Security Certificate Setup for IM and Presence Service

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

This chapter describes how to configure security certificates using a standalone CA. If you use an enterprise CA, see 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.

Set Up Standalone Root Certificate Authority (CA)

Complete the following procedure to configure the standalone root 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** and double-click **Add or Remove Programs**.

Step 4 Select **Add/Remove Windows Components**.

Step 5 Select **Application Server**, then select **Internet Information Services (IIS)**.

Step 6 Complete the installation procedure.

Step 7 Select **Add/Remove Windows Components**.

Step 8 Select **Certificate Services**, then select **Next**.

Step 9 Select **Standalone root CA**, then select **Next**.

Step 10 Type the name of the CA root.

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

Step 11 Change the time to the number of years required for this certificate and select **Next** to begin installation.

Step 12 Select the location for the certificate database and the certificate database files.

Step 13 Select **Next**.

Step 14 Select **Yes** when prompted to stop IIS.

Step 15 Select **Yes** when prompted with a message regarding Active Server Pages, then select **Finish**.

What to do next

Download Root Certificate from CA Server, on page 2.

Download Root Certificate from CA Server

Complete the following procedure to download the root certificate from the 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 Select on Download a CA certificate, certificate chain, or CRL.

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

Step 5 Select **Download CA Certificate**.

Step 6 Save the certificate file certnew.cer to the local disk.

Important 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 a 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 to IM and Presence Service, on page 3

Related Topics

Set Up Standalone Root Certificate Authority (CA), on page 1

Upload Root Certificate to IM and Presence Service

Complete the following procedure to upload the 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.

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

Step 3 Select **Upload Certificate**.

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

Note Leave the **Root Name** field blank.

Step 5 Select Browse and locate the certnew.cer file on your local computer.

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

Step 6 Select 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 Certificate Signing Request for IM and Presence Service, on page 3

Related Topics

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

Generate Certificate Signing Request for IM and Presence Service

Complete the following procedure to generate a Certificate Signing Request (CSR) for IM and Presence Service.

Before you begin

Upload the Root Certificate onto IM and Presence Service.

Procedure

Step 1 Select Cisco Unified Operating System **Administration** > **Security** > **Certificate Management**.
Step 2 Select **Generate CSR**.
Step 3 Select cup from the **Certificate Name** menu.
Step 4 Select **Generate CSR**.

What to do next

Download CSR from IM and Presence Service, on page 4

Related Topics

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

Download CSR from IM and Presence Service

Complete the following procedure to download the CSR from IM and Presence Service.

Before you begin

Generate a CSR for IM and Presence Service.

Procedure

Step 1 Select Cisco Unified Operating System **Administration** > **Security** > **Certificate Management**.
Step 2 Select **Download CSR**.
Step 3 Select cup from the **Certificate Name** menu.
Step 4 Select **Download CSR**.
Step 5 Select **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 Certificate Signing Request for IM and Presence Service, on page 3

Submit Certificate Signing Request on CA Server

Complete the following procedure to submit the CSR on the CA server.

Before you begin

Download the CSR 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 Select **Request a certificate**, then select **Advanced certificate request**.

Step 4 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 5 Using a text editor like Notepad, open the cup self-certificate that you generated.

Step 6 Copy all information from and including

-----BEGIN CERTIFICATE REQUEST

to and including

END CERTIFICATE REQUEST-----

Step 7 Paste the content of the certificate request into the **Certificate Request** text box.

Step 8 Select **Submit**.

The Request ID number displays.

Step 9 Open Certificate Authority in Administrative Tools.

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

Step 10 Right-click on your certificate request and select **All TasksIssue.**

Step 11 Select Issued certificates and verify that your certificate has been issued.

What to do next

Download Signed Certificate from CA Server, on page 5

Related Topics

Download CSR from IM and Presence Service, on page 4

Download Signed Certificate from CA Server

Complete the following procedure to download the signed certificate from the CA server.

Before you begin

Submit the CSR on the CA Server.

Procedure

Step 1 Open `http://<local_server>/certsrv` on the Windows server that CA is running on.
Step 2 Select **View** the status of a pending certificate request.
Step 3 Select the option to view the request that was just submitted.
Step 4 Select **Base 64 encoded**.
Step 5 Select **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

Complete the following procedure to upload the signed certificate to IM and Presence Service.

Before you begin

Download the signed certificate from the CA Server.

Procedure

Step 1 Select Cisco Unified Operating System **Administration** > **Security** > **Certificate Management**.
Step 2 Select **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 Select **Browse** and locate the signed cup.pem certificate on your local computer.
Step 6 Select **Upload File**.

What to do next

Lync Remote Call Control Installation

Related Topics

Download Signed Certificate from CA Server, on page 5