Product Documentation:

Microsoft Teams Authentication & Permissions

Thought Industries Confidential — Copyright © 2023

Table of Contents

Overview

Authentication

The Microsoft Teams integration works by connecting the Thought Industries platform to a Thought Industries application that was created within Azure Active Directory. The method of authentication used is OAuth 2.0. In order to authenticate and connect an Microsoft Teams account, a user or Admin must simply log in and consent to the delegated permissions.

When a user grants consent, they are enabling the Thought Industries Azure app to access the necessary data in Microsoft for this integration to work.

> **Note:** With OAuth, Thought Industries customers will NOT need to register an app in Azure on their own (this can be necessary for other methods of authentication that are client ID and token-based.)

Granting Consent to Delegated Permissions

The following document includes links to a collection of Microsoft documentation that covers **how users will grant consent** to requested permissions during the initial setup of the Thought Industries Microsoft Teams integration. The actual user flow may depend on the user's role and their organization's settings in Microsoft.

The delegated permissions we request do NOT require Admin consent, so users should be able to grant consent for the permissions themselves. However, if user consent is turned off for an organization, users will be prompted to request Admin approval. In this case, we recommend using an Admin account to perform the initial integration setup. This will avoid any confusion that users may experience by having to track down the right person to request approval.

Admins can grant consent to permissions for themselves *and* can consent on behalf of their entire organization. When consent is granted for their entire organization, other users will not see a prompt for consent in the future.

Permissions

A user must grant consent for the following delegated permissions in order to use the Thought Industries Microsoft Teams Integration. None of these require Admin consent. Tracking scripts are pieces of code that are added by injecting these code pieces into various parts of the system.

Type	Permission	Display String	Description	Admin Consent Required?	Microsoft Account Supported?
User permissions	User.Read	Sign-in and read user profile	Allows users to sign-in to the app, and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.	No	Yes
Online meetings permissions	OnlineMeetings.ReadWrite	Read and Create Online Meetings.	Allows an app to create, read online meetings on behalf of the signed-in user.	No	No
Online meetings permissions	OnlineMeetingArtifact.Read.All	Read Online Meeting artifacts.	Allows the app to read online meeting artifacts on behalf of the signed-in user.	No	No
Calendars permissions	Calendars.ReadWrite	Have full access to user calendars	Allows the app to create, read, update, and delete events in user calendars.	No	Yes
OpenID Connect (OIDC) scopes	openid	Sign users in	By using this permission, an app can receive a unique identifier for the user in the form of the sub claim. The permission also gives the app access to the UserInfo endpoint. The openid scope can be used at the Microsoft identity platform token endpoint to acquire ID tokens. The app can use these tokens for authentication.	No	Yes
OpenID Connect (OIDC) scopes	email	View users' email address	Allows the app to read your users' primary email address.	No	Yes
OpenID Connect (OIDC) scopes	profile	View users' basic profile	Allows the app to see your users' basic profile (name, picture, user name).	No	Yes
OpenID Connect (OIDC) scopes	offline_access	Access user's data anytime	Allows the app to read and update user data, even when they are not currently using the app.	No	Yes

Consent

There are two Consent types to consider.

- User Consent
- Administrator Consent

User Consent

User consent happens when a user attempts to sign into an application. The user provides their sign-in credentials. These credentials are checked to determine whether consent has already been granted. If no previous record of user or admin consent for the required permissions exists, the user is shown a consent prompt, and asked to grant the application the requested permissions. In many cases, an admin may be required to grant consent on behalf of the user.

Administrator Consent

Depending on the permissions they require, some applications might require an administrator to be the one who grants consent. For example, application permissions and many high-privilege delegated permissions can only be consented to by an administrator. Administrators can grant consent for themselves or for the entire organization. For more information about user and admin consent, see user and admin consent overview.

User Consent Experience

There are two scenarios regarding user consent.

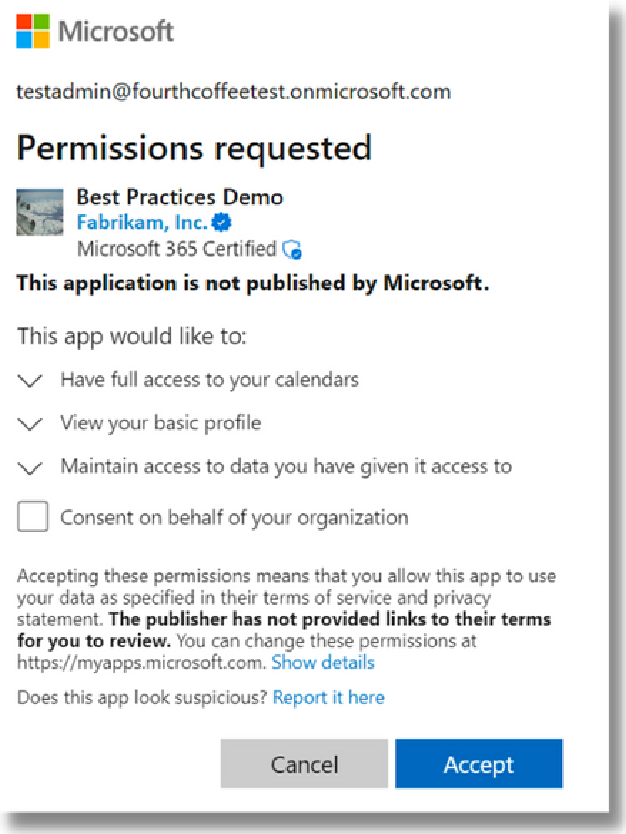
- App requires a permission that the user has the right to grant
- App requires a permission that the user has no right to grant

Scenario 1: App requires a permission that the user has the right to grant

In this consent scenario, the user accesses an app that requires a permission set that is within the user's scope of authority. The user is directed to the user consent flow.

Admins will see an additional control on the traditional consent prompt that will allow to give consent on behalf of the entire tenant. The control will be defaulted to off, so only when admins explicitly check the box will consent be granted on behalf of the entire tenant. The check box will only show for the Global Admin role, so Cloud Admin and App Admin won't see this checkbox.

View of Admin Consent Experience



Microsoft

testadmin@fourthcoffeetest.onmicrosoft.com

Permissions requested

Best Practices Demo
Fabrikam, Inc.
Microsoft 365 Certified

This application is not published by Microsoft.

This app would like to:

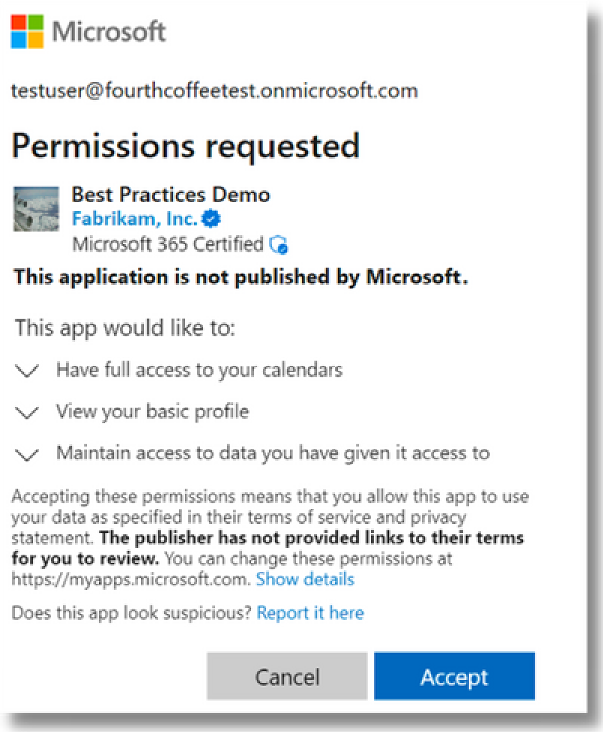
- Have full access to your calendars
- View your basic profile
- Maintain access to data you have given it access to

□ Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

View of User Consent Experience



Microsoft

testuser@fourthcoffeetest.onmicrosoft.com

Permissions requested

Best Practices Demo
Fabrikam, Inc.
Microsoft 365 Certified

This application is not published by Microsoft.

This app would like to:

- Have full access to your calendars
- View your basic profile
- Maintain access to data you have given it access to

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

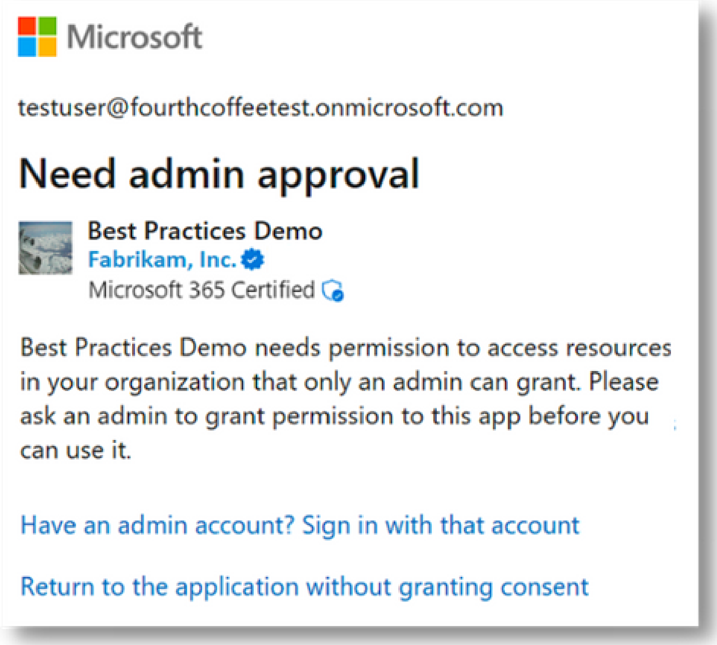
Does this app look suspicious? Report it here

Scenario 2: App requires a permission that the user has no right to grant

In this consent scenario, the user accesses an app that requires at least one permission that is outside the user's scope of authority.

Non-admin users will be blocked from granting consent to the application, and they'll be told to ask their admin for access to the app. If the admin consent workflow is enabled in the user's tenant, non-admin users are able to submit a request for admin approval from the consent prompt. For more information on admin consent workflow, see Admin consent workflow.

Admin Consent Workflow is Disabled



Microsoft

testuser@fourthcoffeetest.onmicrosoft.com

Need admin approval

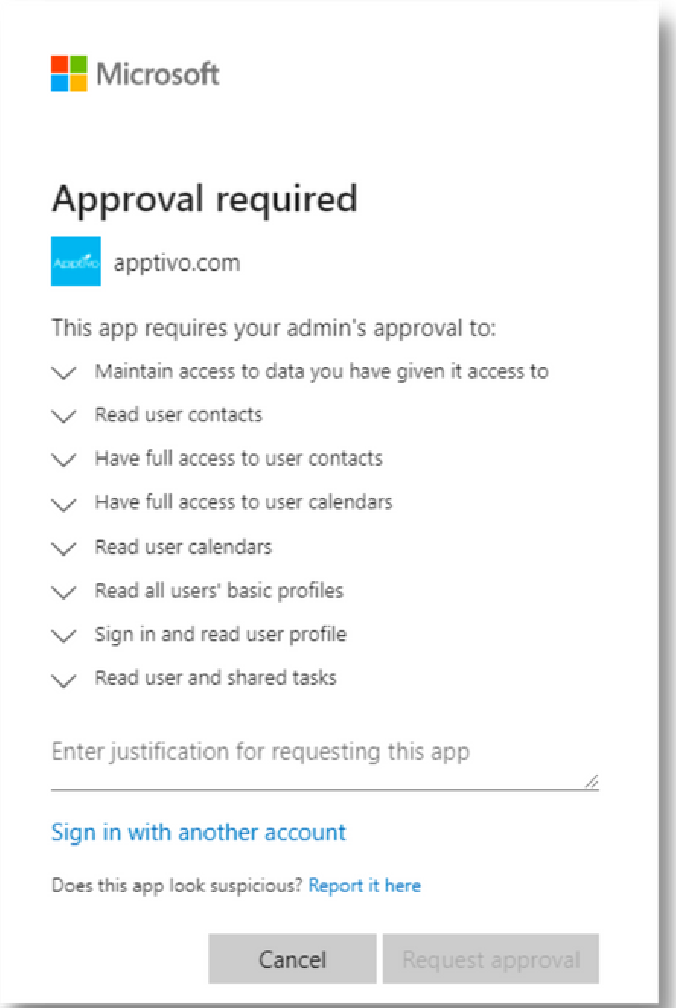
Best Practices Demo
Fabrikam, Inc.
Microsoft 365 Certified

Best Practices Demo needs permission to access resources in your organization that only an admin can grant. Please ask an admin to grant permission to this app before you can use it.

Have an admin account? Sign in with that account

Return to the application without granting consent

Admin Consent Workflow is Enabled



Microsoft

Approval required

apptivo.com

This app requires your admin's approval to:

- Maintain access to data you have given it access to
- Read user contacts
- Have full access to user contacts
- Have full access to user calendars
- Read user calendars
- Read all users' basic profiles
- Sign in and read user profile
- Read user and shared tasks

Enter justification for requesting this app

Sign in with another account

Does this app look suspicious? Report it here

Admin Consent Workflow

There may be situations where your end-users need to consent to permissions for applications that they're creating or using with their work accounts. However, non-admin users aren't allowed to consent to permissions that require admin consent. Also, users can't consent to applications when user consent is disabled in the user's tenant.

How the Admin Consent Workflow Works

Admin Consent through Azure Portal

Admin Roles that can consent to delegated permissions are the following:

- Application Administrator
- Cloud Application Administrator
- Global Administrator

Application Administrator

This role also grants the ability to consent for delegated permissions and application permissions, with the exception of application permissions for Microsoft Graph.

Cloud Application Administrator

This role also grants the ability to consent for delegated permissions and application permissions, with the exception of application permissions for Microsoft Graph.

Global Administrator

This is a more privileged role than Application Administrator. The person who signs up for the Azure AD organization becomes a Global Administrator. There can be more than one Global Administrator at your company. This role can Grant consent for any permission to any application.

Thought Industries Confidential — Copyright © 2023

Powering the Business of Learning

Thought INDUSTRIES

Thought Industries Confidential — Copyright © 2022