



Configure the IM and Presence Service

- [IM and Presence Calendar Integration Task Flow, on page 1](#)

IM and Presence Calendar Integration Task Flow

Complete these tasks on the IM and Presence Service to set up calendar integration with Microsoft Outlook for either of the following Microsoft deployments:

- An on-premise Microsoft Exchange server
- A hosted Microsoft Office 365 server

Procedure

	Command or Action	Purpose
Step 1	Configure a Presence Gateway, on page 2	On the IM and Presence server configure the Exchange server or Office 365 server as a Presence Gateway.
Step 2	Configure Pull Interval for Office 365 Integration, on page 4	(Office 365 only) Configure the interval schedule by which the IM and Presence Service pulls calendar information from Office 365. The default value is 60 minutes.
Step 3	Configure Service Parameters for Exchange Integration, on page 4	(Exchange only) Configure optional service parameters that outline the calendar sync interaction with the Microsoft Exchange server.
Step 4	Restart the Cisco Presence Engine, on page 6	If you edited any service parameters, restart the Cisco Presence Engine service.
Step 5	Enable calendaring for users using one of the following procedures: <ul style="list-style-type: none"> • Enable Calendaring for LDAP Synchronized Users, on page 6 • Enable Calendar Integrations by Bulk, on page 8 	Select the procedure that fits your needs: <ul style="list-style-type: none"> • If you have not yet completed an LDAP sync, enable calendaring via the LDAP sync.

	Command or Action	Purpose
	<ul style="list-style-type: none"> • Enable Calendar Integration for a User, on page 8 	<ul style="list-style-type: none"> • Otherwise, use the Bulk Administration Tool to configure calendaring for a large number of users. • Or enable the feature on a user by user basis.

Configure a Presence Gateway

Use this procedure to configure a Presence Gateway to set up calendar integration with Microsoft Outlook. You can assign either a Microsoft Exchange server or an Office 365 server as the Presence Gateway.

Procedure

-
- Step 1** From Cisco Unified CM IM and Presence Administration, choose **Presence > Gateways**.
- Step 2** Click **Add New**.
- Step 3** From the **Presence Gateway Type** field, choose one of the following options:
- Select **Exchange - - EWS Server**, if you are integrating with an on-premise Exchange server.
 - Select **Office 365 Server**, if you are integrating with a hosted Office 365 server.
- If you choose **Office 365 Server**, then you need to choose an **Authentication Type** from the drop-down list, by choosing either **Basic** or **OAuth**.
- Note** • The fields **Application (client) ID**, **Directory (tenant) ID**, and **Client Secret** are applicable only if you choose the **Authentication Type** as **OAuth**.
- Note** This note is applicable from release 12.5(1)SU8 onwards.
- The **Basic** Authentication Type for Office 365 server is deprecated. Please re-configure the Authentication Type with the default option **OAuth** from 12.5(1)SU8 onwards.
- See section [Office 365 Pre-Configuration for Authentication type OAuth, on page 3](#) to configure the fields **Application (client) ID**, **Directory (tenant) ID**, **Client Secret**, to set application permissions and grant admin consent.
- Step 4** In the **Description** field, enter a description that will help you to distinguish the presence gateway instance.
- Step 5** In the **Presence Gateway** field, enter the fully qualified domain name or IP address of the Presence Gateway server. This value must match the server address that is displayed in the **Subject Common Name (CN)** or **Subject Alternate Name** field of the server certificate.
- Step 6** In the **Account Name** field, enter the account name to access the server.
- Step 7** Enter the password that the account uses to access the server in both the **Account Password** and **Confirm Password** fields.
- Step 8** In the **HTTP/HTTPS Proxy URL** field, assign HTTP/HTTPS Proxy server details, if the **Presence Gateway Type** is **Office 365 Server** and IM and Presence Service doesn't have access to Office 365Server.
- Step 9** In the **HTTP/HTTPS Proxy Username** field, enter the user name to access the HTTP/HTTPS proxy server.

- Step 10** In the **HTTP/HTTPS Proxy Password** field, enter the password for the user name provided for HTTP/HTTPS proxy server.
- Step 11** Complete the remaining fields in the **Presence Gateway Settings** window. For more information on the fields and settings, see the online help.
- Step 12** Click **Save**.
-

What to do next

You can configure optional parameters for your Microsoft integration type:

- [Configure Pull Interval for Office 365 Integration, on page 4](#)
- [Configure Service Parameters for Exchange Integration , on page 4](#)

Office 365 Pre-Configuration for Authentication type OAuth

Use this procedure to configure the Presence Gateway Authentication Type as OAuth.

You need to follow the steps mentioned in the procedure to fetch the Application (client) ID, Directory (tenant) ID and Client Secret, to set application permission and to grant admin consent from Microsoft Azure portal.

Procedure

- Step 1** Log in to Microsoft Azure portal: <https://portal.azure.com>.
- Step 2** Register the new Application and fetch **Application (client) ID** and **Directory (tenant) ID** by following the steps available at: <https://docs.microsoft.com/en-gb/azure/active-directory/develop/quickstart-register-app#register-a-new-application-using-the-azure-portal>.
- Step 3** To create the **Client Secret**, under **Manage**, click **Certificates & Secrets > New Client Secret**.
- Note** If you choose **Presence Gateway Type** as **Office 365 Server** and **Authentication Type** as **OAuth**, use the same values to configure the Application (client) ID, Directory (tenant) ID and Client Secret fields on IM and Presence during the Presence Gateway configuration.
- Step 4** Click **Manage > API Permissions > Add a permission**, and choose **Office 365 Exchange Online** under **APIs my organization uses**.
- Step 5** To add an application permission, select **Application permissions > Permission**, check the check box **full_access_as_app** and click **Add permissions**.
- Step 6** To grant admin consent, click **Manage > API permissions**.
- Step 7** Under **Grant consent**, click **Grant admin consent for "registered Azure Active Directory"** and choose **Yes**.
- Step 8** Check if there is a green tick mark against **Status** column for **full_access_as_app** permission.
-

Configure Pull Interval for Office 365 Integration

Use this procedure to configure the interval period following which the IM and Presence Service pulls calendar information from Office 365.

Procedure

- Step 1** From Cisco Unified CM IM and Presence Administration, choose **System** > **Service Parameters**.
 - Step 2** From the **Server** drop-down, choose the IM and Presence publisher node.
 - Step 3** From the **Service** drop-down, choose **Cisco Presence Engine**.
 - Step 4** Configure an interval, in minutes for the **Office 365 Calendar Information Pull Interval** service parameter. The default is 60 minutes.
 - Step 5** Click **Save**.
-



Note The IM and Presence Service pulls information from Office 365 at scheduled intervals as specified by the **Office 365 Calendar Information Pull Interval** service parameter (default value is 60 minutes). However, there is no mechanism for pushing information from Office 365 to the IM and Presence Service. As a result, if a non-scheduled Presence update occurs in Office 365 between scheduled pulls (for example, an ad hoc meeting), the results do not register with the IM and Presence Service until after the next scheduled pull.

What to do next

Enable calendaring for IM and Presence Service users. To enable the feature for a large number of users at once, you can use either an LDAP sync for users whom are synced from an external LDAP directory, or the Bulk Administration Tool for non-LDAP users. Otherwise, you can enable the feature for users on an individual basis.

- [Enable Calendaring for LDAP Synchronized Users, on page 6](#)
- [Enable Calendar Integrations by Bulk, on page 8](#)
- [Enable Calendar Integration for a User, on page 8](#)

Configure Service Parameters for Exchange Integration

Use this optional procedure to configure optional service parameters for Outlook calendar integration with a Microsoft Exchange server. The default values may be sufficient for many parameters.

Procedure

- Step 1** From Cisco Unified CM IM and Presence Administration, choose **System** > **Service Parameters**.
- Step 2** From the **Server** drop-down, choose the IM and Presence publisher node.
- Step 3** From the **Service** drop-down, choose **Cisco Presence Engine**.

Step 4 Under **Calendaring Configuration**, configure values for the following parameters:

Table 1: Service Parameters for Exchange Integration

Service Parameter	Description
Microsoft Exchange Notification Port	The port number that the Presence Engine will listen on for incoming notifications from the Exchange server. UDP is used for WebDav and TCP is used for EWS (Exchange Web Services). Possible values are 1024-65535 with a default value of 50020.
Calendar Spread (seconds)	This parameter specifies the range of duration in seconds. Each user will be assigned an offset duration by a hash. The duration will determine the number of seconds after the top-of-minute that meeting transitions will be sent. The duration can be shortened for smaller numbers of users (approx. users / 100 = seconds). It is used for WebDav and EWS (Exchange Web Services). The range of values is 0-59 with a default value of 50 seconds.
Exchange Timeout (seconds)	This parameter specifies the duration, in seconds, before a request made to an Exchange server times out. This change requires a restart of the Cisco Presence Engine. The range of possible values is 1 - 20 with a default value of 3 seconds.
Exchange Queue	This parameter specifies the maximum length of the Exchange request queue. If a request is made and the queue length is exceeded, the request will fail and a recovery procedure will be initiated. This change requires a restart of the Cisco Presence Engine. Possible values are 1-5000 with a default value of 2200.
Exchange Threads	This parameter specifies the number of threads that are used to service Exchange requests. You can increase this value if there are a large number of users (for example, 5000) or if some Exchange transactions take longer than 3 seconds. If calendar integration is disabled, set this parameter to 1. This change requires a restart of the Cisco Presence Engine. Possible values are 1-100 with a default value of 60.
EWS Status Frequency (minutes)	This parameter specifies how often notification messages are sent from the Exchange server when EWS (Exchange Web Services) is used. The duration is in minutes. Possible values are 10 - 1440 with a default value of 60.

Step 5 Click **Save**.

What to do next

[Restart the Cisco Presence Engine, on page 6](#)

Restart the Cisco Presence Engine

If you changed the values for any of the Calendaring Configuration service parameters, restart the Cisco Presence Engine service.

Procedure

-
- Step 1** From Cisco Unified IM and Presence Serviceability, choose **Tools > Control Center - Feature Services**.
- Step 2** From the **Server** drop-down, choose the IM and Presence server and click **Go**.
- Step 3** Under **IM and Presence Services**, select **Cisco Presence Engine** and click **Restart**.
-

What to do next

Enable calendaring for IM and Presence Service users. To enable the feature for a large number of users at once, you can use an LDAP sync if users are synced from an external LDAP directory, or the Bulk Administration Tool for non-LDAP users. Otherwise, you can enable the feature for users on an individual basis.

- [Enable Calendaring for LDAP Synchronized Users, on page 6](#)
- [Enable Calendar Integrations by Bulk, on page 8](#)
- [Enable Calendar Integration for a User, on page 8](#)

Enable Calendaring for LDAP Synchronized Users

Complete these tasks to enable calendaring via the initial LDAP directory sync. You can use the initial LDAP sync to enable calendaring for users synced from the LDAP directory.

Procedure

	Command or Action	Purpose
Step 1	Add Calendar Integration to a Feature Group Template, on page 6	Assign calendaring to a feature group template.
Step 2	Add Feature Group Template to LDAP Sync, on page 7	Assign your calendaring-enabled feature group template to an LDAP directory sync and complete a sync.

Add Calendar Integration to a Feature Group Template

Use this procedure to assign Microsoft Outlook calendaring integration to a feature group template. You can use the template to configure Outlook calendar integration for all users synchronized from an LDAP directory



-
- Note** You can only add or edit feature group template settings for an LDAP directory that has not yet been synced. If the directory is already synced, use [Enable Calendar Integrations by Bulk, on page 8](#) instead.
-

Procedure

- Step 1** From Cisco Unified CM Administration, choose **User Management > User Phone/Add > Feature Group Template**.
- Step 2** Complete one of the following steps:
- Click **Add New** to create a new template.
 - Click **Find** and select an existing template
- Step 3** Check the **Enable User for Unified CM IM and Presence** check box
- Step 4** Check the **Include meeting information in Presence** check box
- Step 5** Complete the remaining fields in the **Feature Group Template** configuration window. For help with the fields and their settings, see the online help.
- Step 6** Click **Save**.
-

What to do next

[Add Feature Group Template to LDAP Sync, on page 7](#)

Add Feature Group Template to LDAP Sync

Use this procedure to assign the calendaring-enabled feature group template that you just created to an LDAP Directory sync. This will allow you to enable Outlook calendar integration for all users synced from this LDAP Directory.



Note You can only add a feature group template to an LDAP directory that has not yet been synced. If the directory is already synced, use [Enable Calendar Integrations by Bulk, on page 8](#) instead.

Before you begin

[Add Calendar Integration to a Feature Group Template, on page 6](#)

Procedure

- Step 1** From Cisco Unified CM Administration choose **System > LDAP > LDAP Directory**.
- Step 2** Click **Find** and select an existing LDAP Directory.
- Step 3** From the **Feature Group Template** drop-down menu, select the calendaring-enabled feature group template that you created in the previous task.
- Step 4** Complete the remaining fields in the **LDAP Directory** window. For help with the fields and their settings, see the online help.
- Step 5** Click **Save**.
- Step 6** Click **Perform Full Sync Now**.
-

Enable Calendar Integrations by Bulk

Use Bulk Administration to enable calendar integration for a large number of users in a single operation.

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:
- Bulk Administration > Users > Insert Users.**
 - Bulk Administration > Users > Update Users > Query.**
 - 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**.
-

Enable Calendar Integration for a User

Use this procedure to enable calendar integration for an IM and Presence Service 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**.
-