

Configure Integration of Office 365 (Microsoft Graph API) with IM&P for Calendar/Meeting and Out-of-Office Status in Jabber.

Introduction

This document describes the steps to configure "Calendar/Meeting and Out of Office status" for Cisco Jabber.

Prerequisites

Cisco recommends that you have knowledge of these topics:

- Windows/Mac
- Jabber
- Cisco Unified Communication Manager server(CUCM)
- Instant Messaging & Presence server(IMP)
- Office 365 account
- Microsoft outlook

Components Used

The information in this document is based on these software versions:

- CUCM 15SU4
- IMP 15SU4
- Jabber 15.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.



Note: Background Information Microsoft is deprecating EWS for third-party applications to integrate with Microsoft 365 and replacing it with Graph API. Starting October 1, 2026, Microsoft blocks EWS requests from non-Microsoft apps to Microsoft 365. For more details please refer [Field Notice](#).

Configure

Steps include configuring the “**Calendar/Meeting and Out of Office Status**” feature and integrating the IM&P server with Office 365.

Step 1. Configure Office 365 and Microsoft Graph API Permissions

1. Log in to the [Microsoft Azure portal](#)
2. Register a new application and obtain the Application (client) ID and Directory (tenant) ID using the [Instructions](#)
3. Create a Client Secret by Going to **Manage > Certificates & Secrets > New Client Secret**, then copy and save the client secret value.



Note: Use the same Application (client) ID, Directory (tenant) ID, and Client Secret when configuring the IM and Presence Service during Presence Gateway setup.

4. Go to **Manage > API Permissions > Add a permission**, then select Office 365 Exchange Online under “**APIs my organization use.**”
5. Click **Add an application permission** and Select Application permissions, choose *Calendars.ReadBasic.All*, and click Add permissions.



Note: To retrieve Out of Office information, also grant the *MailBoxSettings.Read* permission.

6. Navigate to **Manage > API permissions** and Under **Grant consent**, click *Grant admin consent for "Registered Azure Active Directory"*, then select **Yes**.
7. Verify that a green check mark appears in the Status column for the assigned permissions.

HOME | New | App registrations | IMP-Calendar

IMP-Calendar | API permissions

Search Refresh Got feedback?

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
 - Branding & properties
 - Authentication (Preview)
 - Certificates & secrets
 - Token configuration
 - API permissions**
 - Expose an API
 - App roles
 - Owners
 - Roles and administrators
 - Manifest
- Support + Troubleshooting
 - New support request

Successfully granted admin consent for the requested permissions.

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf are not affected.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the actual consent status.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for Cisco

API / Permissions name	Type	Description	Admin consent required	Status
Microsoft Graph (2)				
Calendars.ReadBasic.All	Application	Read basic details of calendars in all mailboxes	Yes	Granted for Cisco
MailboxSettings.Read	Application	Read all user mailbox settings	Yes	Granted for Cisco

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Step 2. Configuring the Office 365 Presence Gateway

Use these steps to configure the Presence Gateway on the IM and Presence (IM&P) server:

1. From **Cisco Unified CM IM and Presence Administration**, navigate to **Presence > Gateways**.
2. Click **Add New**.
3. From the **Presence Gateway Type** field, choose **Office 365 Server** from the drop down list
 - If **Office 365 Server** is selected, the **Authentication Type** defaults to **OAuth**.
 - The fields **Application (client) ID**, **Directory (tenant) ID**, and **Client Secret** apply only to Office 365 Server.
 - These values must match those configured in Step 1 on the Office 365 server.
4. In the **Description** field, enter a description to distinguish the presence gateway instance.
5. In the **Presence Gateway** field, enter the fully qualified domain name (FQDN) or IP address of the Presence Gateway server.



Warning: In the Account Name field, enter the account name created in Office 365. Enter the password for the account in both the Account Password and Confirm Password fields.

6. In the **Presence Gateway Port** field, enter the port used to connect to the calendaring service (default is 443)
7. In the **HTTP/HTTPS Proxy URL** field, enter the proxy server details if IM and Presence Service

does not have direct access to the Office 365 server.

Presence Gateway Type*	Office 365 Server
Authentication Type*	OAuth
Application (client) ID*	a318f438-f69f-49ba-a828-87523e970c11
Directory (tenant) ID*	cafae64a-ffb2-4585-8c11-2d86aa8b3bf5
Client Secret*
Description*	O365 config
Presence Gateway*	graph.microsoft.com
Account Name*@cisco.....onmicrosoft.com
Account Password*
Confirm Password*
Presence Gateway Port*	443
HTTP/HTTPS Proxy URL	http://proxy.....cisco.com:8080
HTTP/HTTPS Proxy Username	
HTTP/HTTPS Proxy Password	

Step 3. Upload Microsoft Certificates to IM and Presence Service

1. Download the Office 365 root certificate and intermediate certificate. Refer to the link for the list of supported root and intermediate [certificates](#):
2. Upload all downloaded certificates to the **cup-trust** and **tomcat-trust** stores on all the IM and Presence Servers

Step 4. Enable Calendar Out of Office in IM and Presence Cluster

1. From **Cisco Unified CM IM and Presence Administration**, choose **System > Service Parameters**.
2. From the **Server** drop-down list, select the **IM and Presence publisher node**.
3. From the **Service** drop-down list, select **Cisco Presence Engine**.
4. In the **Calendar Out of Office information** service parameter, select **Display Out of Office availability** to update the user's availability status in Cisco Jabber to **"Out of Office"** whenever it is set in Microsoft Office 365 or Exchange.
5. Click **Save**.

Calendaring Configuration (Parameters that apply to all servers)

Calendar Spread (seconds) *	<input type="text" value="50"/>
Exchange Timeout (seconds) *	<input type="text" value="3"/>
Exchange Quota *	<input type="text" value="2200"/>
Exchange Threads *	<input type="text" value="60"/>
EWS Status Frequency (minutes) *	<input type="text" value="60"/>
Office 365 Calendar Information Pull Interval (minutes) *	<input type="text" value="60"/>
FIPS Mode Exchange Server Authentication *	<input type="text" value="Auto"/>
Calendar Out of Office information *	<input type="text" value="Display Out of Office availability"/>

The 'Calendar Out of Office information' dropdown menu is expanded, showing three options: 'Display Out of Office availability', 'Display Out of Office availability', and 'Display Out of Office availability'. The bottom option is highlighted in blue.

Step 5. Restart the Cisco Presence Engine

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

Database and Admin Services			
	Service Name	Status	Activation Status
<input checked="" type="radio"/>	Cisco AXL Web Service	Started	Wed Feb 11 09:49:43 2026
<input type="radio"/>	Cisco Bulk Provisioning Service	Started	Wed Feb 11 09:49:44 2026

Performance and Monitoring Services			
	Service Name	Status	Activation Status
<input type="radio"/>	Cisco Serviceability Reporter	Started	Wed Feb 11 09:49:42 2026

IM and Presence Services			
	Service Name	Status	Activation Status
<input type="radio"/>	Cisco Presence Engine	Started	Wed Feb 11 10:16:43 2026
<input type="radio"/>	Cisco XCP Text Conference Manager	Started	Wed Feb 11 21:40:11 2026
<input type="radio"/>	Cisco XCP Web Connection Manager	Started	Wed Feb 11 21:33:12 2026
<input type="radio"/>	Cisco XCP Connection Manager	Started	Wed Feb 11 21:33:12 2026
<input type="radio"/>	Cisco XCP SIP Federation Connection Manager	Not Running	Wed Feb 11 21:33:12 2026
<input type="radio"/>	Cisco XCP XMPP Federation Connection Manager	Started	Wed Feb 11 21:33:12 2026
<input type="radio"/>	Cisco XCP File Transfer Manager	Started	Wed Feb 11 21:33:12 2026
<input type="radio"/>	Cisco XCP Message Archiver	Not Running	Wed Feb 11 21:33:12 2026
<input type="radio"/>	Cisco XCP Directory Service	Started	Wed Feb 11 21:33:12 2026
<input type="radio"/>	Cisco XCP Authentication Service	Started	Wed Feb 11 21:33:12 2026

Step 6. Configure End User for Calendaring integration

1. Go to cucm administrator > **Navigate to User Management** > **End User** and click Find to display the full list of end users. Select user from the list and check the box **Include meeting information in presence**

End User Configuration

Save Delete Add New Revoke Refresh Token

User ID* shabbsye

Password **Edit Credential**

Confirm Password

Self-Service User ID

PIN **Edit Credential**

Confirm PIN

Last name* Syed

Middle name

First name Shabbir

Display name Shabbir Syed

Title Mr.

Directory URI

Telephone Number 2010

Home Number

Mobile Number

Pager Number

Mail ID

Manager User ID

Department Cisco TAC

User Locale < None >

Associated PC/Site Code

Digest Credentials

Confirm Digest Credentials

User Profile Use System Default("Standard (Factory Default) Us" [View Details](#)

User Rank* 1-Default User Rank

Service Settings

Home Cluster

Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)

Include meeting information in presence(Requires Exchange Presence Gateway to be configured on CUCM IM and Presence server)

[Presence Viewer for User](#)

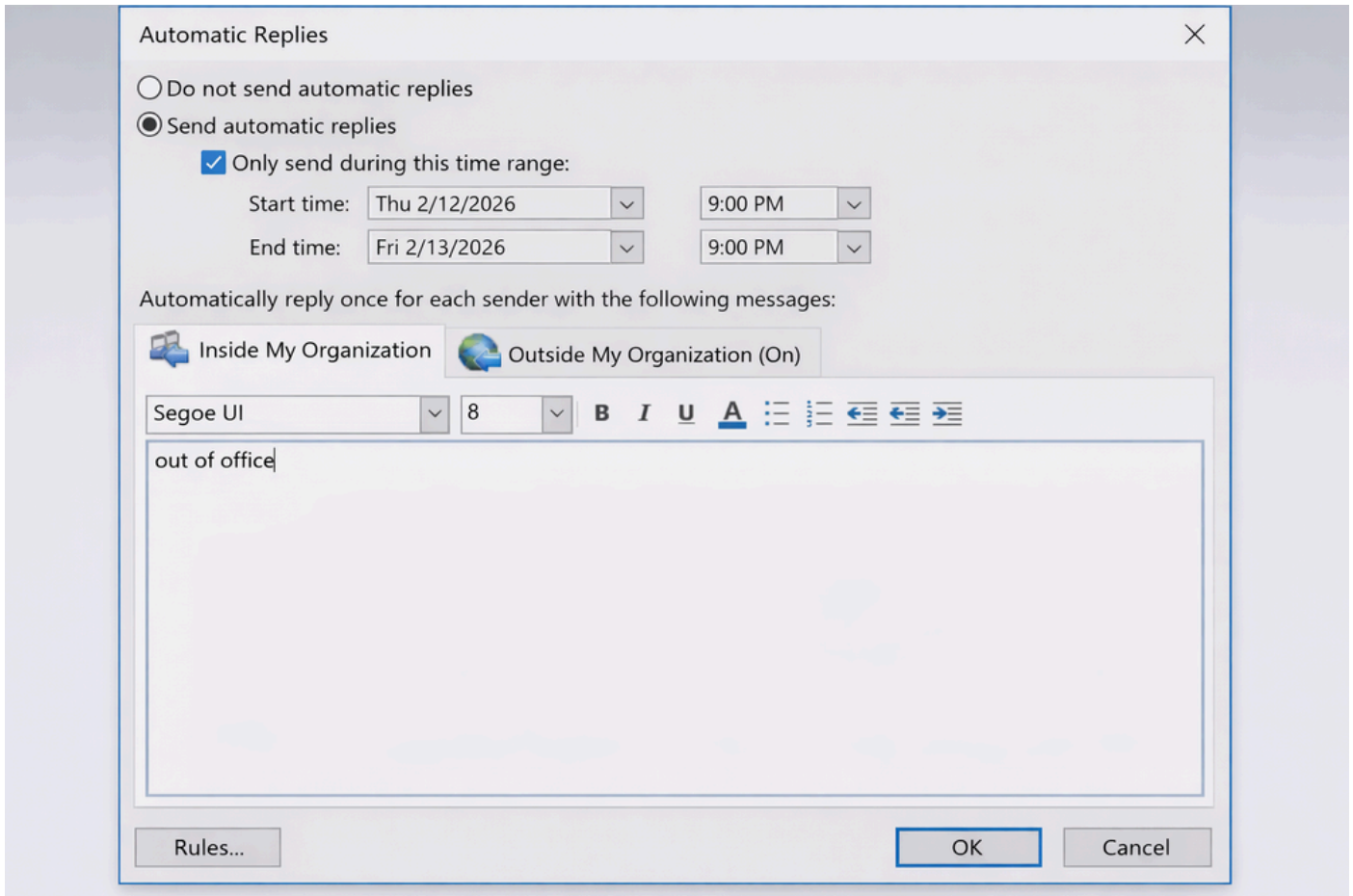
UC Service Profile user1-SP [View Details](#)

Verify

Step 1. Verify 'Out of office' Status

1. Apply and Test the Out of Office Configuration, We configure the **Out of Office** and test with user account on jabber

Open Outlook (a shortcut is in the Windows taskbar). Go to File > **Automatic Replies (Out of Office)** and check the box Send automatic replies.

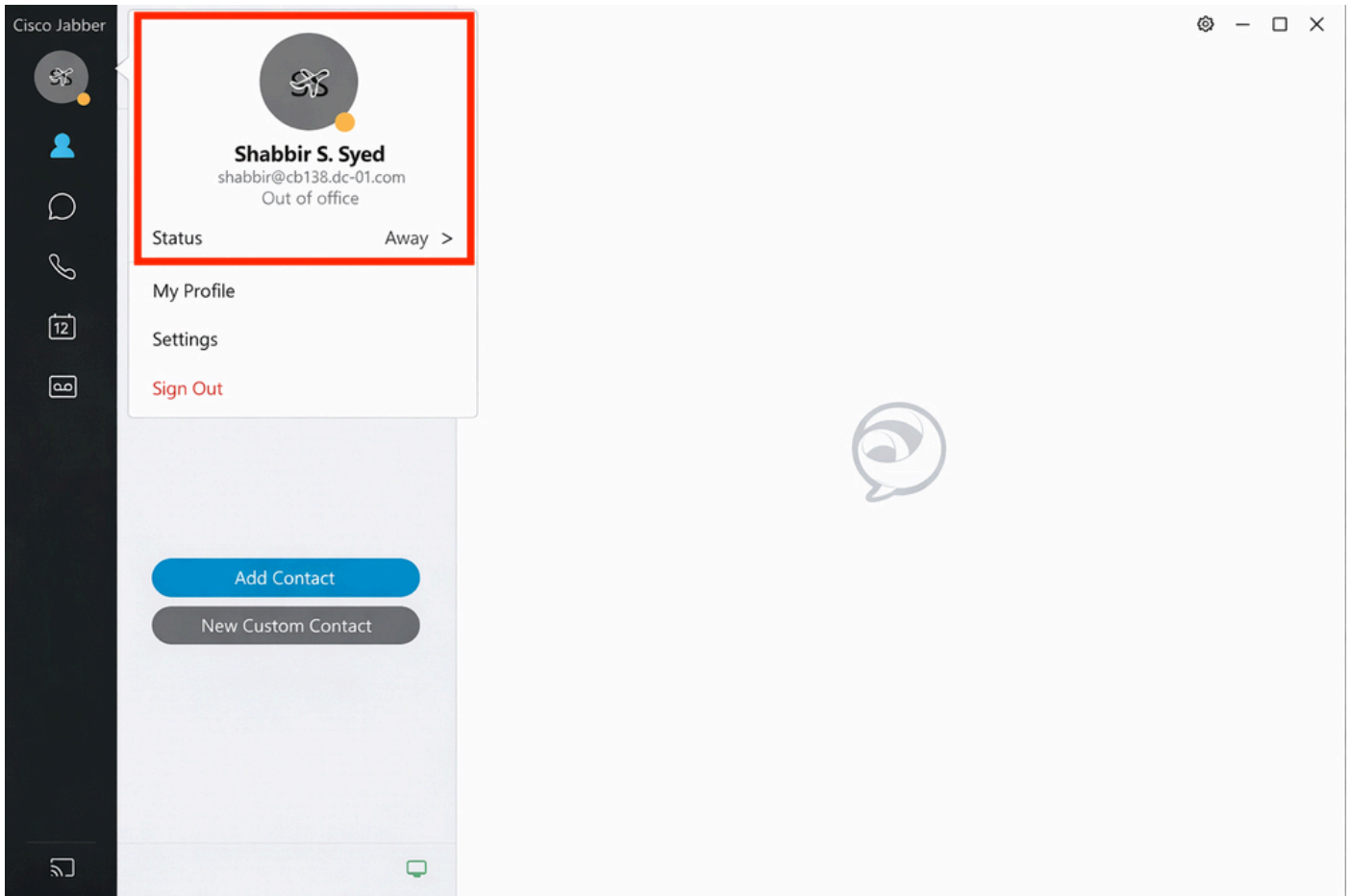


2. Add any Out of Office message into the **Automatically reply field for Inside / Outside MyOrganization**. Click OK to activate Out of Office on Exchange.



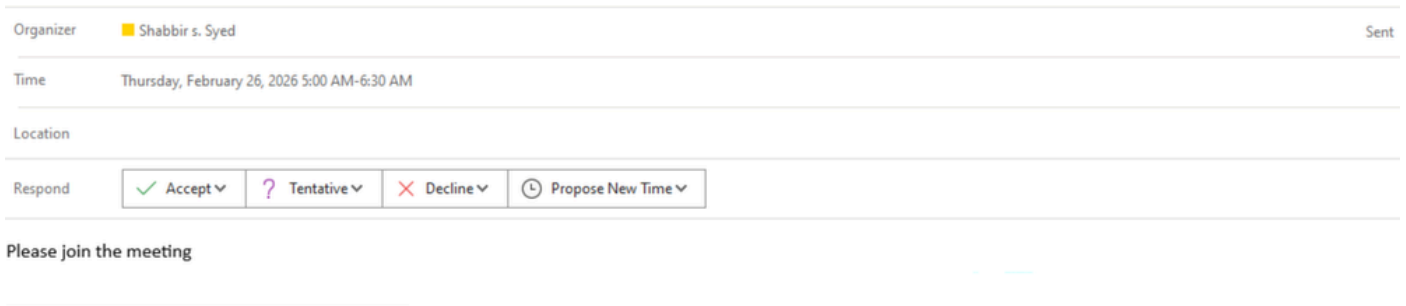
Note: By default, IM&P retrieves this information from Office 365 and updates the client every 60 minutes. This interval can be reduced to a minimum of 10 minutes. In Step 4, there is an option called the Office 365 Calendar Pull Information Timer, which is set to 60 minutes by default; you can change it to 10 minutes if required. If an immediate update is needed, restart the Presence Engine service, ensuring this is performed during a maintenance window.

Navigate back to the Jabber client; you can notice the out-of-office icon showing on your profile.



Step 2. Verify 'Calendar Meeting' status

Schedule a calendar meeting in your Outlook.



Verify the status in the Jabber client; it displays as “In a meeting.”



Shabbir s. Syed
shabbir@dcloud.cisco.com

Status In a meeting >

My Profile

Settings

Sign Out

Add Contact

New Custom Contact

