Main page: Cisco Unified Presence, Release 7.x

Contents

Previous Topic

- Configuring Microsoft Active Directory for Integration with Cisco Unified Presence

While the certificate exchange process below applies to Windows 2003 and Windows 2008, note that some of the configuration procedures will differ depending on your platform.

- Installing the CA Service
- Downloading the Root Certificate
- Uploading the Root Certificate to the Cisco Unified Presence Server
- Generating a CSR on IIS of Exchange Server
- Submitting the CSR to the CA Server
- Downloading the Signed Certificate.
- Uploading the Signed Certificate onto Exchange IIS

Installing the CA Service

The Certificate Authority can be the same as the Exchange server. However, Cisco recommends you to use a different Windows server to run the CA.

- Installing the CA on Windows Server 2003
- Installing the CA on Windows Server 2008

Installing the CA on Windows Server 2003

Before You Begin

Ensure that you have Windows Server disc 1 and SP1 discs.

Procedure

1. Select **Start > Control Panel > Add or Remove Programs**.
2. Click **Add/Remove Windows Components** in the Add or Remove Programs window.
3. Check **Certificate Services** under Components.
4. Click **Yes** when the Warning displays about domain membership.
5. Perform the following actions in the CA Type window:
    1. Select **Stand-alone Root CA.**
    2. Click **Next**.
6. Perform the following actions in the CA Identifying Information window:
7. Enter the name of the server in the Common Name field for the CA Server. If there is no DNS, type the IP address.
8. Click **Next**.
9. Accept the defaults settings in the Certificate Database Settings window, and click **Next**.
10. Click **Yes** when you are prompted to stop Internet Information Services.
11. Click **Yes** when you are prompted to enable Active Server Pages (ASP).
12. Click **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.

Related Topics

- Prerequisites for this Integration

What To Do Next

Downloading the Root Certificate

Installing the CA on Windows Server 2008

Procedure

1. Select **Start > Administrative Tools > Server Manager**.
2. Click **Roles** in the console tree.
3. Select **Action > Add Roles**.
4. Perform the following actions to complete the Add Roles wizard:

Window	Configuration Steps
Before You Begin Window	1. Ensure that you have completed all prerequisites listed in the window.

Page 1 of 13	2. Click **Next**.
Select Server Roles Window Page 2 of 13	1. Check **Active Directory Certificate Services**. 2. Click **Next**.
Introduction Window Page 3 of 13	Click **Next**.
Select Role Services Window Page 4 of 13	1. Check these check boxes: ◊ Certificate Authority ◊ Certificate Authority Web Enrollment ◊ Online Responder 2. Click **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 specified expiration date.
Configure Certificate Database Window Page 11 of 13	Select the default certificate database locations.
Confirm Installation Selections Window	Click **Install**.

Page 12 of 13	
Installation Results Window Page 13 of 13	1. Verify that the **Installation Succeeded** message displays for all components. 2. Click **Close**. **Note:** Active Directory Certificate Services is now listed as one of the roles on the Server Manager.

Related Topics

- Prerequisites for this Integration

What To Do Next

Downloading the Root Certificate

Downloading the Root Certificate

Before You Begin

Install the CA service.

Procedure

1. Log in to your CA server and open a web browser. 2. Open the URL specific to your windows platform type:

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

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

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

5. Select **Download CA Certificate**.

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.

Related Topics

- Installing the CA Service
- Getting More Information

What To Do Next

Uploading the Root Certificate to the Cisco Unified Presence Server

Uploading the Root Certificate to the Cisco Unified Presence Server

Cisco Unified Presence allows you to upload Exchange server trust certificates with or without a Subject Common Name (CN).

Before You Begin

- Download the root certificate.
- 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 Presence Engine (PE) trust certificate.

Procedure

1. Complete the steps based on your choice of upload method:

If a certificate is:	Upload the certificate via:	Actions
Not yet uploaded, and has no Subject CN	Presence Gateway window in Cisco Unified Presence Administration **Note:** You can upload any number of root CA certificates but you must upload five certificates at a time.	1. Select **Presence > Gateways**. 2. Click **Add New** in the Find and List Presence Gateways window. 3. Enter the appropriate value in the Trust Certificate Subject CN field. Ensure that the IIS certificate Subject CN is the same as the Host (URI or IP address) you are trying to reach. This parameter is subsequently used in the configuration of the presence gateway. 4. Perform one of the following actions in the Upload Certificate(s) field.

		• Enter the full path of the file(s) that you want to upload. • Click **Browse** to locate the file(s) that you require.
Already uploaded, and has a Subject CN	Cisco Unified Operating System Administration	1. Copy or FTP the **certnew.cer** certificate file to the computer that you use to administer your Cisco Unified Presence server. 2. From the Navigation menu on the Cisco Unified Presence Administration login window, select Cisco Unified OS Administration and click **Go**. 3. Enter your username and password for Cisco Unified Operating System Administration and click **Login**. 4. Select **Security > Certificate Management**. 5. Click **Upload Certificate** in the Certificate List window. 6. Perform the following actions when the Upload Certificate pop-up window displays: • Select **Presence Engine Trust** from the Certificate Name list box. • Enter the root certificate name without any extension. 7. Click **Browse** and select **certnew.cer**. 8. Click **Upload File**.

2. Restart the Presence Engine and SIP Proxy service after you upload all Exchange trust certificates.

Troubleshooting Tips

You must restart the Presence Engine and SIP Proxy for all types of certificates if the Meeting Notification feature is used. After you upload your certificates, go to Cisco Unified Serviceability and restart the Presence Engine first followed by the Proxy restart.

Related Topics

- Downloading the Root Certificate
- Getting More Information
- Configuring a Presence Gateway on the Cisco Unified Presence Server

What To Do Next

Generating a CSR on IIS of Exchange Server

Generating a CSR on IIS of Exchange Server

Generating a CSR - Running Window Server 2003

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

Before You Begin

Upload the root certificate to Cisco Unified Presence.

Procedure

1. From Administrative Tools, open **Internet Information Services**.\
2. Complete the following steps in the Internet Information Services window:
    1. Right-click **Default Web Site**
    2. Select **Properties**.
3. Complete the following steps in the Default Web Site Properties window:
    1. Select the **Directory Security** tab.
    2. Click **Server Certificate**.
4. Click **Next** when the Web Server Certificate Wizard window displays.
5. Perform the following actions to complete the Web Server Certificate Wizard:

Window	Configuration Steps
Server Certificate Window Page 1 of 9	1. Select **Create a new certificate**. 2. Click **Next**.
Delayed or Immediate Request Window Page 2 of 9	1. Select **Prepare the request now, but send it later**. 2. Click **Next.**
Name and Security Settings Window Page 3 of 9	1. Accept the Default Web Site certificate name. 2. Select **1024** for the bit length.# Click **Next**.
Organization Information Window	1. Enter your Company name in the Organization field.

Page 4 of 9	2. Enter the organizational unit of your company in the Organizational Unit field. 3. Click **Next**.
Your Site's Common Name Window Page 5 of 9	1. 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. 2. Click **Next**.
Geographical Information Window Page 6 of 9	1. Enter your geographical information, as follows: ◊ Country/Region ◊ State/province ◊ City/locality 2. Click **Next**.
Certificate Request File Name Window Page 7 of 9	1. Enter an appropriate filename for the certificate request. 2. Click **Next**. **Note:** Make sure that you save the CSR without any extension and only use Notepad to open the file.
Request File Summary Window Page 8 of 9	1. Review your information about the Request File Summary window. 2. Click **Next**.
Web Server Certificate Completion Window Page 9 of 9	Click **Finish**.

Related Topics

- Uploading the Root Certificate to the Cisco Unified Presence Server
- Getting More Information

What To Do Next

Submitting the CSR to the CA Server

Generating a CSR - Running Window Server 2008

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

Before You Begin

Upload the root certificate to Cisco Unified Presence.

Procedure

1. From Administrative Tools, open **Internet Information Services (IIS) Manager**.
2. Select the Exchange Server under Connections in the left frame of the IIS Manager.
3. Double-click **Server Certificates**.
4. Select **Create Certificate Request** under Actions in the right frame of the IIS Manager.
5. Perform the following actions to complete the Request Certificate Wizard:

Window	Configuration Steps
Distinguished Name Properties Window Page 1 of 5	1. 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. 2. Enter your Company name in the Organization field. 3. Enter the organizational unit that your company belongs to in the Organizational Unit field. 4. Enter your geographical information, as follows: ◊ City/locality ◊ State/province ◊ Country/Region 5. Click **Next**.
Cryptographic Service Provider Properties Window Page 2 of 5	1. Accept the default Cryptographic service provider. 2. Select **1024** for the bit length. 3. Click **Next**.
Certificate Request File Name Window Page 3 of 5	1. Enter an appropriate filename for the certificate request. 2. Click **Next**. **Note:** Make sure that you save the CSR without any extension and only use Notepad to open the file.
Request File Summary Window Page 4 of 5	1. Confirm that the information is correct in the Request File Summary window. 2. Click **Next**.
Request Certificate Completion Window	Click **Finish**.

Related Topics

- Getting More Information

What To Do Next

Submitting the CSR to the CA Server

Submitting the CSR to the CA Server

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 is trusted by Cisco Unified Presence. 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.
- Outlook Gateway field in Cisco Unified Presence Administration.

Before You Begin

Generate a CSR on IIS of the Exchange server.

Procedure

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

2. Open the following URL:

   http://*local-server*/certserv
   or
   http://127.0.0.1/certsrv

3. Select **Request a certificate**.

4. Select **advanced certificate request**.

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**.

6. Using a text editor like Notepad, open the CSR 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 CSR into the Certificate Request text box.

9. Click **Submit**.

10. 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.

11. Right-click on your request, and perform the following actions:

◊ Navigate to **All Tasks**.
◊ Select **Issue**.
◊ Click **Issued certificates** and verify that your certificate has been issued.

Related Topics

- Generating a CSR on IIS of Exchange Server
- Getting More Information

What To Do Next

Downloading the Signed Certificate.

Downloading the Signed Certificate

Before You Begin

Submit the CSR to the CA server.

Procedure

1. In Administrative Tools, open the Certification Authority. The Certificate Request that you just issued displays in Issued Requests.
2. Right click the request and select **Open**.
3. Click the **Details** tab.
4. Click **Copy to File**.
5. Click **Next** when the Certificate Export Wizard displays.

6. Perform the following actions to complete the **Certificate Export Wizard**:

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

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

Related Topics

- Submitting the CSR to the CA Server
- Getting More Information

What To Do Next

Uploading the Signed Certificate onto Exchange IIS

Uploading the Signed Certificate onto Exchange IIS

- Uploading the Signed Certificate - Running Windows 2003
- Uploading the Signed Certificate - Running Windows 2008

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

Download the signed certificate.

Procedure

1. From Administrative Tools, open **Internet Information Services**.
2. Complete the following steps in the Internet Information Services window:
    1. Right click **Default Web Site**
    2. Select **Properties**.
3. Complete the following steps in the Default Web Site Properties window:
    1. Select the **Directory Security** tab.
    2. Click **Server Certificate**.
4. Click **Next** when the Web Server Certificate Wizard window displays.
5. Perform the following actions to complete the Web Server Certificate Wizard:

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

Troubleshooting Tips

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

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

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

Download the signed certificate.

Procedure

1. From Administrative Tools, open **Internet Information Services (IIS) Manager**.
2. Select the Exchange Server under Connections in the left frame of the IIS Manager.
3. Double-click **Server Certificates**.
4. Select **Complete Certificate Request** under Actions in the right frame of the IIS Manager.
5. Perform the following actions in the Specify Certificate Authority Response window:
    1. Click **the ellipsis '***[...]* **'to** locate your certificate.
    2. Navigate to the correct path and filename.
    3. Enter a user-friendly name for your certificate.
    4. Click **Ok**. The certificate that you completed will display in the certificate list.
6. Complete the following steps in the Internet Information Services window to bind the certificate:
    1. Click **Default Web Site.**
    2. Select **Bindings** under Actions in the right frame of the IIS Manager.
7. Complete the following steps in the Site Bindings window:
    1. Select **https**.
    2. Click **Edit**.
8. Complete the following steps in the Edit Site Binding window:
    1. Select the certificate that you just created from the SSL certificate list box. The "friendly name" that you applied to the certificate will display.
    2. Click **Ok**.

Related Topics

- Downloading the Signed Certificate
- Getting More Information