Security Certificate Configuration for IM and Presence Service

This topic is only applicable if you require a secure connection between IM and Presence Service and Microsoft OCS.

This topic describes how to configure security certificates using a standalone CA. If you use an enterprise CA, refer to the *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager* for an example of the certificate exchange procedure using an enterprise CA.

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

Configure Standalone Root Certificate Authority (CA)

Procedure

Step 1 Sign in to the CA server with Domain Administrator privileges.

Step 2 Insert the Windows Server 2003 CD.

Step 3 Select**Start** > **Settings** > **Control Panel**.

Step 4 Double-click **Add or Remove Programs**.

Step 5 Click **Add/Remove Windows Components**.

Step 6 Select **Application Server**.

Step 7 Select **Internet Information Services (IIS)**.

Step 8 Complete the installation procedure.

Step 9 Click **Add/Remove Windows Components**.

Step 10 Select **Certificate Services**.

Step 11 Click **Next**.

Step 12 Select **Standalone root CA**.

Step 13 Click **Next**.

Step 14 Type the name of the CA root.

Note This name can be a friendly name for the CA root in the forest root.

Step 15 Change the time to the number of years required for this certificate.

Step 16 Click **Next** to begin installation.

Step 17 Select the location for the certificate database and the certificate database files.

Step 18 Click **Next**.

Step 19 Click **Yes** when prompted to stop IIS.

Step 20 Click **Yes** when prompted with a message regarding Active Server Pages.

Step 21 Click **Finish**.

What to Do Next

Download Root Certificate from CA Server, on page 2.

Download Root Certificate from CA Server

Before You Begin

Configure the Standalone Root Certificate Authority.

Procedure

Step 1 Sign in to your CA server and open a web browser.

Step 2 Open the URL **http://<ca_server_IP_address>/certsrv**.

Step 3 Click on **Download a CA certificate, certificate chain, or CRL**.

Step 4 Click **Base 64** for the Encoding Method.

Step 5 Click **Download CA Certificate**.

Step 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

Upload Root Certificate onto IM and Presence Service, on page 3

Related Topics

Configure Standalone Root Certificate Authority (CA), on page 2

Upload Root Certificate onto IM and Presence Service

Before You Begin

Download the Root Certificate from the CA Server.

Procedure

Step 1 Copy the certnew.cer file to the local computer that you use to administer the IM and Presence Service node.

Step 2 Select **Cisco Unified IM and Presence Operating System Administration** > **Security** > **Certificate Management**.

Step 3 Click **Upload Certificate**.

Step 4 Select **cup-trust** from the Certificate Name menu.

Note Leave the Root Name field blank.

Step 5 Click **Browse**.

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

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

Step 7 Click **Upload File**.

Tip Make a note of the new CA certificate filename you have uploaded to the cup-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

Generate a Certificate Signing Request for IM and Presence Service, on page 4

Related Topics

Download Root Certificate from CA Server, on page 2
Upload Signed Certificate to IM and Presence Service, on page 6

Generate a Certificate Signing Request for IM and Presence Service

Before You Begin

Upload the Root Certificate onto IM and Presence Service.

Procedure

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

Step 2 Click **Generate CSR**.

Step 3 Select **cup** from the Certificate Name menu.

Step 4 Click **Generate CSR**.

What to Do Next

Download Certificate Signing Request from IM and Presence Service, on page 4

Related Topics

Upload Root Certificate onto IM and Presence Service, on page 3

Download Certificate Signing Request from IM and Presence Service

Before You Begin

Generate a Certificate Signing Request for IM and Presence Service.

Procedure

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

Step 2 Click **Download CSR**.

Step 3 Select **cup** from the Certificate Name menu.

Step 4 Click **Download CSR**.

Step 5 Click **Save** to save the cup.csr file to your local computer.

What to Do Next

Submit Certificate Signing Request on CA Server, on page 5

Related Topics

Generate a Certificate Signing Request for IM and Presence Service, on page 4

Submit Certificate Signing Request on CA Server

Before You Begin

Download the Certificate Signing Request from IM and Presence Service.

Procedure

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

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

Step 3 Click **Request a certificate**.

Step 4 Click **Advanced certificate request**.

Step 5 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 6 Using a text editor like Notepad, open the cup self-certificate that you generated.

Step 7 Copy all information from and including
-----BEGIN CERTIFICATE REQUEST

to and including

END CERTIFICATE REQUEST-----

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

Step 9 Click **Submit**.
The Request ID number displays.

Step 10 Open **Certificate Authority** in Administrative Tools.
The Certificate Authority window displays the request you just submitted under Pending Requests.

Step 11 Right-click on your certificate request.

Step 12 Select **All TasksIssue**.

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

What to Do Next

Download Signed Certificate from CA Server, on page 6

Related Topics

Download Certificate Signing Request from IM and Presence Service, on page 4

Download Signed Certificate from CA Server

Before You Begin

Submit the Certificate Signing Request on the CA Server.

Procedure

Step 1 Open **http://<local_server>/certsrv** on the Windows server that CA is running on.

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

Step 3 Select the option to view the request that was just submitted.

Step 4 Click **Base 64 encoded**.

Step 5 Click **Download certificate**.

Step 6 Save the signed certificate to the local disk

Step 7 Rename the certificate **cup.pem**.

Step 8 Copy the cup.pem file to your local computer.

What to Do Next

Upload Signed Certificate to IM and Presence Service, on page 6

Related Topics

Submit Certificate Signing Request on CA Server, on page 5

Upload Signed Certificate to IM and Presence Service

Before You Begin

Download the Signed Certificate from the CA Server.

Procedure

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

Step 2 Click **Upload Certificate**.

Step 3 Select **cup** from the Certificate Name menu**.**

Step 4 Specify the root certificate name. The root certificate name must contain the .pem or .der extension.

Step 5 Click **Browse**.

Step 6 Locate the signed **cup.pem** certificate on your local computer.

Step 7 Click **Upload File**.

What to Do Next

Security Certificate Configuration for Microsoft OCS

Related Topics

Download Signed Certificate from CA Server, on page 6