CHAPTER 5

Configuring Secure Certificate Exchange between Cisco Unified Presence and Microsoft Exchange

Revised: November 30, 2012

Checklist for Managing Self-Signed and Third-Party Certificate Exchanges

Table 5-1 provides an overview of the steps for configuring secure certificate exchange for self-signed and third-party certificates.

Table 5-1 Self-signed and Third-party Certificate Checklist

Configuration Steps		Procedures To Complete This Configuration
Step 1	Install the Certificate CA Service	**Self-Signed Certificates** How to Install the Certificate Authority (CA) Service, page 5-3
Step 2	Generate a CSR on IIS of Exchange server	**Self-Signed Certificates** How to Generate a CSR on IIS of Exchange Server, page 5-6 **Third-Party Certificates** How to Generate a CSR on IIS of Exchange Server, page 5-6
Step 3	Submit the CSR to the CA Server/Certificate Authority	**Self-Signed Certificates** Submitting the CSR to the CA Server/Certificate Authority, page 5-10 **Third-Party Certificates** Request the CSR from your Certificate Authority.
Step 4	Download the signed certificate	**Self-Signed Certificates** Downloading the Signed Certificate, page 5-11 **Third-Party Certificates** Your Certificate Authority will provide you with the signed certificate.
Step 5	Upload the signed certificate onto Exchange IIS	**Self-Signed Certificates** How to Upload the Signed Certificate onto Exchange IIS, page 5-12 **Third-Party Certificates** How to Upload the Signed Certificate onto Exchange IIS, page 5-12
Step 6	Download the root certificate	**Self-Signed Certificates** Downloading the Root Certificate, page 5-14 **Third-Party Certificates** Request the root certificate from your Certificate Authority.
Step 7	Upload the root certificate to the Cisco Unified Presence server	**Self-Signed Certificates** Uploading the Root Certificate to the Cisco Unified Presence Server, page 5-14 **Third-Party Certificates** If you have a third-party CA-signed Exchange server certificate, note that you must upload *all* CA certificates in the certificate chain to Cisco Unified Presence as a Cisco Unified Presence Trust certificate (cup-trust).

How to Install the Certificate Authority (CA) Service

Although the CA can run on the Exchange server, we recommend that you use a different Windows server as a Certificate Authority (also known as CA) to provide extended security for third-party certificate exchanges.

Installing the CA on Windows Server 2003

Before You Begin

- In order to install the CA you must first install Internet Information Services (IIS) on a Windows Server 2003 computer. IIS is not installed with the default Windows 2003 installation.
- Ensure that you have Windows Server disc 1 and SP1 discs.

Procedure

Step 1 Select **Start > Control Panel > Add or Remove Programs**.

Step 2 Select **Add/Remove Windows Components** in the Add or Remove Programs window.

Step 3 Complete the Windows Components wizard:

Window	Configuration Steps
Windows Components Window Page 1 of	a. Check **Certificate Services** under Components. b. Select **Yes** when the Warning displays about domain membership and computer renaming constraints.
CA Type Window Page 2 of	a. Select **Stand-alone Root CA.** b. Select **Next**.
CA Identifying Information Window Page 3 of	a. Enter the name of the server in the Common Name field for the CA Server. If there is no DNS, type the IP address. b. Select **Next**.
Certificate Database Settings Window Page 4 of	a. Accept the defaults settings. b. Select **Next.**

Step 4 Select **Yes** when you are prompted to stop Internet Information Services.

Step 5 Select **Yes** when you are prompted to enable Active Server Pages (ASP).

Step 6 Select **Finish** after the installation process completes.

Troubleshooting Tips

Remember that the CA is a third-party authority. The common name of the CA should *not* be the same as the common name used to generate a CSR.

What To Do Next

Submitting the CSR to the CA Server/Certificate Authority, page 5-10, page 5-9

Installing the CA on Windows Server 2008

Procedure

Step 1 Select **Start > Administrative Tools > Server Manager**.

Step 2 Select **Roles** in the console tree.

Step 3 Select **Action > Add Roles**.

Step 4 Complete the Add Roles wizard:

Window	Configuration Steps
Before You Begin Window Page 1 of 13	a. Ensure that you have completed all prerequisites listed in the window. b. Select **Next.**
Select Server Roles Window Page 2 of 13	a. Check **Active Directory Certificate Services**. b. Select **Next.**
Introduction Window Page 3 of 13	Select **Next.**
Select Role Services Window Page 4 of 13	a. Check these check boxes: – Certificate Authority – Certificate Authority Web Enrollment – Online Responder b. Select **Next.**
Specify Setup Type Window Page 5 of 13	Select **Standalone**.
Specify CA Type Window Page 6 of 13	Select **Root CA.**
Set Up Private Key Window Page 7 of 13	Select **Create a new private key.**
Configure Cryptography for CA Window Page 8 of 13	Select the default cryptographic service provider.
Configure CA Name Window Page 9 of 13	Enter a common name to identify the CA.
Set Validity Period Window Page 10 of 13	Set the validity period for the certificate generated for the CA. **Note** The CA will issue valid certificates only to the expiration date that you specify.
Configure Certificate Database Window Page 11 of 13	Select the default certificate database locations.

Window	Configuration Steps
Confirm Installation Selections Window Page 12 of 13	Select **Install**.
Installation Results Window Page 13 of 13	**a.** Verify that the **Installation Succeeded** message displays for all components. **b.** Select **Close**. **Note** Active Directory Certificate Services is now listed as one of the roles on the Server Manager.

What To Do Next

How to Generate a CSR on IIS of Exchange Server, page 5-6

How to Generate a CSR on IIS of Exchange Server

Generating a CSR - Running Windows Server 2003

You must generate a Certificate Signing Request (CSR) on the IIS server for Exchange, which is subsequently signed by the CA server.

Before You Begin

[Self-signed Certificates] Install the certificate CA service if required.

Procedure

Step 1 From Administrative Tools, open **Internet Information Services**.

Step 2 Perform these actions in the Internet Information Services (IIS) Manager:

a. Right-click **Default Web Site**

b. Select **Properties**.

Step 3 Select the **Directory Security** tab.

Step 4 Select **Server Certificate**.

Step 5 Select **Next** when the Web Server Certificate Wizard window displays.

Step 6 Complete the Web Server Certificate Wizard:

Note If the Certificate has the Subject Alternative Name (SAN) field populated, it must match the Common Name (CN) of the certificate.

Window	Configuration Steps
Server Certificate Window Page 1 of 9	a. Select **Create a new certificate**. b. Select **Next.**
Delayed or Immediate Request Window Page 2 of 9	a. Select **Prepare the request now, but send it later**. b. Select **Next.**
Name and Security Settings Window Page 3 of 9	a. Accept the Default Web Site certificate name. b. Select **2048** for the bit length. c. Select **Next.**
Organization Information Window Page 4 of 9	a. Enter your Company name in the Organization field. b. Enter the organizational unit of your company in the Organizational Unit field. c. Select **Next.**
Your Site's Common Name Window Page 5 of 9	a. For Common Name, enter the Exchange Server hostname or IP address. **Note** The IIS certificate Common Name that you enter is used to configure the Presence Gateway on Cisco Unified Presence, and must be identical to the Host (URI or IP address) you are trying to reach. b. Select **Next**.
Geographical Information Window Page 6 of 9	a. Enter your geographical information, as follows: – Country/Region – State/province – City/locality b. Select **Next**.
Certificate Request File Name Window Page 7 of 9	a. Enter an appropriate filename for the certificate request and specify the path and file name where you want to save your CSR. b. Select **Next**. **Note** Make sure that you save the CSR without any extension (.txt) and remember where you save it because you will need to be able to find this CSR file later. Only use Notepad to open the file.
Request File Summary Window Page 8 of 9	a. Confirm that the information is correct in the Request File Summary window. b. Select **Next**.
Web Server Certificate Completion Window Page 9 of 9	Select **Finish**.

What To Do Next

Submitting the CSR to the CA Server/Certificate Authority, page 5-10

Generating a CSR - Running Windows Server 2008

You must generate a Certificate Signing Request (CSR) on the IIS server for Exchange, which is subsequently signed by the CA server.

Before You Begin

Procedure

Step 1 From Administrative Tools, open **Internet Information Services (IIS) Manager**.

Step 2 Select the Exchange Server under Connections in the left frame of the IIS Manager.

Step 3 Double-click **Server Certificates**.

Step 4 Select **Create Certificate Request** under Actions in the right frame of the IIS Manager.

Step 5 Complete the Request Certificate Wizard:

Window	Configuration Steps
Distinguished Name Properties Window Page 1 of 5	**a.** For Common Name, enter the Exchange Server hostname or IP address. **Note** The IIS certificate Common Name that you enter is used to configure the Presence Gateway on Cisco Unified Presence, and must be identical to the Host (URI or IP address) you are trying to reach. **b.** Enter your Company name in the Organization field. **c.** Enter the organizational unit that your company belongs to in the Organizational Unit field. **d.** Enter your geographical information, as follows: – City/locality – State/province – Country/Region **e.** Select **Next.**
Cryptographic Service Provider Properties Window Page 2 of 5	**a.** Accept the default Cryptographic service provider. **b.** Select **2048** for the bit length. **c.** Select **Next.**
Certificate Request File Name Window Page 3 of 5	**a.** Enter an appropriate filename for the certificate request. **b.** Select **Next**. **Note** Make sure that you save the CSR without any extension (.txt) and remember where you save it because you will need to be able to find this CSR file later. Only use Notepad to open the file.
Request File Summary Window Page 4 of 5	**a.** Confirm that the information is correct in the Request File Summary window. **b.** Select **Next**.
Request Certificate Completion Window Page 5 of 5	Select **Finish**.

What To Do Next

Submitting the CSR to the CA Server/Certificate Authority, page 5-10

Submitting the CSR to the CA Server/Certificate Authority

We recommend that the default SSL certificate, generated for Exchange on IIS, should use the Fully Qualified Domain Name (FQDN) of the Exchange server and be signed by a Certificate Authority that Cisco Unified Presence trusts. This procedure allows the CA to sign the CSR from Exchange IIS. Perform the following procedure on your CA server, and configure the FQDN of the Exchange server in the:

- Exchange certificate.
- Presence Gateway field of the Exchange Presence Gateway in Cisco Unified Presence Administration.

Before You Begin

Generate a CSR on IIS of the Exchange server.

Procedure

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

Step 2 Open one of the following URLs:

- Windows 2003 or Windows 2008: http://*local-server*/certserv

  or

- Windows 2003: *http://127.0.0.1/certserv*
  Windows 2008: *http://127.0.0.1/certsrv*

Step 3 Select **Request a certificate**.

Step 4 Select **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 CSR 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 CSR into the Certificate Request text box

Step 9 (Optional) By default the Certificate Template drop-down list defaults to the Administrator template, which *may or may not* produce a valid signed certificate appropriate for server authentication. If you have an enterprise root CA, select the “Web Server”certificate template from the Certificate Template drop-down list. The “Web Server” certificate template may not display, and therefore this step may not apply, if you have already modified your CA configuration.

Step 10 Select **Submit**.

Step 11 In Administrative Tools, select **Start > Administrative Tools > Certification > Authority >CA name > Pending request** to open the Certification Authority. The Certificate Authority window displays the request you just submitted under Pending Requests.

Step 12 Right click on your request, and complete these actions:

- Navigate to **All Tasks**.

- Select **Issue**.

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

What To Do Next

Downloading the Signed Certificate, page 5-11

Downloading the Signed Certificate

Before You Begin

[Self-signed Certificates] Submit the CSR to the CA server.

[Third-Party Certificates] Request the CSR from your Certificate Authority.

Procedure

Step 1 In Administrative Tools, open the Certification Authority. The Certificate Request that you just issued displays in Issued Requests.

Step 2 Right click the request and select **Open**.

Step 3 Select the **Details** tab.

Step 4 Select **Copy to File**.

Step 5 Select **Next** when the Certificate Export Wizard displays.

Step 6 Complete the Certificate Export Wizard:

Window	Configuration Steps
Export File Format Window Page 1 of 3	a. Select **Base-64 encoded X.509**. b. Select **Next.**
File to Export Window Page 2 of 3	a. Enter the location where you want to store the certificate and use **cert.cer** for the certificate name, for example, *c:\cert.cer* b. Select **Next.**
Certificate Export Wizard Completion Window Page 3 of 3	a. Review the summary information and verify that the export was successful. b. Select **Finish**.

Step 7 Copy or FTP the cert.cer to the computer that you use to administer Cisco Unified Presence.

What To Do Next

How to Upload the Signed Certificate onto Exchange IIS, page 5-12

How to Upload the Signed Certificate onto Exchange IIS

Uploading the Signed Certificate - Running Windows 2003

This procedure takes the signed CSR and uploads it onto IIS. To upload the signed certificate, perform the following step on the computer that you use to administer Cisco Unified Presence.

Before You Begin

[Self-signed Certificates] Download the signed certificate.

[Third-party Certificates] Your Certificate Authority will provide you with the signed certificate.

Procedure

Step 1 From Administrative Tools, open **Internet Information Services**.

Step 2 Complete the following steps in the Internet Information Services window:

a. Right click **Default Web Site**

b. Select **Properties**.

Step 3 Complete the following steps in the Default Web Site Properties window:

a. Select the **Directory Security** tab.

b. Select **Server Certificate**.

Step 4 Select **Next** when the Web Server Certificate Wizard window displays.

Step 5 Complete the Web Server Certificate Wizard:

Window	Configuration Steps
Pending Certificate Request Window Page 1 of 4	a. Select **Process the pending request and install the certificate.** b. Select **Next**.
Process a Pending Request Window Page 2 of 4	a. Select **Browse to** locate your certificate. b. Navigate to the correct path and filename. c. Select **Next.**
SSL Port Window Page 3 of 4	a. Enter **443** for the SSL port. b. Select **Next.**
Web Server Certificate Completion Window Page 4 of 4	Select **Finish**.

Troubleshooting Tips

If your certificate is not in the trusted certificates store, the signed CSR will not be trusted. To establish trust, Complete these actions:

- Select **View Certificate** in the Directory Security tab.
- Select **Details > Highlight root certificate,** and select **View**.
- Select the Details tab for the root certificate and install the certificate.

What To Do Next

Downloading the Root Certificate, page 5-14

Uploading the Signed Certificate - Running Windows 2008

This procedure takes the signed CSR and uploads it onto IIS. To upload the signed certificate, perform the following step on the computer that you use to administer Cisco Unified Presence.

Before You Begin

[Self-signed Certificates] Download the signed certificate.

[Third-party Certificates] Your Certificate Authority will provide you with the signed certificate.

Procedure

Step 1 From Administrative Tools, open **Internet Information Services (IIS) Manager**.

Step 2 Select the Exchange Server under Connections in the left frame of the IIS Manager.

Step 3 Double-click **Server Certificates**.

Step 4 Select **Complete Certificate Request** under Actions in the right frame of the IIS Manager.

Step 5 Complete these actions in the Specify Certificate Authority Response window:

a. Select the ellipsis **[...]** to locate your certificate.

b. Navigate to the correct path and filename.

c. Enter a user-friendly name for your certificate.

d. Select **Ok.** The certificate that you completed will display in the certificate list.

Step 6 Complete the following steps in the Internet Information Services window to bind the certificate:

a. Select **Default Web Site.**

b. Select **Bindings** under Actions in the right frame of the IIS Manager.

Step 7 Complete the following steps in the Site Bindings window:

a. Select **https**.

b. Select **Edit**

Step 8 Complete the following steps in the Edit Site Binding window:

a. Select the certificate that you just created from the SSL certificate list box. The "friendly name" that you applied to the certificate will display.

b. Select **Ok.**

What To Do Next

Downloading the Root Certificate, page 5-14

Downloading the Root Certificate

Before You Begin

Upload the Signed Certificate onto Exchange IIS.

Procedure

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

Step 2 Open the URL specific to your windows platform type:

- Windows server 2003 - http://127.0.0.1/certserv
- Windows server 2008 - https://127.0.0.1/certsrv

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

Step 4 For the Encoding Method, select **Base 64**.

Step 5 Select **Download CA Certificate**.

Step 6 Save the certificate, **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 this information. On a Windows operating system, right-click the certificate file with a .CER extension and open the certificate properties.

What To Do Next

Uploading the Root Certificate to the Cisco Unified Presence Server, page 5-14

Uploading the Root Certificate to the Cisco Unified Presence Server

Before You Begin

- [Self-signed Certificates] Download the root certificate.
- [Third-party Certificates] Request the root certificate from your Certificate Authority. If you have a third-party CA-signed Exchange server certificate, note that you must upload all CA certificates in the certificate chain to Cisco Unified Presence as a Cisco Unified Presence Trust certificate (cup-trust).

Procedure.

Step 1 Use the Certificate Import Tool in Cisco Unified Presence Administration to upload the certificate:

Upload the certificate via:	Actions
Certificate Import Tool in Cisco Unified Presence Administration. The Certificate Import tool simplifies the process of installing trust certificates on Cisco Unified Presence and is the primary method for certificate exchange. The tool allows you to specify the host and port of the Exchange server and attempts to download the certificate chain from the server. Once approved, the tool will automatically install missing certificates. **Note** This procedure describes one way to access and configure the Certificate Import Toolin Cisco Unified Presence Administration. You can also view a customized version of the Certificate Import Tool when you configure the Exchange Presence Gateway for a specific type of calendaring integration (select **Presence > Gateways**).	**a.** Select **System > Security > Certificate Import Tool** in Cisco Unified Presence Administration. **b.** Select **CUP Trust** as the Certificate Trust Store where you want to install the certificates. This stores the Presence Engine trust certificates required for Exchange Integration. **c.** Enter one of these values to connect with the Exchange server: – IP address – Host name – FQDN The value that you enter in this Peer Server field must exactly match the IP address, host name or FQDN of the Exchange server. **d.** Enter the port that is used to communicate with the Exchange server. This value must match the available port on the Exchange server. **e.** Select **Submit**. After the tool finishes, it reports these states for each test: – Peer Server Reachability Status—indicates whether or not Cisco Unified Presence can reach (ping) the Exchange server. See Troubleshooting Exchange Server Connection Status, page 6-1. – SSL Connection/Certificate Verification Status—indicates whether or not the Certificate Import Tool succeeded in downloading certificates from the specified peer server and whether or not a secure connection has been established between Cisco Unified Presence and the remote server. See Troubleshooting SSL Connection/Certificate Status, page 6-2.

Step 2 If the Certificate Import Tool indicates that certificates are missing (typically the CA cert is missing on Microsoft servers), manually upload the CA certificate(s) using the Cisco Unified OS Admin Certificate Management window

Upload the certificate via:	Actions
Cisco Unified Operating System Administration If the Exchange server does not provide the CA certificates during the SSL/TLS handshake, you cannot use the Certificate Import Tool to import those certificates. In this case, you must manually import the missing certificates using the Certificate Management tool in Cisco Unified OS Administration (select Security > Certificate Management).	**a.** Copy or FTP the **certnew.cer** certificate file to the computer that you use to administer your Cisco Unified Presence server. **b.** From the Navigation menu on the Cisco Unified Presence Administration login window, select Cisco Unified OS Administration and select **Go**. **c.** Enter your username and password for Cisco Unified Operating System Administration and select **Login**. **d.** Select **Security > Certificate Management**. **e.** Select **Upload Certificate** in the Certificate List window. **f.** Complete these actions when the Upload Certificate pop-up window displays: – Select **cup-trust** from the Certificate Name list box. – Enter the root certificate name without any extension. **g.** Select **Browse** and select **certnew.cer**. **h.** Select **Upload File**.

Step 3 Return to the Certificate Import Tool (Step 1) and verify that all status tests succeed.

Step 4 Restart the Cisco UP Presence Engine and SIP Proxy service after you upload all Exchange trust certificates. Select **Cisco Unified Serviceability > Tools > Service Activation.**

Troubleshooting Tips

- Cisco Unified Presence allows you to upload Exchange server trust certificates with or without a Subject Common Name (CN).
- Note that Meeting Notification and Cisco IP Phone Messenger features will only work if your network integration is over WebDAV. These features are not supported with EWS integrations.
- If you use the Meeting Notification feature, you must restart the Presence Engine and SIP Proxy for all types of certificates. After you upload your certificates, go to Cisco Unified Serviceability and restart the Presence Engine first followed by the Proxy restart. Note that this can affect Calendaring connectivity.