Configure IM and Presence Service for Calendar Integration

Configure a Presence Gateway for Microsoft Exchange Integration

You must configure an Exchange Server (Microsoft Outlook) as a Presence Gateway for calendaring information exchange. The Exchange gateway enables the IM and Presence Service node to reflect the availability information 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

When configuring your Exchange Web Services (EWS) Presence Gateway for Exchange integration through the **Cisco Unified CM IM and Presence Administration** user interface, note the following:

- You can add, update, or delete *one or more* EWS servers with no maximum limit. However, the Troubleshooter on the **Presence Gateway Configuration** 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 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 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.

Configure Exchange 2007, 2010, or 2013 as a Presence Gateway over Exchange Web Services

Before you begin

Before you configure a Presence Gateway, you must upload a valid certificate chain to the IM and Presence Service.

If the connection to the Microsoft Exchanger server is over IPv6, ensure that the enterprise parameter is configured for IPv6 and that Eth0 is set for IPv6 on each IM and Presence Service node in the deployment. For information about configuring IPv6 on IM and Presence Service, see the *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

Procedure

Step 1 Log in to the **Cisco Unified CM IM and Presence Administration** user interface.

Step 2 Choose **Presence** > **Gateways**.

Step 3 Click **Add New**.

Step 4 Choose **Exchange -- EWS Server** for the Presence Gateway Type.

For configuration changes to take effect, you must restart the Cisco Presence 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 Subject Alternative Name field of the Exchange Server certificate. 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 that is protected by the Wildcard Certificate. For example, if a Wildcard Certificate protects the subdomain `*.imp.cisco.com`, you must enter a node value of *`server_name`*`.imp.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.

For IPv6, the IPv6 address you enter must match the value that is entered in the SAN field of the Exchange Server certificate.

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

Step 8 Enter the Exchange Account Password required for the IM and Presence Service 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. The IM and Presence Service integration with Exchange occurs over a secure HTTP connection. Cisco recommends that you use port 443 (default port) and not change to other ports.

Step 10 Click **Save**.

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

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

What to do next

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

- Did the connection between the IM and Presence Service and the Exchange Server succeed? The Exchange Server Status area in the **Presence Gateway Configuration** window reports the connection status. If you need to take corrective action, see Troubleshooting Exchange Server Connection Status.
- Is the status of the Exchange SSL certificate chain correct (verified)? The Exchange Server Status area in the **Presence Gateway Configuration** window indicates if there is a certificate Subject CN mismatch. If you need to take corrective action, see Troubleshooting SSL Connection Certificate Status.

SAN and Wildcard Certificate Support

The IM and Presence Service uses X.509 certificates for secure calendaring integration with Microsoft Exchange. The IM and Presence Service supports SAN and wildcard certificates, along with standard certificates.

SAN certificates allow multiple hostnames and IP addresses to be protected by a single certificate, by specifying a list of hostnames, IP addresses, or both in the X509v3 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 For SAN certificates, the protected host must be contained in the list of hostnames/IP addresses in the Subject Alternative Name field. When you configure the Presence Gateway, the Presence Gateway field must exactly match the protected host listed in the Subject Alternative Name field.

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

Configure Secure Certificate Exchange Between the IM and Presence Service 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 a CA on Windows Server 2003
- Installing a CA on Windows Server 2008

Installing a 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 Component** wizard:

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

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

Installing a 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 the check box for **Active Directory Certificate Services** and click **Next**.
c) In the **Introduction Window** window, click **Next**.
d) In the **Select Role Services** window, check these check boxes and click **Next**.

- Certificate Authority
- Certificate Authority Web Enrollment
- Online Responder

e) In the **Specify Setup Type** window, click **Standalone**.
f) In the **Specify CA Type** window, click **Root CA**.
g) In the **Set Up Private Key** window, click **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 up 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 The Active Directory Certificate Services is now listed as one of the roles on the Server Manager.

What to do next

Generating a CSR – Running Windows Server 2008

Generation of a CSR on IIS of a Microsoft 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**.

a) Right-click **Default Web Site**.
b) Choose **Properties**.

Step 2 Choose the **Directory Security** tab.

Step 3 Choose **Server Certificate**.

Step 4 Click **Next** when the **Web Server Certificate** wizard displays.

Step 5 Complete the **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, choose **1024** for the bit length, and click **Next**.
d) In the **Organization Information** window, enter your Company name in the Organization field, the organizational unit of your company in the Organizational Unit field, and click **Next**
e) In the **Your Site's Common Name** window, enter the Exchange Server hostname or IP address and click **Next**.

Note The IIS certificate Common Name that you enter is used to configure the Presence Gateway on the IM and Presence Service, 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, and click **Next**.

- Country/region
- State/province
- City/locality

g) In the **Certificate Request File Name** window, enter an appropriate filename for the certificate request, 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 need to be able to find this CSR file after. Only use Notepad to open the file.

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

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

What to do next

Submitting a CSR to the CA Server/Certificate Authority

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 the **Internet Information Services (IIS) Manager** window.

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 **Create Certificate Request**.

Step 5 Complete the **Request Certificate** wizard:

a) In the **Distinguished Name Properties** window, enter the following information:

- In the **Common Name** field, 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 geographic 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 the IM and Presence Service, 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 need to be able to find this CSR file later. 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 a CSR to the CA Server/Certificate Authority

Submitting a 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 the IM and Presence Service 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 CM IM and 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://*locall_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 the **Administrative Tools** window, 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:

- Navigate to **All Tasks**.
- Choose **Issue**.

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

What to do next

Downloading a Signed Certificate

Downloading a Signed Certificate

Before you begin

[Self-signed Certificates] Submit the Certificate signing request (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 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 When the **Certificate Export** wizard displays, click **Next**.

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, use cert.cer for the certificate name, and choose `c:\cert.cer`.
c) In the **Certificate Export Wizard Completion** window, review the summary information, verify that the export was successful, then click **Finish**.

Step 7 Copy or FTP the cert.cer to the computer that you use to administer the IM and Presence Service.

What to do next

Upload a signed certificate for your server type:

- Uploading a Signed Certificate – Running Windows 2003
- Uploading a Signed Certificate – Running Windows 2008

Upload of Signed Certificate onto Exchange IIS

Uploading a 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 the IM and Presence Service.

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 Complete the following steps in the **Internet Information Services** window:

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 displays, 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, click **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**.

Tip

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, click **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 a Root Certificate

Uploading a 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 the IM and Presence Service.

Before you begin

[Self-signed Certificates] Download the signed certificate.

[Third-party Certificates] Your Certificate Authority provides the signed certificate.

Procedure

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

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) To locate your certificate, choose the ellipsis [...].
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 Complete the following steps in the **Site Bindings** window:

a) Choose **https**.
b) Choose **Edit**.

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

a) Choose the certificate that you just created from the SSL certificate drop-down list. The name that you applied to the certificate displays.
b) Click **Ok**.

What to do next

Downloading a Root Certificate

Downloading a Root Certificate

Before you begin

Upload the Signed Certificate onto Exchange IIS.

Procedure

Step 1 Log in to your CA Server user interface and open a web browser.

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

a) Windows Server 2003 – http://127.0.0.1/certserv
b) Windows Server 2008 – https://127.0.0.1/certsrv

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

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

Step 5 Click **Download CA Certificate**.

Step 6 Save the certificate, **certnew.cer**, to the local disk.

Tip

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

Upload a Root Certificate to the IM and Presence Service Node

Upload a Root Certificate to the IM and Presence Service Node

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 the IM and Presence Service as a CiscoUnified Presence Trust certificate (cup-trust).

Procedure

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

Upload the certificate via:	Actions
Certificate Import Tool in **Cisco Unified CM IM and Presence Administration**. The Certificate Import tool simplifies the process of installing trust certificates on the IM and Presence Service 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 CM IM and Presence Administration**. You can also view a customized version of the Certificate Import Tool in **Cisco Unified Presence Administration** when you configure the Exchange Presence Gateway for a specific type of calendaring integration (Log in to **Cisco Unified CM IM and Presence Administration** and choose **Presence** > **Gateways**).	**a.** Log in to the **Cisco Unified CM IM and Presence Admi** **b.** Choose **System** > **Security** > **Certificate Import Tool**. **c.** Choose **IM and Presence(IM/P) Trust** as the Certificate to install the certificates. This stores the Presence Engine t Exchange integration. **d.** Enter one of these values to connect with the Exchange Se • IP address • Hostname • FQDN The value that you enter in this Peer Server field must exa hostname or FQDN of the Exchange Server. **e.** Enter the port that is used to communicate with the Excha match the available port on the Exchange Server. **f.** Click **Submit**. After the tool finishes, it reports these state • Peer Server Reachability Status — indicates whether Service can reach (ping) the Exchange Server. See Trou Connection Status. • SSL Connection/Certificate Verification Status — in Certificate Import Tool succeeded in downloading ce peer server and whether or not a secure connection ha the IM and Presence Service and the remote server. S Connection Certificate Status.

Step 2 If the Certificate Import Tool indicates that certificates are missing (typically the CA certificate 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 IM and Presence 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 (Log in to **Cisco Unified IM and Presence Operating System Administration**. Choose **Security** > **Certificate Management**).	**a.** Copy or FTP the **certnew.cer** certificate file to the computer th your IM and Presence Service node. **b.** Log in to the **Cisco Unified IM and Presence Operating Sy** user interface. **c.** Choose **Security** > **Certificate Management**. **d.** In the **Certificate List** window, choose **Upload Certificate/C** **e.** Complete these actions when the **Upload Certificate/Certific** opens: • From the Certificate Name drop-down list, choose **cup-t** • Enter the root certificate name without any extension. **f.** Click **Browse** and choose **certnew.cer**. **g.** Click **Upload File**.

Step 3 Return to the Certificate Import Tool (Step 1, on page 12) and verify that all status tests succeed.

Step 4 Restart the CiscoPresence Engine and SIP Proxy service after you upload all Exchange trust certificates. Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools** > **Control Center - Feature Services**.

Tips

The IM and Presence Service allows you to upload Exchange Server trust certificates with or without a Subject Common Name (CN).

What to do next

IM and Presence Calendar Integration Task Flow

Enabling Calendar Integration

Calendar integration is enabled by the administrator, either on an individual basis or for groups of users.

Note Ensure the Presence Gateway is configured on Cisco Unified Communications Manager. For more information, see Configure a Presence Gateway for Microsoft Exchange Integration , on page 1.

Enabling Calendar Integration for Individual Users

Use this procedure to configure Microsoft Outlook calendar integration for an individual end user.

Procedure

Step 1 Log in to the **Cisco Unified CM Administration** user interface.

Step 2 Choose **User Management** > **End User**.

Step 3 Click **Find** and select an end user.

Step 4 Check the **Enable User for Unified CM IM and Presence** check box.

Step 5 Check the **Include meeting information in presence** check box.

Step 6 Click **Save**.

Enabling Calendar Integrations in Bulk

Procedure

Step 1 On a Cisco Unified Communications Manager node, log in to the **Cisco Unified CM Administration** user interface.

Step 2 Enabling calendar integrations in bulk can be performed from the following windows:

a) **Bulk Administration** > **Users** > **Insert Users**.
b) **Bulk Administration** > **Users** > **Update Users** > **Query**.
c) **Bulk Administration** > **Users** > **Update Users** > **Custom File**.

Note For information on the different types of update options, refer to the *Bulk Administration Guide for Cisco Unified Communications Manager*.

Step 3 For all end users for whom you want to enable calendar integration, make sure that the following end user configuration options are checked:

- **Enable User for Unified CM IM and Presence**
- **Include meeting information in Presence**

Step 4 If you are updating from a csv file, in the appropriate Users area, choose a File Name.

Note Click **View Sample File** for the correct file format.

Step 5 Click **Run Immediately** or **Run Later**.

Step 6 Click **Submit**.

[Optional] Configure the Frequency of Exchange Calendar Notifications Sent Over Exchange Web Services

Note This procedure only applies if you are integrating Microsoft Exchange Server 2007, 2010, or 2013 over Exchange Web Services (EWS).

The EWS Status Frequency parameter specifies an interval (in minutes) that determines how long it takes before the Exchange Server updates the subscription on the IM and Presence Service. By default this parameter is 60 minutes. Shorten this duration if you want the Presence Engine on the IM and Presence Service 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 IM and Presence Service node.

Procedure

Step 1 Log in to the **Cisco Unified CM IM and Presence Administration** user interface.

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

Step 3 From the Server drop-down list, choose the IM and Presence Service node.

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

Step 5 In the Calendaring Configuration (Parameters that apply to all servers) area, edit the parameter value in the EWS Status Frequency field, 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 Presence Engine to effect the parameter change for all users at once. Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools** > **Service Activation**.

[Optional] Configure the Microsoft Exchange Notification Port

This topic only applies if you want the Cisco Presence Engine to listen for incoming notifications from the Exchange Server on another port specific to your network configuration.

With 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 the **Cisco Unified CM IM and Presence Administration** user interface.

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

Step 3 From the Server drop-down list, choose the IM and Presence Service node.

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

Step 5 In the Calendaring Configuration area, edit the parameter value for the Microsoft Exchange Notification Port field and click **Save**.

What to do next

We recommend that you restart the Cisco Presence Engine to effect the parameter change for all users at once. Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools** > **Control Center - Feature Services**.

Tip

- If you change from the default port, the Cisco 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 Cisco Presence Engine to receive notifications that a user’s calendar has changed.
- We recommend that you restart the Cisco Presence Engine to effect the change for all users at once.

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

By default, the Cisco Presence Engine allows for meeting/busy notifications to be sent 50 seconds after the top-of-the-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 the **Cisco Unified CM IM and Presence Administration** user interface.

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

Step 3 From the Server drop-down list, choose the IM and Presence Service node.

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

Step 5 In the Calendaring Configuration area, edit the parameter value in the Calendar Spread field. 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 Presence Engine to effect the parameter change for all users at once. Log in to **Cisco Unified IM and Presence Serviceability**. Choose **Tools** > **Control Center - Feature Services**.

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

Other Microsoft Exchange Calendaring Parameters

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

- Exchange Timeout (seconds) — the duration, in seconds, before a request made to an 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 adversely affect your Exchange integration. Contact Cisco Technical Assistance Center (TAC) for support.

Out of Office Presence Status

The IM and Presence service supports Out of Office (OOO) as the user's availability status. As a result, when you set the out of office notification in Micorsoft Outlook for a specific duration, your Jabber presence status will be displayed as **Out of Office** instead of showing **Away** or **Offline**.

Moreover, it improves the user experience while collecting the user status information and helps others know about your availability as out of office along with the start and end dates of the OOO period. This brings in better user experience by enhancing instant messaging system through provisioning the user presence state with much clarity and precision.

Moreover, you can override your OOO presence status using the custom presence settings and switch back and forth to Active and OOO status when required. This helps you handle urgent communications and critical meetings much effectively. Hence, it eliminates the gap arise between the on-premise and cloud-based calendaring services as it supports both the MS Exchange Server and Office 365 server.

For example John Smith, a lead customer support executive, who proceeds on a vacation, has set the out of office notification in Office 365 for a period between December 10 20XX 0800 Hrs. and December 20 20XX 2300 Hrs. Upon implementing this feature, his presence status in Jabber on December 10 is shown as Active/Away/Offline (as the case may be) with a message stating - *Out of office from 10th March 2019 10:00 AM GMT till 12th March 2019 6:00 PM GMT*. The availability status icon will turn orange (except when he is offline). On December 14, John gets a call from his manager who asks him to join a business-critical meeting over Jabber to address an urgent technical issue. With this new enhancement in the IM and Presence service, John can temporarily override the OOO status and manually turn the availability status to Active and join the meeting with the customer. After the meeting is over, he can turn presence status back to OOO till the end of his scheduled vacation.

Out of Office Notification in Jabber and WebEx Teams

When you configure out of office in your calendaring service, such as MS Exchange or Office 365, the IM and Presence service pulls the OOO notification during the defined polling interval and displays your presence status as Out of Office. During this period, the availability status icon is displayed in orange. It shows the OOO time in the local time zone, for example, the message states*Out of office from 10th March 2019 10:00 AM GMT till 12th March 2019 6:00 PM GMT*. It also handles the localization of the message.

However, if you are offline during the out of office period, the status is displayed as Offline along with the Out of Office message.

Enable Out of Office Notification in IM and Presence Administration Console

The Calendar Out of Office Information parameter of the Cisco Presence Service helps to enable or disable display of the Out of Office availability status in the IM client applications. Complete the following procedure to enable out of office notification in the IM and Presence node.

Note In multimode IM and Presence deployment, if you enable the out of office notification option in one node, it is applicable to other nodes of the cluster.

1. In the Cisco Unified CM IM and Presence Administration console, choose **System** > **Service Parameters**.
2. In the Service Parameter Configuration page, select the **Server** where the IM and Presence node is deployed.
3. In the **Service** field, select **Cisco Presence Engine**.
4. In the **Calendaring Configuration (Parameters that apply to all servers)** section, set the **Calendar Out of Office Information** field to **Display Out of Office Availability**. This is done by default.
5. Click **Save**.

To disable display of out of office availability information, select **Do not display out of office availability** in the **Calendar Out of Office Information** field and click **Save**. This disables the service across all IM and Presence nodes in the cluster.

Note You must restart the PE service after making this change.