificate from the CA Server for Remote Call Control

Before You Begin

Submit the Certificate Signing Request on the CA Server.

Procedure

1. Open http://<local_server>/certsrv on the Windows server that CA is running on.
2. Select **View the status of a pending certificate request**.
3. Select the option to view the request that was just submitted.
4. Select **Base 64 encoded**.
5. Select **Download certificate**.
6. Save the signed certificate to the local disk
7. Rename the certificate sipproxy.pem.
8. Copy the sipproxy.pem file to your local computer.

What To Do Next

Uploading the Signed Certificate to Cisco Unified Presence for Remote Call Control

Uploading the Signed Certificate to Cisco Unified Presence for Remote Call Control

Before You Begin

Download the Signed Certificate from the CA Server.

Procedure

1. Select **Cisco Unified Operating System Administration > Security > Certificate Management**.
2. Select **Upload Certificate**.
3. Select **sipproxy** from the Certificate Name menu.
4. Specify the root certificate name. The root certificate name must contain the .pem or .der extension.
5. Select **Browse**.
6. Locate the signed sipproxy.pem certificate on your local computer.
7. Select **Upload File**.

What To Do Next

- How to Configure the Security Certificate for Microsoft OCS