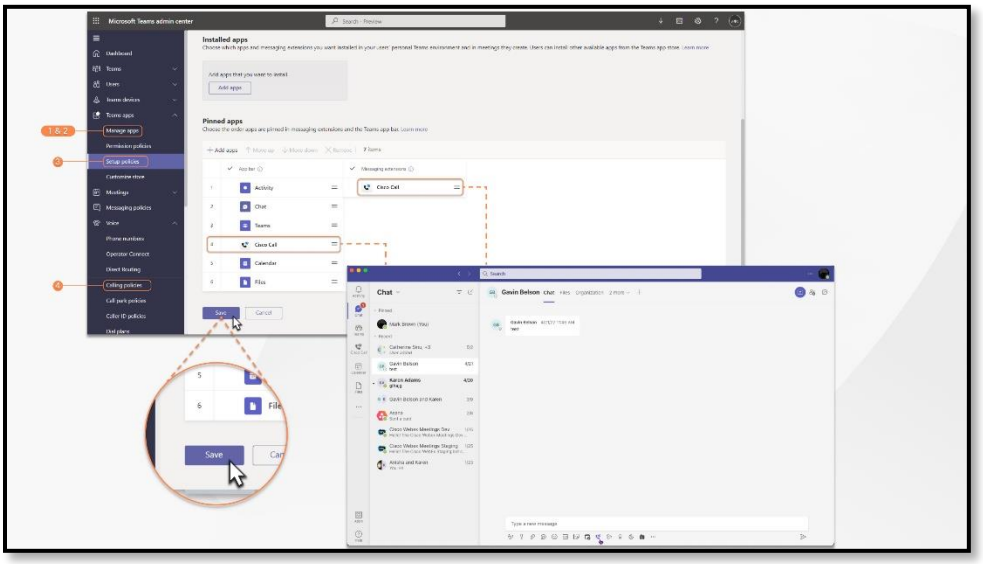
ProConnect with Cisco Call for Teams

Description

This document outlines the steps required to authorize the Cisco Call app in your Microsoft Teams environment.

Teams Tenant Admin (Customer) Tasks



1. Sign in to Teams admin center to manage your apps and allow Cisco Call.
    a. In the Dashboard menu, go to Teams apps > Manage apps.
    b. In the search box, enter Cisco Call and select the app name, then click Allow > Allow.
    c. When you allow an app on the Manage apps page, it's allowed org-wide.
2. Manage who can install Cisco Call.
    a. In the Dashboard menu, go to Teams apps > Manage apps.
    b. In the search box, enter Cisco Call and select the app name to open its details page.
    c. Click the Users and groups tab, and then click Edit availability.
    d. Select the following required options:
        i. Everyone—Select this option to allow all users, including users in your organization and external users to install Cisco Call.

ii. Specific users or groups—Select this option to allow only selected users or groups to install Cisco Call. When assigning this option, search for the user or the group from the Search for users or groups menu.
iii. No one—Select this option if you don't want anyone to install Cisco Call.

e. Click Apply.

3. Install Cisco Call, then add the icon to the Webex App and unpin the built-in calling option.
   a. In the Dashboard menu, go to Teams apps and click Setup policies > + Add. Give the new policy a name.
   b. Under Installed apps, click +Add apps and search for Cisco Call.
   c. Hover over the app name and click Add > Add.
   d. Under Pinned apps, click +Add apps and search for Cisco Call.
   e. Hover over the app name and click Add > Add.
   f. To unpin the built-in calling option, remove Calling from the App bar list.

Make sure Cisco Call is added to the top of both the App bar column list, and to the Messaging extensions column.

   g. Click Save.

The Cisco Call is pinned to the apps menu and as a messaging extension for all users.

4. Optional—disable the built-in calling option org-wide and make Cisco Call the only call option:
   a. In the Dashboard menu, go to Voice > Calling policies.
   b. Select the Default policy (or create a new policy).
   c. Turn Make private calls to Off, then click Save.

Accept presence sync permissions

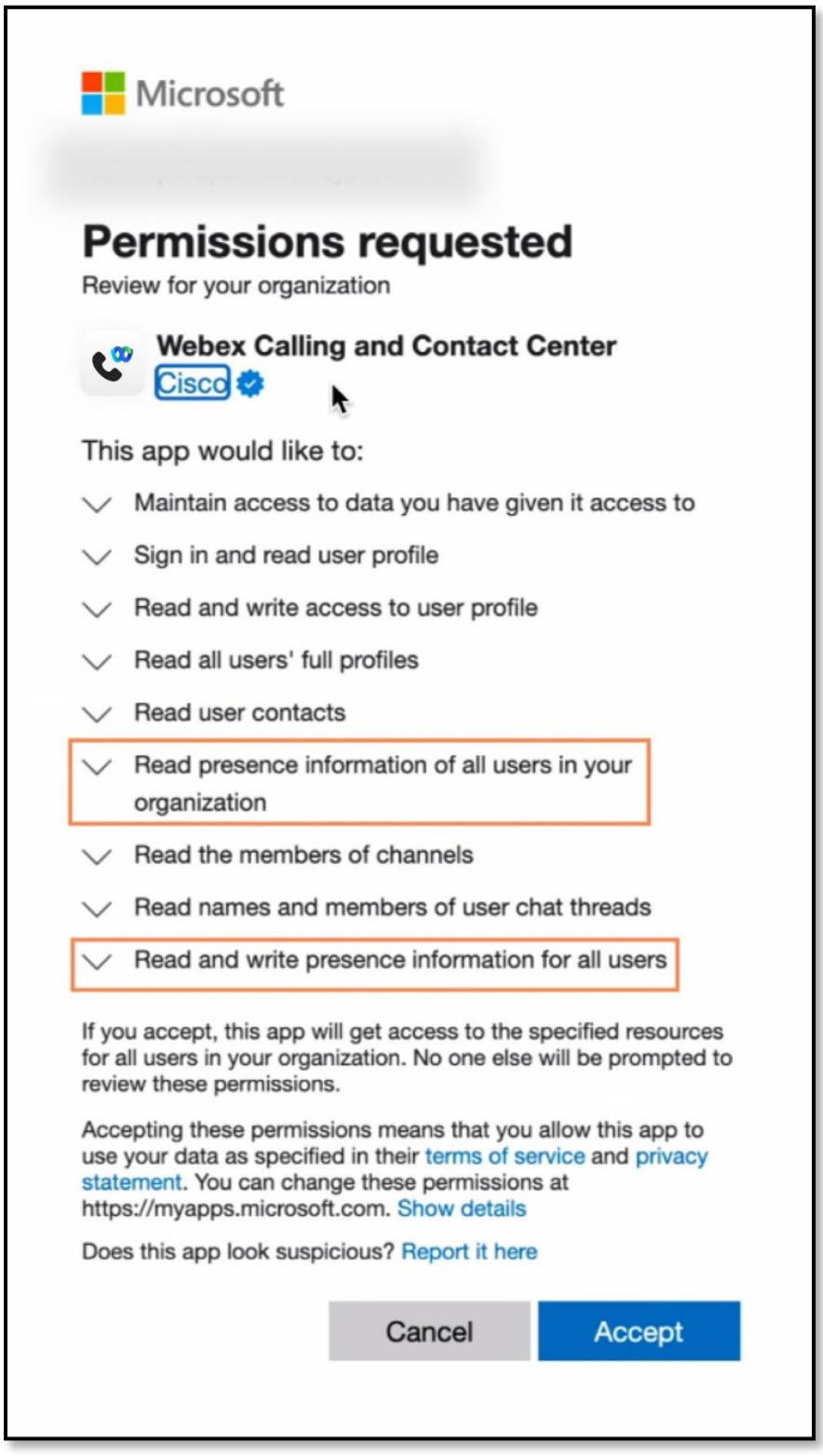
Review and accept the presence sync permissions in Microsoft Teams to bidirectionally synchronize the user's presence status between Microsoft Teams and Webex.

1. In the Dashboard menu, go to Teams apps > Manage apps
2. In the search box, enter Cisco Call and select the app name to open its details page.
3. Click the Permissions tab, and then click Grant admin consent.
4. Check if the following permissions are included.

a. Read Presence information of all users in your organization
b. Read and write Presence information for all users.

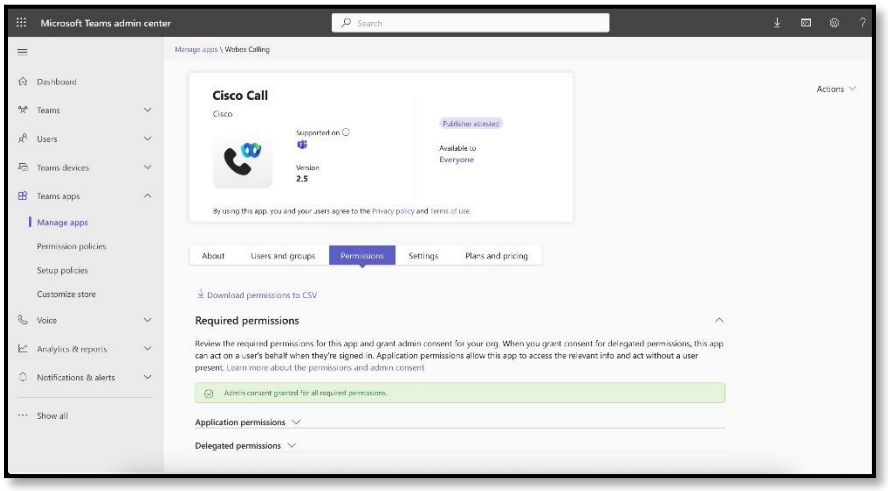
fidium business

ProConnect with Cisco Call for Teams



Revised **Dec**. 06, 2024

5. Click Accept to accept the permissions.
6. Ensure that new permissions are showing up as granted:
    a. A confirmation in the permissions tab lets you know that consent is granted for the required permissions.



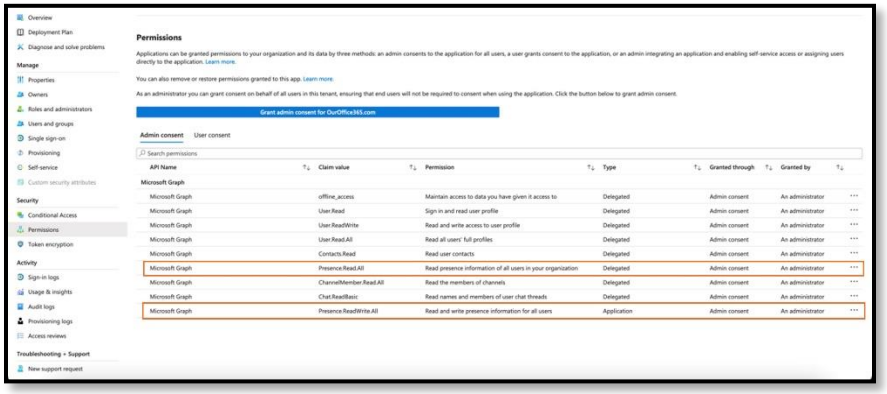
Confirmation screen in the permissions tab

Or

    b. Sign in to the Azure portal and then go to Microsoft Entra ID > Enterprise applications > Webex Calling > Security > Permissions.

The following permissions should be observed in the admin consent:

- Presence.ReadWrite.All
- Presence.Read
- Presence.Write



Permissions for Cisco Call and Microsoft Teams integration

The integration service uses Webex and Microsoft APIs to access data, such as call history, for displaying and updating statuses, such as marking voicemails as read, without storing any user data. All data transfers between the integration and the Webex/Microsoft backends occur over encrypted HTTPS channels. Thereby, the service ensures that user data are not stored in the cloud, strengthening the data privacy and security.

We request the minimum required permissions from Microsoft to call Microsoft API for enabling the integration functionality. The following table describes each permission that we request and why it's required.

Permission	Reason
offline_access	Allows the integration service to generate a new access token without asking the user to re-authorize often
User.Read	Allows the integration service to read the user's basic information such as the email address
User.ReadWrite	Allows the integration service to store speed dials in user profiles
User.Read.All	Allows the integration service to search for users in the active directory to make calls
Contacts.Read	Allows the integration service to search for the user's outlook contact to make calls
Presence.Read.All	Allows the integration service to subscribe for presence status changes
ChannelMember.Read.All	Allows the integration message extension to read members of a channel so that the user can search for a specific channel member to call
Chat.ReadBasic	Allows the integration message extension to read members of a group chat so that the user can search for a specific member to call
Presence.ReadWrite.All	Allow the integration service to subscribe for presence status change notifications