CHAPTER 5

Configuring Cisco Unified Presence for Integration with Microsoft Exchange Server

Revised: November 28, 2013

Configuring the Presence Gateway on Cisco Unified Presence for Microsoft Exchange Integration

You must configure an Exchange Server (Microsoft Outlook) as a Presence Gateway for calendaring information exchange. The Presence Gateway to Exchange enables the Cisco Unified Presence Server to reflect the availability information (calendar/meeting status) status of the user on a per-user basis.

When you configure the presence gateway, you can use one of the following values to connect the Exchange Server:

- FQDN (resolvable by DNS)
- IP address

Note For an overview of each type of Exchange integration, we recommend that you review Chapter 2, "Planning for Cisco Unified Presence Integration with Microsoft Exchange".

When configuring your EWS Presence Gateway for Exchange integration in Cisco Unified Presence Administration, note the following:

- You cannot deploy a mixed environment of WebDAV and EWS servers. You must either configure a single WebDAV Server or one or more EWS Server gateways but not both.
- You can add, update or delete *one or more* EWS servers with no maximum limit. However, the Troubleshooter on the Presence Gateway window is designed to only verify and report status of the first 10 EWS servers that you configure.
- EWS Server gateways share the Impersonation Account credentials (Account Name and Password) that you configure for the first EWS Server gateway. If you change the credentials for one EWS Server gateway, the credentials change accordingly on *all* of the configured EWS gateways.
- You must restart the Cisco UP Presence Engine *after* you add, update or delete one or more EWS servers for your configuration changes to take effect. If you add multiple EWS Servers one after another, you can restart the Cisco UP Presence Engine once to effect all your changes simultaneously.

Note

- For SAN certificates, the protected host must be contained in the list of hostnames/IP addresses in the Subject Alternative Name field.
- When you are configuring the presence gateway, the Presence Gateway field must exactly match the protected host listed in the Subject Alternative Name field.

Configuring Microsoft Exchange as a Presence Gateway (WebDAV)

Before You Begin

Before you configure a Presence Gateway, you must upload a valid certificate chain to Cisco Unified Presence.

Procedure

Step 1 Log in to **Cisco Unified Presence Administration**.

Step 2 Choose **Presence > Gateways**.

Step 3 Click **Add New**.

Step 4 To integrate Exchange Server 2003 or 2007 over WebDAV, choose **Exchange -- WebDAV** for the Presence Gateway type.

Note For the configuration changes to take effect, you must restart the Cisco UP Presence Engine after you add, update, or delete a WebDAV Server or multiple Exchange Web Services (EWS) servers. However, you cannot mix WebDAV and EWS server types in your deployment. If you add multiple EWS servers one after another, you can restart the Cisco UP Presence Engine once to effect all your changes simultaneously.

Step 5 In the Description field, enter a meaningful description that helps you to distinguish between Presence Gateway instances when you have configured more than one type of gateway.

Step 6 For the Presence Gateway field, enter the server location for the Presence Gateway and ensure that it matches the subject Common Name (CN) or is present in the SAN field of the IIS certificate of the Exchange Server. One of these values must be used to connect with the Exchange Server:

- FQDN
- IP address

To configure a Presence Gateway for use with a Wildcard Certificate, the server location value that you specify must be part of the subdomain protected by the Wildcard Certificate. For example, if a Wildcard Certificate protects the subdomain *.cup.cisco.com, you must enter a node location value of *server_name*.cup.cisco.com in the Presence Gateway field.

Note If you enter a FQDN, it must match the Subject Common Name (CN) or match one of the protected hosts in the Subject Alternative Name field on the Exchange Server leaf certificate in the certificate chain. The FQDN must resolve to the address that services the request and uses the certificate.

Step 7 For the Account Name field, enter the name of the Receive As account that Cisco Unified Presence uses to connect to the Exchange Server, in this format: *domain\username*, bearing in mind the following:.

- If the Exchange Server is configured to specify a default domain, it may not be necessary to include the domain as part of the user name.
- Otherwise, specify the domain in front of the account name to avoid potential certificate errors (401 and 404 authentication responses).

Step 8 Enter the Exchange Account Password required for Cisco Unified Presence to connect to the Exchange Server. Enter the password again to confirm it. This value must match the Account Password of the previously configured account on the Exchange Server.

Step 9 Enter the port that is used to connect with the Exchange Server. Cisco Unified Presence integration with Exchange must occur over a secure HTTP connection. We recommend you to use port 443 (default port) and not to change to other ports.

Step 10 Click **Save**.

Step 11 Confirm the Exchange Server status is showing green for:

- **Ensure Exchange Reachability (pingable)**
- **Exchange SSL Connection/Certification Verification.**

Note Before Cisco Unified Presence Release 8.6, when you add, change or delete any exchange gateway, calendaring turns off for every user in the cluster. In Cisco Unified Presence, Release 8.6, the bulk disabling of user calendaring only happens when you delete the WebDAV gateway or the last EWS gateway.

Configuring Microsoft Exchange as a Presence Gateway (EWS)

Procedure

Step 1 Log in to **Cisco Unified Presence Administration**.

Step 2 Choose **Presence > Gateways**.

Step 3 Click **Add New**.

Step 4 To integrate Exchange Server 2007 or 2010 over Exchange Web Services (EWS), choose **Exchange -- EWS Server** for the Presence Gateway Type. For configuration changes to take effect, you must restart the Cisco UP Engine after you add, update, or delete one or more EWS servers. If you add multiple EWS servers one after another, you can restart the Cisco Presence Engine once to effect all your changes simultaneously.

Step 5 Enter a meaningful description in the Description field that helps you to distinguish between Presence Gateway instances when you have configured more than one type of gateway.

Step 6 For the Presence Gateway field, enter the server location for the Presence Gateway, and ensure that it matches the subject Common Name (CN) or is present in the SAN field of the IIS certificate of the Exchange Server. One of these values must be used to connect with the Exchange Server:

- FQDN
- IP address

To configure a Presence Gateway for use with a Wildcard Certificate, the node location value that you specify must be part of the subdomain protected by the Wildcard Certificate. For example, if a Wildcard Certificate protects the subdomain *.cup.cisco.com, you must enter a node value of server_name.cup.cisco.com in the Presence Gateway field.

Note If you enter a FQDN, it must match the Subject Common Name (CN) or match one of the protected hosts in the Subject Alternative Name field on the Exchange Server leaf certificate in the certificate chain. The FQDN must resolve to the address that services the request and uses the certificate.

Step 7 Enter the name of the Impersonation account that Cisco Unified Presence uses to connect to the Exchange Server, either in the form of a User Principal Name (for example, user@domain) or in the form of a Down-Level Logon Name (for example, domain\user).

Step 8 Enter the Exchange Account Password required for Cisco Unified Presence to connect to the Exchange Server. Enter the password again to confirm it. This value must match the Account Password of the previously configured account on the Exchange Server.

Step 9 Enter the port that is used to connect with the Exchange Server. Cisco Unified Presence integration with Exchange must occur over a secure HTTP connection. We recommend you to use port 443 (default port) and not to change to other ports.

Step 10 Click **Save**.

Step 11 Confirm the Exchange Server status is showing green for:

- **Ensure Exchange Reachability (pingable)**
- **Exchange SSL Connection/Certification Verification.**
- **Account Name and Password Validation**

Note Before Cisco Unified Presence Release 8.6, when you add, change or delete any exchange gateway, calendaring turns off for every user in the cluster. In Cisco Unified Presence Release 8.6, the bulk disabling of user calendaring only happens when you delete the WebDAV gateway or the last EWS gateway.

What To Do Next

After you configure the Exchange Presence Gateway, verify the following:

1. Did the connection between Cisco Unified Presence and the Exchange Server succeed? The Troubleshooter on the Presence Gateway configuration window reports the connection status. If you must take corrective action, see Troubleshooting Exchange Server Connection Status, page 6-1.
2. Is the status of the Exchange SSL certificate chain correct (Verified)? The Exchange Server Status area on the Presence Gateway Configuration window indicates if there is a certificate Subject CN mismatch. If you must take corrective actions, see Troubleshooting SSL Connection/Certificate Status, page 6-2.
3. Are the Account Name and Password credentials correct (Authenticated)? The Exchange Server Status area on the Presence Gateway Configuration window reports the validation of the impersonation account username and password credentials. If you need to take corrective action, see Troubleshooting Account Name and Password, page 6-4.
4. [Optional] Do desk phones enabled with Cisco IP Phone Messenger display the scheduled meetings of users? For more information, see Troubleshooting Account Name and Password, page 6-4.

SAN and Wildcard Certificate Support

Cisco Unified Presence uses X.509 certificates for secure calendaring integration with Exchange.

From Release 8.6(4) onwards, Cisco Unified Presence supports SAN (Subject Alternative Name) and wildcard certificates, along with standard certificates. For information about certificate compatibility for Cisco Unified Presence Release 8.6(3) and earlier, see SAN and Wildcard Certificate Compatibility - Pre Release 8.6(4), page 5-6.

SAN certificates allow multiple hostnames and IP addresses to be protected by a single certificate, by specifying a list of hostnames and/or IP addresses in the X509v3 Subject Alternative Name field.

Note For SAN certificates, the protected host must be contained in the list of hostnames/IP addresses in the Subject Alternative Name field. When you are configuring the presence gateway, the Presence Gateway field must exactly match the protected host listed in the Subject Alternative Name field.

Wildcard certificates allow a domain and unlimited sub-domains to be represented by specifying an asterisk (*) in the domain name. Names may contain the wildcard character * which is considered to match any single domain name component. For example, ***.a.com** matches **foo.a.com** but not **bar.foo.a.com**.

Note Wildcards can be placed in the Common Name (CN) for standard certificates, and in the Subject Alternative Name for SAN certificates.

SAN and Wildcard Certificate Compatibility - Pre Release 8.6(4)

Cisco Unified Presence uses X.509 certificates for secure calendaring integration with Exchange. Cisco Unified Presence only supports standard certificates, no Subject Alternative Name field or wildcard entries are allowed. It is still possible to use SAN and/or Wildcard certificates with the following caveat, when using SAN/Wildcard certificates, there are some scenarios where the **Exchange Server Status** on the **Presence Gateway Configuration** window reports a **Subject CN Mismatch**, but calendaring integration continues to work.

Table 5-1 lists and describes the certificate types that Cisco Unified Presence supports for calendaring integration with Exchange.

Table 5-1 Cisco Unified Presence SAN and Wildcard Certificates —Backwards Compatibility

X.509 Certificate Type	Description	Caveats
Standard	Presence gateway hostname/IP address contained in **Subject Common Name**.	None
Standard/Wildcard	Presence gateway subdomain wildcard contained in **Subject Common Name**.	**Presence Gateway Configuration Exchange Server Status** reports Subject CN Mismatch error.
SAN	Presence gateway hostname/IP address contained in both **Subject Common Name** and **Subject Alternative Name**.	None
SAN	Presence gateway hostname/IP address contained in **Subject Alternative Name** only.	**Presence Gateway Configuration Exchange Server Status** reports **Subject CN Mismatch** error.
SAN/Wildcard	Presence gateway subdomain wildcard contained in **Subject Alternative Name** only.	**Presence Gateway Configuration Exchange Server Status** reports **Subject CN Mismatch** error.

Configuring Secure Certificate Exchange between Cisco Unified Presence and Microsoft Exchange

How to Install the Certificate Authority Service

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

- Installing the CA on Windows Server 2003, page 5-7
- Installing the CA on Windows Server 2008, page 5-7

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 Choose **Start > Control Panel > Add or Remove Programs**.

Step 2 In the Add or Remove Programs window, choose **Add/Remove Windows Components**.

Step 3 Complete the Windows Components wizard:

a. In the Windows Components window, check **Certificate Services** and when the warning displays about domain partnership and computer renaming constraints, click **Yes**.

b. In the CA Type window, choose Stand-alone Root CA and click **Next**.

c. In the CA Identifying Information window, enter the name of the server in the Common Name field for the CA server. If there is no DNS, type the IP address and click **Next**.

Note 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.

d. In the Certificate Database Settings window, accept the default settings and click **Next**.

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

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

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

What To Do Next

Generating a CSR - Running Windows Server 2003, page 5-8

Installing the CA on Windows Server 2008

Procedure

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

Step 2 In the console tree, choose **Roles**.

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

Step 4 Complete the Add Roles wizard:

a. In the Before You Begin window, ensure that you have completed all prerequisites listed and click **Next**.

b. In the Select Server Roles window, check **Active Directory Certificate Services** and click **Next**.

c. In the Introduction window, click **Next**.

d. In the Select Role Services window, check the follow boxes and click **Next**:
   - Certificate Authority
   - Certificate Authority Web Enrollment
   - Online Responder

e. In the Specify Setup Type window, choose **Standalone**.

f. In the Specify CA Type window, choose **Root CA**.

g. In the Setup Private Key window, choose **Create a New Private Key**.

h. In the Configure Cryptography for CA window, choose the default cryptographic service provider.

i. In the Configure CA Name window, enter a common name to identify the CA.

j. In the Set Validity Period window, set the validity period for the certificate generated for the CA.

Note The CA issues valid certificates only to the expiration date that you specify.

k. In the Configure Certificate Database window, choose the default certificate database locations.

l. In the Confirm Installation Selections window, click **Install**.

m. In the Installation Results Window, verify that the **Installation Succeeded** message displays for all components and click **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 5-8

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

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 In the Internet Information Services (IIS) Manager, perform these actions:

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

b. Choose **Properties**.

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

Step 4 Choose **Server Certificate**.

Step 5 When the Web Server Certificate wizard window opens, click **Next**.

Step 6 Complete the Web Server Certificate wizard:

a. In the Server Certificate window, choose **Create a new certificate** and click **Next**.

b. In the Delayed or Immediate Request window, choose **Prepare the request now**, **but send it later** and click **Next**.

c. In the Name and Security Settings window, accept the Default Web Site certificate name and choose **2048** for the bit length.

d. In the Organization Information window, enter your Company name in the Organization field and the organizational unit of your company in the Organizational Unit field.

e. In the Your Site's Common Name window, enter the Exchange Server hostname or IP address for Common Name and click **Next**.

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.

f. In the Geographical Information window, enter your geographical information as follows:
   - Country/Region
   - State/province
   - City/locality

g. In the Certificate Request File Name window, enter an appropriate filename for the certificate request and specify the path and file name where you want to save your CSR and click **Next**.

Note Make sure that you save the CSR without any extension (.txt) and remember where you save it because you must find this CSR file in a later step. Only use Notepad to open the file.

h. In the Request File Summary window, confirm that the information is correct and click **Next**.

i. In the Web Server Certificate Completion window, click **Finish**.

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

What To Do Next

Submitting the CSR to the CA Server/Certificate Authority, page 5-11

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.

Procedure

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

Step 2 In the left pane of the IIS Manager, under Connections, choose the Exchange Server.

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

Step 4 In the right pane of the IIS Manager, under Actions, choose **Create Certificate Request**.

Step 5 Complete the Request Certificate wizard:

a. In the Distinguished Name Property window, enter the following information:

- For Common Name, enter the Exchange Server hostname or IP address.
- In the Organization field, enter your company name.
- In the Organizational Unit field, enter the organizational unit that your company belongs to.

b. Enter your geographical information as follows and click **Next**:

- City/locality
- State/province
- Country/Region

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.

c. In the Cryptographic Service Provider Properties window, accept the default Cryptographic service provider. Choose **2048** for the bit length and click **Next**.

d. In the Certificate Request File Name Window, enter the appropriate filename for the certificate request and click **Next**.

Note Make sure that you save the CSR without any extension (.txt) and remember where you save it because you must find this CSR file in a later step. Only use Notepad to open the file.

e. In the Request File Summary window, confirm that the information is correct and click **Next**.

f. In the Request Certificate Completion window, click **Finish**.

What To Do Next

Submitting the CSR to the CA Server/Certificate Authority, page 5-11

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 CA 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 Choose **Request a certificate**.

Step 4 Choose **advanced certificate request**.

Step 5 Choose **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, choose 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 Click **Submit**.

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

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

a. Navigate to **All Tasks**.

b. Choose **Issue**.

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

What To Do Next

Downloading the Signed Certificate, page 5-12

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 the Issued Requests area.

Step 2 Right-click the request and choose **Open**.

Step 3 Choose the **Details** tab.

Step 4 Choose **Copy to File**.

Step 5 Click **Next** when the Certificate Export wizard displays.

Step 6 Complete the Certificate Export wizard:

a. In the Export File Format window, choose Base-64 encoded X.509 and click **Next**.

b. In the File to Export window, enter the location where you want to store the certificate and use cert.cer for the certificate name and choose

```
c:\cert.cer
```

c. In the Certificate Export wizard Completion window, review the summary information and verify that the export was successful and click **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 steps 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 provides you with the signed certificate.

Procedure

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

Step 2 In the Internet Information Services window, complete the following steps:

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

b. Choose **Properties**.

Step 3 In the Default Web Site Properties window, complete the following steps:

a. Choose the **Directory Security** tab.

b. Choose **Server Certificate**.

Step 4 When the Web Server Certificate wizard window opens, click **Next**.

Step 5 Complete the Web Server Certificate wizard:

a. In the Pending Certificate Request window, choose **Process the pending request and install the certificate** and click **Next**.

b. In the Process a Pending Request window, choose **Browse** to locate your certificate and navigate to the correct path and filename.

c. In the SSL Port window, enter 443 for the SSL port and click **Next**.

d. In the Web Server Certificate Completion window, click **Finish**.

Troubleshooting Tips

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

- Under the Directory Security tab, choose **View Certificate**.
- Choose **Details > Highlight root certificate**, and click **View**.
- Choose 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 provides you with the signed certificate.

Procedure

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

Step 2 Under Connections in the left pane of the IIS Manager, choose the Exchange Server.

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

Step 4 Under Actions in the right pane of the IIS Manager, choose **Complete Certificate Request**.

Step 5 In the Specify Certificate Authority Response window, complete these actions:

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

b. Navigate to the correct path and filename.

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

d. Click **Ok**. The certificate that you completed displays in the certificate list.

Step 6 In the Internet Information Services window, complete the following steps to bind the certificate:

a. Choose **Default Web Site**.

b. Under Actions in the right pane of the IIS Manager, choose **Bindings**.

Step 7 In the Site Bindings window, complete the following steps:

a. Choose **https**.

b. Click **Edit**.

Step 8 In the Edit Site Binding window, complete the following steps:

a. From the SSL certificate drop-down list, choose the certificate that you just created. The “friendly name” that you applied to the certificate displays.

b. Click **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 Log 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 Choose **Download a CA certificate**, **certificate chain**, **or CRL**.

Step 4 For Encoding Method, choose **Base 64**.

Step 5 Click **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

[Optional] How to Configure Multilingual Support for Calendaring Integration, page 5-19

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 automatically installs missing certificates. **Note** This procedure describes one way to access and configure the Certificate Import Tool in 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 (choose **Presence > Gateways**).	**a.** Choose **System > Security > Certificate Import Tool** in Cisco Unified Presence Administration. **b.** Choose **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 – hostname – FQDN The value that you enter in this Peer Server field must exactly match the IP address, hostname, 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.** Click **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 (choose **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. Log in to **Cisco Unified OS Administration**. c. Choose **Security > Certificate Management**. d. In the Certificate List window, choose **Upload Certificate**. e. When the Upload Certificate dialog box opens, complete these actions: – From the Certificate Name list box, choose **cup-trust**. – Enter the root certificate name without any extension. f. Choose **Browse** and choose **certnew.cer**. g. Click **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. Log in to **Cisco Unified Serviceability**. Choose **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 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.

Enabling Calendar Integration

Calendaring must be enabled on a per-user basis and must be done by the end user, not the administrator. By default, Cisco Jabber automatically determines the availability status of each person. It detects when a person is signed into the application. Your system administrator can also integrate your Microsoft Outlook calendar to show you are in a meeting. You can choose if you display your meeting status by setting an option.

Complete the following procedure to set an option to display your meeting status.

Note Calendar integration can only be enabled on an individual basis, however calendar integration can be disabled for all users by removing the last calendar Presence Gateway from the configuration.

Before You Begin

Ensure the Presence Gateway is configured on Cisco Unified Presence. For more information, see Configuring the Presence Gateway on Cisco Unified Presence for Microsoft Exchange Integration, page 5-1.

Procedure

Step 1 Log in to **Cisco Unified Presence User Options**.

Note Calendaring can also be enabled from within the Cisco Unified Presence client and the Cisco Jabber client.

Step 2 Choose **User Options > Preferences**.

Step 3 Under **Calendar Settings**, set the **Include Calendar Information in my Presence Status** to **On**.

Step 4 Click **Save**.

[Optional] Configuring the Frequency of Microsoft Exchange Calendar Notifications Sent over EWS

Note that this procedure only applies if you are integrating Exchange Server 2007 or 2010 over EWS. These steps are *not* required for WebDAV calendar integration.

The EWS Status Frequency parameter specifies an interval (in minutes) that determines how long it takes before the Exchange Server updates the subscription on Cisco Unified Presence. By default this parameter is 60 minutes. Shorten this duration if you want the Presence Engine on Cisco Unified Presence to detect that it has lost the subscription more frequently than every 60 minutes (default). Error detection improves if you shorten the duration but there is a corresponding increased load on the Exchange Server and the Cisco Unified Presence Server.

Procedure

Step 1 Log in to **Cisco Unified Presence Administration**.

Step 2 Choose **System > Service Parameters**.

Step 3 From the Server drop-down list, choose the Cisco Unified Presence Server.

Step 4 From the Service drop-down list, choose Cisco UP Presence Engine (Active).

Step 5 In the EWS Status Frequency field, edit the parameter value, this parameter limit is 1440 minutes. By default this parameter is 60 minutes.

Step 6 Click **Save**.

What To Do Next

EWS Status Frequency parameter changes are updated incrementally as calendar integration occurs on a per-user basis. However, we recommend that you restart the Cisco UP Presence Engine to effect the parameter change for all users at once. Log in to **Cisco Unified Serviceability**. Choose **Tools > Service Activation**.

[Optional] How to Configure Multilingual Support for Calendaring Integration

Note that this procedure only applies if you are integrating Exchange Server 2003 or 2007 over WebDAV. These steps are *not* required for EWS calendar integration.

User locales are country-specific, and user locale files provide the translated text for user applications and user web pages in a given locale. If you want to expand your Exchange deployment to support multiple languages, you must configure Cisco Unified Communications Manager and Cisco Unified Presence to support the user locales that you require in your calendaring integration. There is no limit to the number of supported languages.

- Installing the Locale Installer on Cisco Unified Communications Manager, page 5-19
- Installing the Locale Installer on Cisco Unified Presence, page 5-20
- Setting User Locales for Multilingual Calendaring Integration, page 5-22

Installing the Locale Installer on Cisco Unified Communications Manager

Before you begin this procedure, consider the following caveats:

- You must install Cisco Unified Communications Manager (Release 6.x or a higher release) on every server in the cluster before you install the Cisco Unified Communications Manager locale installer.
- The default setting for installed locales is “English, United States”. We strongly recommend that you install the appropriate language/locale on Cisco Unified Communications Manager and choose the appropriate language/locale on the Exchange Server the first time the user signs in. Note the following considerations that apply to WebDAV integrations only:
  - If you set the default language (English) on the Exchange Mailbox of an end user when there is a different language/local installed on Cisco Unified Communications Manager, you cannot change the locale for the user later. For more information about this issue, see Localization Caveat with WebDAV Calendaring Integrations, page 6-6.
  - If you set a locale other than English, you must install the appropriate language installers on both Cisco Unified Communications Manager *and* on Cisco Unified Presence. Ensure the locale installer is installed on every server in the cluster (install on the Publisher Server before the Subscriber servers).
- User locales should *not* be set until all appropriate locale installers are loaded on *both* systems. Users may experience problems with calendaring if they inadvertently set their user locale *after* the locale installer is loaded on Cisco Unified Communications Manager but *before* the locale installer is loaded on Cisco Unified Presence. If issues are reported, we recommend that you notify each user to log in to **Cisco Unified Communications Manager User Options** and change their locale from the current setting to English and then back again to the appropriate language. You can also use the Bulk Administration Tool (BAT) to synchronize user locales to the appropriate language.

- You must restart the server for the changes to take effect. After you complete all locale installation procedures, restart each server in the cluster. Updates do not occur in the system until you restart all servers in the cluster; services restart after the server reboots.
- Make sure that you install the same components on every server in the cluster.

To complete this procedure on Cisco Unified Communications Manager, see the *Cisco Unified Communications Operating System Administration Guide* here:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/cucos/8_0_1/cucos/iptpch7.html#wp1054072

What To Do Next

Installing the Locale Installer on Cisco Unified Communications Manager, page 5-19

Installing the Locale Installer on Cisco Unified Presence

Before You Begin

- Install the locale installer on Cisco Unified Communications Manager. If you want to use a locale other than English, you must install the appropriate language installers on both Cisco Unified Communications Manager *and* on Cisco Unified Presence.
- If your Cisco Unified Presence cluster has more than one node, make sure that the locale installer is installed on every server in the cluster (install on the Publisher Server before the Subscriber servers).
- User locales should *not* be set until all appropriate locale installers are loaded on *both* systems. Users may experience problems with calendaring if they inadvertently set their user locale *after* the locale installer is loaded on Cisco Unified Communications Manager but *before* the locale installer is loaded on Cisco Unified Presence. If issues are reported, we recommend that you notify each user to log in to **Cisco Unified Communications Manager User Options** and change their locale from the current setting to English and then back again to the appropriate language. Yo u can also use the Bulk Administration Tool (BAT) to synchronize user locales to the appropriate language.
- You must restart the server for the changes to take effect. After you complete all locale installation procedures, restart each server in the cluster. Updates do not occur in the system until you restart all servers in the cluster; services restart after the server reboots.

Procedure

Step 1 Go to this location on cisco.com to locate the Cisco Unified Presence locale installer:

http://tools.cisco.com/support/downloads/go/ReleaseType.x?optPlat=&isPlatform=Y&mdfid=281820245&sftType=Unified+Presence+Locale+Installer&treeName=Voice+and+Unified+Communications&modelName=Cisco+Unified+Presence+Version+7.0&mdfLevel=Software%20Version/Option&treeMdfId=278875240&modifmdfid=null&imname=&hybrid=Y&imst=N

Step 2 Choose the version of the Cisco Unified Presence locale installer that is appropriate for your working environment.

Step 3 After downloading the file, save the file to the hard drive and note the location of the saved file.

Step 4 Copy this file to a server that supports SFTP.

Step 5 Log in to **Cisco Unified OS Administration** using your administrator account and password.

Step 6 Choose **Software Upgrades > Install/Upgrade**.

Step 7 Choose **Remote File System** as the software location source.

Step 8 In the Directory field, enter the file location, for example /tmp.

Step 9 Enter the name of the server that contains the locale installer file (the server that you specified in Step 4). This copies the file to your Cisco Unified Presence Server where you can install it.

Step 10 In the User Name and User Password fields, enter your username and password credentials.

Step 11 For the Transfer Protocol, choose **SFTP**.

Step 12 Click **Next**.

Step 13 From the list of search results, choose the Cisco Unified Presence locale installer.

Step 14 Click **Next** to load the installer file and validate it.

Step 15 After you complete the locale installation, restart each server in the cluster.

Step 16 The default setting for installed locales is "English, United States". While your Cisco Unified Presence Server is restarting, change the language of your browser, if necessary, to match the locale of the installer that you have downloaded.

If you use this browser:	Configuration Steps
Internet Explorer Version 6.x	a. Choose **Tools > Internet Options**. b. Choose the General tab. c. Choose **Languages**. d. Use the Move Up button to move your preferred language to the top of the list. e. Click **OK**.
Mozilla Firefox Version 3.x	a. Choose **Tools > Options**. b. Choose the Content tab. c. In the Languages area of the window, choose **Choose**. d. Use the Move Up button to move your preferred language to the top of the list. e. Click **OK**.

Step 17 Verify that your users can choose the locale(s) for supported products.

Step 18 [Optional] If you are localizing your Calendaring integration, does the Exchange Server URL contain the localized word for "Calendar"? If you must take corrective action, see Troubleshooting Account Name and Password, page 6-4.

Troubleshooting Tips

Make sure that you install the same components on every server in the cluster.

What To Do Next

Setting User Locales for Multilingual Calendaring Integration, page 5-22

Setting User Locales for Multilingual Calendaring Integration

Before You Begin

- Install the Cisco Unified Communications Manager and Cisco Unified Presence locale installers that contain all the available languages. User locales should *not* be set until all appropriate locale installers are loaded on *both* systems.
- The default setting for installed locales is “English, United States”. We strongly recommend that you install the appropriate language/locale on Cisco Unified Communications Manager and choose the appropriate language/locale on the Exchange Server the first time the user signs in. Note that if you set the default language (English) on the Exchange Mailbox of an end user when there is a different language/local installed on Cisco Unified Communications Manager, you cannot change the locale for the user later. For more information about this issue, see Localization Caveat with WebDAV Calendaring Integrations, page 6-6.
- You may experience problems with calendaring if you inadvertently set your user locale *after* the locale installer is loaded on Cisco Unified Communications Manager but *before* the locale installer is loaded on Cisco Unified Presence. To force the system to use the appropriate language, we recommend that you log in to **Cisco Unified Communications Manager User Options** and change the user locale from the current setting to English. Then reset the locale to the language that you require.

Procedure

Step 1 Complete the procedure specific to your role (administrator or user), as follows:

Step 2 If you are an administrator:

a. Log in to **Cisco Unified Communications Manager Administration** using the administrator account and password.

b. Choose **User Management > End User**.

c. Use the Find and List functionality to search for and locate the user that you require.

d. Choose the User ID hyperlink for the user that you require.

e. From the User Locale drop-down list, choose the appropriate language for the user.

f. Click **Save**.

Step 3 If you are a user:

a. Log in to **Cisco Unified Communications Manager User Options** using the user account and password.

b. Choose **User Options > User Settings Configuration**.

c. From the User Locale drop-down list, choose the appropriate language for the user.

d. Click **Save**.

Related Topics

- Installing the Locale Installer on Cisco Unified Communications Manager, page 5-19
- Installing the Locale Installer on Cisco Unified Presence, page 5-20

[Optional] Configuring the Microsoft Exchange Notification Port

This topic only applies if you want the Presence Engine to listen for incoming notifications from the Exchange Server on another port specific to your network configuration. This procedure can apply to both WebDAV and EWS Exchange configurations.

If you have a WebDAV integration, UDP port 50020 is used by default to receive the HTTPU notifications. If you have an EWS integration, a TCP port is used by default to receive the HTTP notifications.

Before You Begin

If you change from the default port, make sure that the replacement port that you assign is not already in use.

Procedure

Step 1 Log in to **Cisco Unified Presence Administration**.

Step 2 Choose **System > Service Parameters**.

Step 3 From the Server menu, choose the Cisco Unified Presence Server.

Step 4 From the Service menu, choose **Cisco UP Presence Engine (Active)**.

Step 5 In the Calendaring Configuration area, edit the parameter value for the Microsoft Exchange Notification Port field. By default this parameter is 50020 for WebDAV configurations.

Step 6 Click **Save**.

What To Do Next

We recommend that you restart the Cisco UP Presence Engine to effect the parameter change for all users at once. Log in to **Cisco Unified Serviceability**. Choose **Tools > Service Activation**.

Troubleshooting Tips

- If you change from the default port, the Presence Engine continues to use the existing calendar information for users, (including the number of meetings and the start and end times) until such time as the Exchange subscription for the user is renewed. It may take up to an hour for the Presence Engine to receive notifications that a user's calendar has changed.
- We recommend that you restart the Cisco UP Presence Engine to effect the change for all users at once.

[Optional] Configuring the Duration Range of Microsoft Exchange Calendar Notifications

By default, the Presence Engine allows for meeting/busy notifications to be sent 50 seconds after the top-of-minute. If you have a small user base, we recommend that your shorten this delay using the formula specified in this procedure. However, note that this topic is optional and only applies if you want to change the duration range for any reason specific to your network configuration.

Before You Begin

Use this formula to configure this field value (in seconds): Maximum number of assigned users / 100. For example, if a node has a maximum number of users of 1000, then the offset range is 10 seconds.

Procedure

Step 1 Log in to **Cisco Unified Presence Administration.**

Step 2 Choose **System > Service Parameters**.

Step 3 From the Server menu, choose the Cisco Unified Presence Server.

Step 4 From the Service menu, choose **Cisco UP Presence Engine (Active)**.

Step 5 In the Calendar Spread field, edit the parameter value. This parameter limit is 59 seconds. If meetings start or end more than one minute late, it interferes with meeting start/end counters and notifications. By default this parameter is 50.

Step 6 Click **Save**.

What To Do Next

Calendar Spread parameter changes are updated incrementally as calendar integration occurs on a per-user basis. However, we recommend that you restart the Cisco UP Presence Engine to effect the parameter change for all users at once. Log in to **Cisco Unified Serviceability**. Choose **Tools > Service Activation**.

Troubleshooting Tip

If a very large number of users transition either in and/or out of meetings, a mass notification event occurs that may delay some notifications up to a few minutes.

Other Microsoft Exchange Parameters

There are three other Exchange calendaring parameters that you can configure in the Service Parameters window of Cisco Unified Presence Administration:

- Exchange Timeout (seconds)—the duration, in seconds, before a request made to a Exchange Server times out.
- Exchange Queue—the length of the request queue.
- Exchange Threads—the number of threads used to service Exchange requests.

Caution We do not recommend that you change the default settings of these parameters because any changes may affect your Exchange integration. Contact Cisco Technical Assistance Center (TAC) for support.