



## Chime for Teams Application Presence Polling Guide

January 2024

## Copyright and Disclaimer

This document, as well as the software described in it, is furnished under license of the Instant Technologies Software Evaluation Agreement and may be used or copied only in accordance with the terms of such license. The content of this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Instant Technologies. Instant Technologies assumes no responsibility or liability for any errors or inaccuracies that may appear in this document. All information in this document is confidential and proprietary.

Except as permitted by the Software Evaluation Agreement, no part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of Instant Technologies .

Copyright © 2005 - 2024 Instant Technologies, All rights reserved.

## Trademarks

All other trademarks are the property of their respective owners.

## Contact Information

See our website for Customer Support information.

<http://www.instant-tech.com/>



ISV/Software Solutions

## CONTENTS

Overview .....	3
Important Roles: .....	3
Configure Application Presence Permission.....	4
Configuring the Presence Settings in Chime .....	7
Grant Azure Admin Consent to the Application Changes .....	8

## OVERVIEW

This document is intended to assist with the setup of the Application Presence Polling feature within Chime that allows you to pull Agent and Manager presence in Microsoft Teams at an application level rather than utilizing a user's permissions to pull presence.

**Note:** This feature is recommended primarily for environments that are experiencing some presence outages with the current delegated user presence settings that are in place. If the existing presence settings are working for you, there is no additional benefit to changing the setting.

As part of this setup, we will need to do 3 main steps to have this feature fully configured:

1. Add the Presence Application Permission onto your Chime App Registration and have it approved by an Azure Admin.
2. Setup the Application Permission Setting in Chime Admin area.
3. Have an Azure Admin consent to the application changes that were made.

## IMPORTANT ROLES:

As part of this setup and configuration process, a tenant administrator for the Microsoft Office 365 tenant will need to perform several actions in order to provide the necessary authorization for the Chime server.

- Azure Admin with permissions to grant consent on App Registration Permission updates
- Chime Admin

## CONFIGURE APPLICATION PRESENCE PERMISSION

For this section of the guide, we cover the portion where the Azure Admin needs to set up permissions.

1. Navigate to <https://portal.azure.com/> and then Microsoft Entra ID (previously Azure Active Directory)
2. Click on the **App Registrations** option on the left-side menu.
3. Select the application that is used for your Chime deployment
4. In this new view, click the **API Permissions** button.

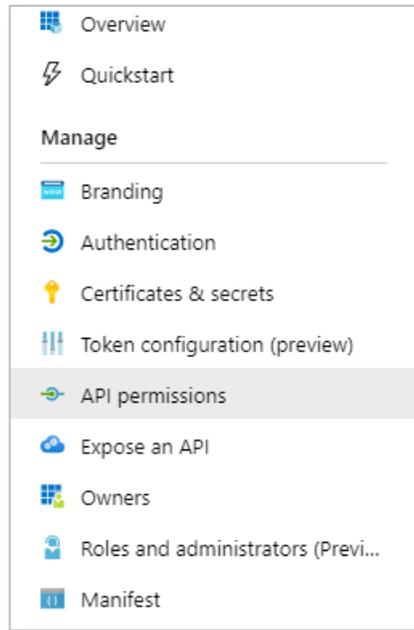


Figure 1: Access Required API Permissions

5. Click the **Add a Permission** button in the API Permissions window.

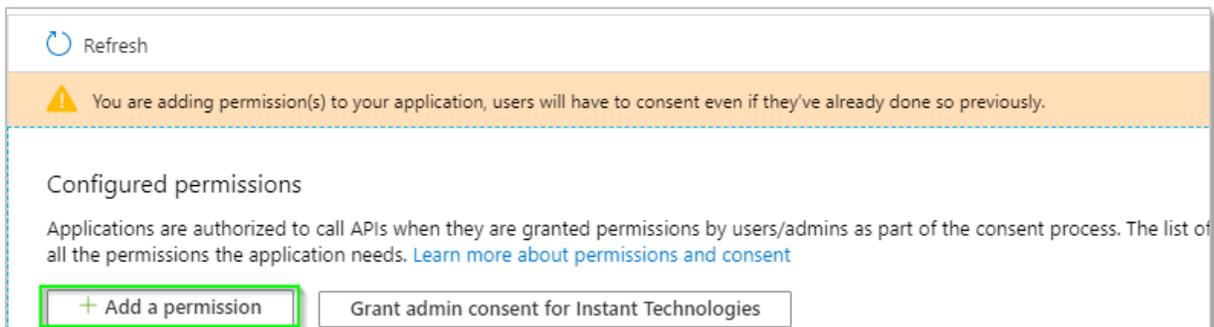


Figure 2: Add a Permission

6. Select **Microsoft Graph** from the list of Microsoft API's listed.

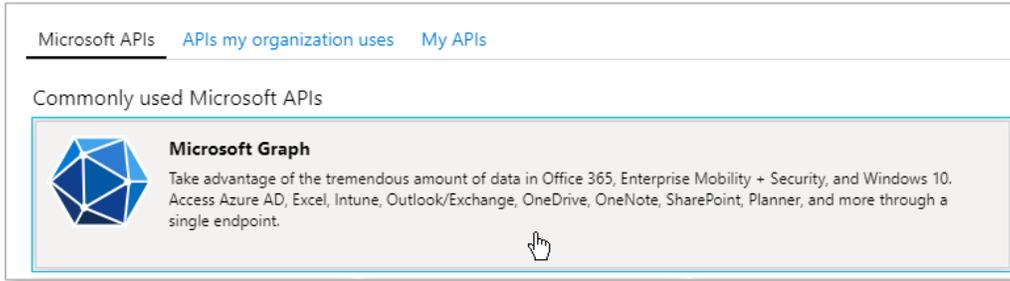


Figure 3: Select from Microsoft Graph API Permissions

7. Select **Application permissions**.
8. Use the search bar to find and add the following required permissions
  - a. Presence.ReadWrite.All

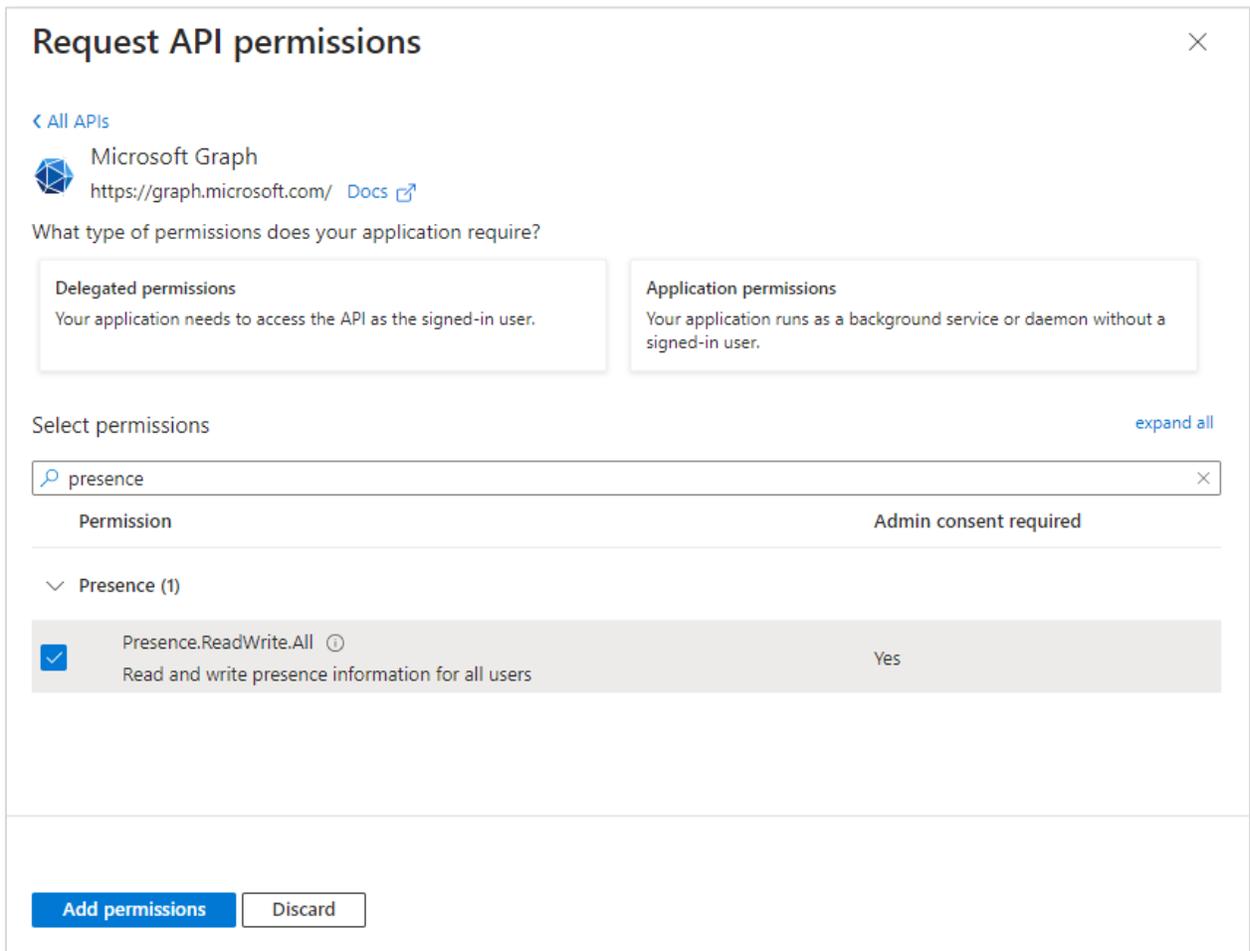


Figure 4: Configure Required Permissions

9. Click the **Add Permissions** button.

10. Finally, it is necessary to grant administrator consent for this permission. Click the Grant admin consent button.

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 Instant Technologies

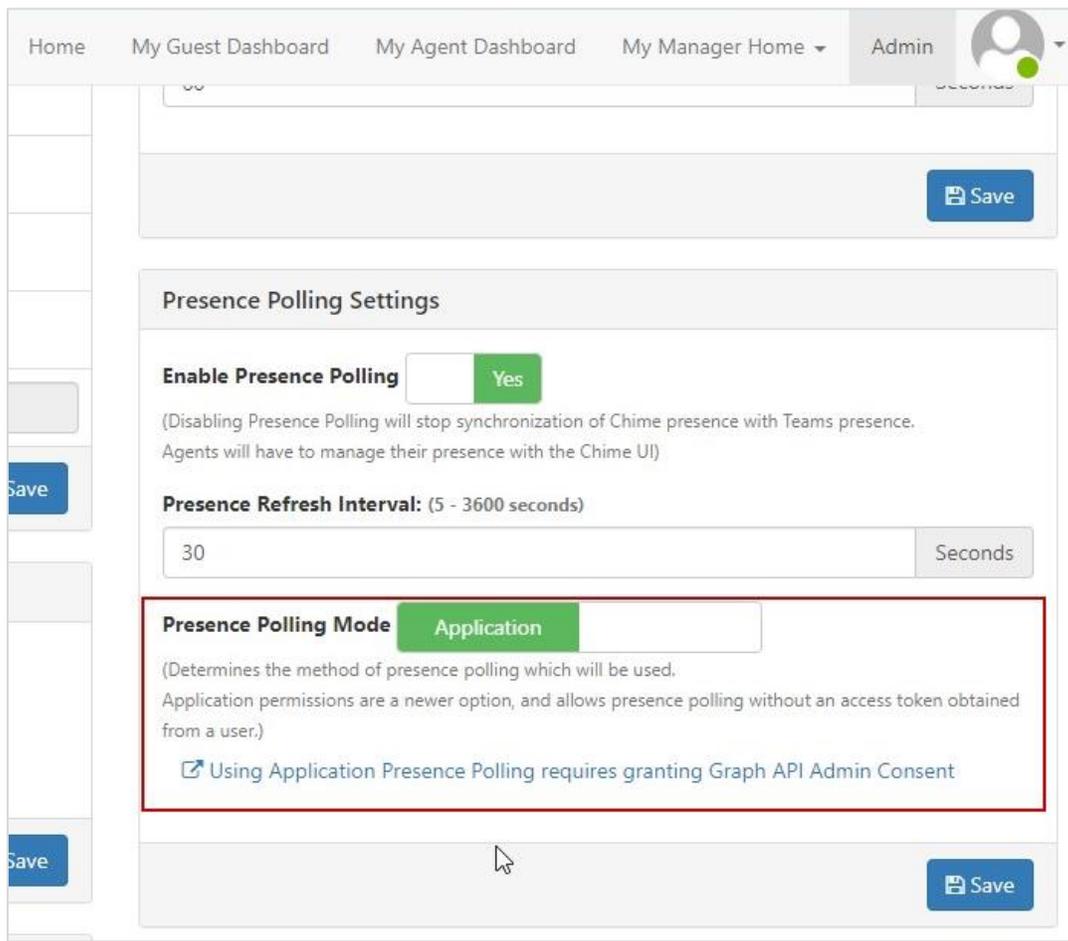
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (9) ...				
<a href="#">AppCatalog.ReadWrite.All</a>	Delegated	Read and write to all app catalogs	Yes	✔ Granted for Instant Tech... ...
<a href="#">Channel.ReadBasic.All</a>	Application	Read the names and descriptions of all channels	Yes	✔ Granted for Instant Tech... ...
<a href="#">Directory.Read.All</a>	Application	Read directory data	Yes	✔ Granted for Instant Tech... ...
<a href="#">Presence.Read.All</a>	Delegated	Read presence information of all users in your organization	No	✔ Granted for Instant Tech... ...
<a href="#">Team.ReadBasic.All</a>	Application	Get a list of all teams	Yes	✔ Granted for Instant Tech... ...
<a href="#">TeamMember.ReadWriteNonOw</a>	Application	Add and remove members with non-owner role for all tea...	Yes	✔ Granted for Instant Tech... ...
<a href="#">TeamsApp.ReadWrite</a>	Delegated	Manage user's Teams apps	No	✔ Granted for Instant Tech... ...
<a href="#">User.Read</a>	Delegated	Sign in and read user profile	No	✔ Granted for Instant Tech... ...
<a href="#">User.ReadBasic.All</a>	Delegated	Read all users' basic profiles	No	✔ Granted for Instant Tech... ...

Figure 5: Grant Admin Consent

## CONFIGURING THE PRESENCE SETTINGS IN CHIME

Once you have added the Presence.ReadWrite.All app permission, you will need to have a Chime Admin configure some settings within the Chime Admin areas. Follow these next steps to configure the Presence Polling Mode settings in Chime:

1. Navigate to the **Admin** area of your Chime application.
2. Click on **Settings**, then on the **Advanced** tab.
3. Scroll down to find the **Presence Polling Settings**.
4. Make sure **Enable Presence Polling** is set to **Yes**.



The screenshot shows the Chime Admin interface with the 'Admin' tab selected. The 'Presence Polling Settings' section is visible, containing the following configuration:

- Enable Presence Polling:** A toggle switch is set to 'Yes'.
- Presence Refresh Interval:** A text input field contains '30', with a 'Seconds' label to its right.
- Presence Polling Mode:** A dropdown menu is set to 'Application'. This section is highlighted with a red border.

Below the 'Presence Polling Mode' dropdown, there is a note: "(Determines the method of presence polling which will be used. Application permissions are a newer option, and allows presence polling without an access token obtained from a user.)" and a link: "Using Application Presence Polling requires granting Graph API Admin Consent".

Figure 6: Configure Presence Polling Mode

5. Set the **Presence Polling Mode** to **Application**.
6. Click **Save**.

## GRANT AZURE ADMIN CONSENT TO THE APPLICATION CHANGES

Now that Chime is configured to use the Application Presence Polling mode, you will need to have the Azure Admin grant consent for the application to use these settings.

1. Have an Azure Administrator click on the link within the **Presence Polling Settings** of the Chime Admin area:

➤ [Using Application Presence Polling requires granting Graph API Admin Consent](#)

2. Review the permissions listed in the request and make sure the new Presence.ReadWrite.All app permission is included in the list. Click that Accept button to fully enable these presence settings within Chime.

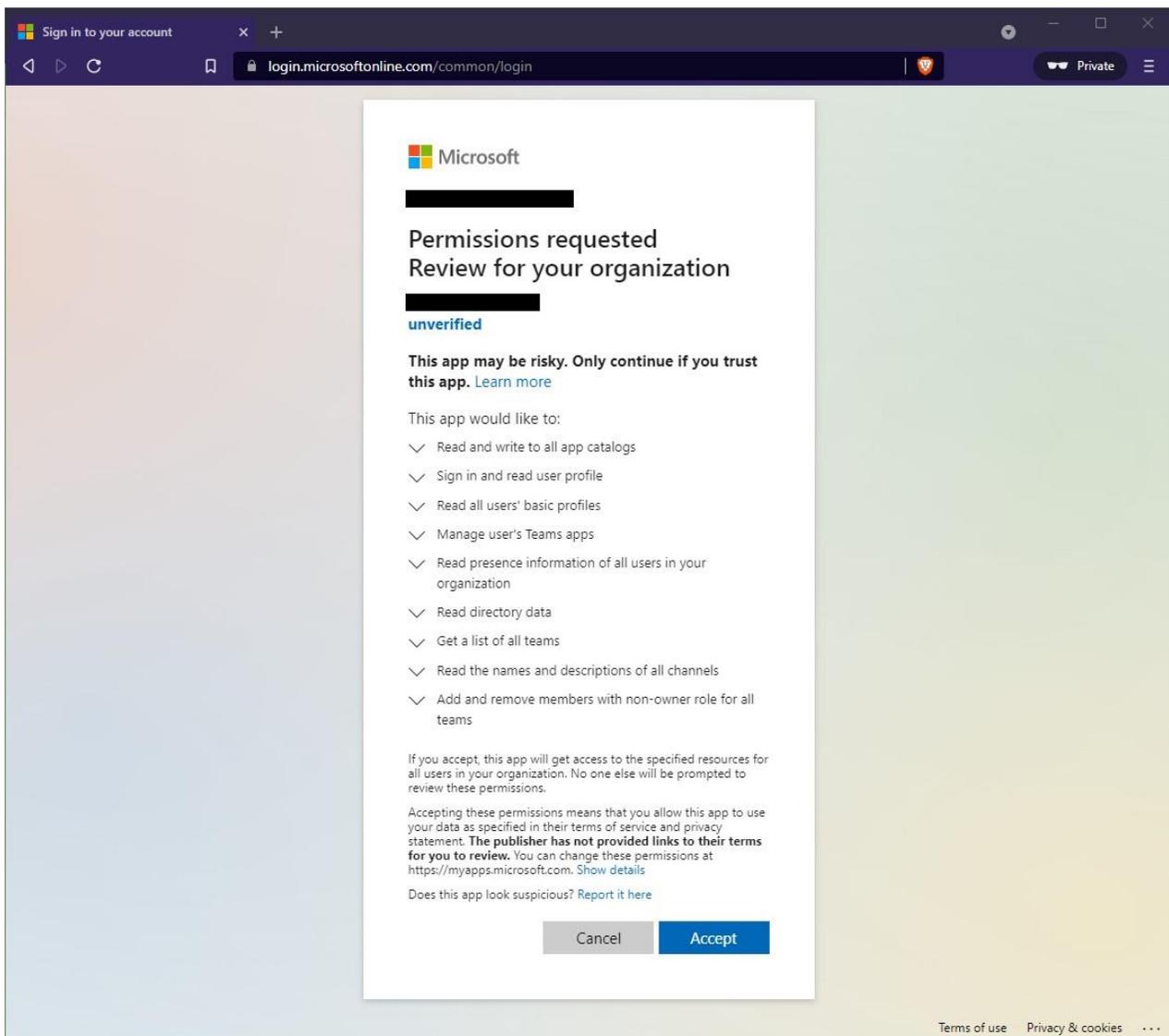


Figure 7: Accept New Chime App Permissions