Administrator's Guide

AudioCodes Continuous Enterprise Productivity Powered by Voice.AI

Next Generation Meeting Insights

Notice

Date Published: July-10-2025

Security Vulnerabilities

All security vulnerabilities should be reported to vulnerability@audiocodes.com.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at https://www.audiocodes.com/services-support/maintenance-and-support.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at https://online.audiocodes.com/documentation-feedback.

Stay in the Loop with AudioCodes

Related Documentation

Document Name
Meeting Insights User's Manual

Document Revision Record

LTRT	Description
12726	Initial document release
12729	MIA auto-invite rule
12750	Power BI. Recording Notifications. Automatic AI. Meeting join & lobby in TAC.
12751	Microsoft Outlook Add-In. User Permissions.
12752	Internal / External Share. Provide permissions in customers' Azure enterprise applications. URL to sign in. Grant permission screenshots. AAD Group - security. AAD Group - Group type. AAD Group - Owners. Create AAD group of users. 'Licensing' separated from group. **Calendar** icon in Teams. New Meeting. Modified instructions for Scheduled | Unscheduled meetings. Outlook add-in restructured. Intro to 'Devices' changed. 'Insights' added to Add User Profile page under 'Automatic AI Triggering'. AI Settings: Transcript & AI Insights separated.
12753	Lock icon in Licensed Users page. Enable Zoom for group of users; view and reset voiceprints
12754	BYOS storage; note added for PowerPoint Live not supported; email notifications updated; publishing time preferences; TLS 1.2
12755	Salesforce integration
12756	Miscellaneous
12757	Salesforce limitation re overwriting existing content removed; Meeting Insights standalone mobile app (enabling app and enabling ad hoc recording for user profiles); Template-based AI-powered summaries
12758	Recording of Microsoft Teams meetings hosted by other organizations; retention period for audit trail and system activity log.
12759	Integration with Zoho for sending action items; AdminRole removed from Azure consent.

Table of Contents

1 Introduction

AudioCodes Meeting Insights is an AI-powered enterprise solution that enables users to record any meeting-generated content (audio and video), and automatically creates meeting minutes for Microsoft Teams meetings.

Meeting Insights records, transcribes, and organizes all aspects of online meetings. It provides a centralized company platform for all meetings, webinars and conference calls, making them easily shareable across the organization. It shifts the focus from individual access to meeting content, to a company-wide approach, aiding informed decision-making.

During the meeting, Meeting Insights' in-meeting voice assistant 'MIA' logs all notes, action items, decisions, and a summary, while allowing you to highlight specific areas in the meeting with one click so that you can easily locate them after the meeting. Meeting Insights provides regular recording options, enabling you to pause and resume recording anytime during the meeting.

Once the meeting recording has ended, you can use Meeting Insights' feature-rich and flexible web-based management tool to manage and edit the meeting recording. This includes publishing and sharing the meeting recording so that all participants and optionally, all or specific contacts in your organization, can also view it even if they weren't present (or invited), and editing the slide presentation (add, replace, or delete slides).

For more information about Meeting Insights, see AudioCodes' website.

Currently, Meeting Insights doesn't record shared content of **PowerPoint Live** in Teams.

Intended Audience

This guide is intended for the admin of the enterprise | organization.

2 Pre-Deployment Requirements

Before deploying Meeting Insights, customers must provide:

- Customer’s domain name
- Emails of customer contact point for the deployment status
- UPNs of default administrator for the initial access to the application
- Preferable region for recording storing (when a region is unavailable in Azure Cloud, a default region will be selected)

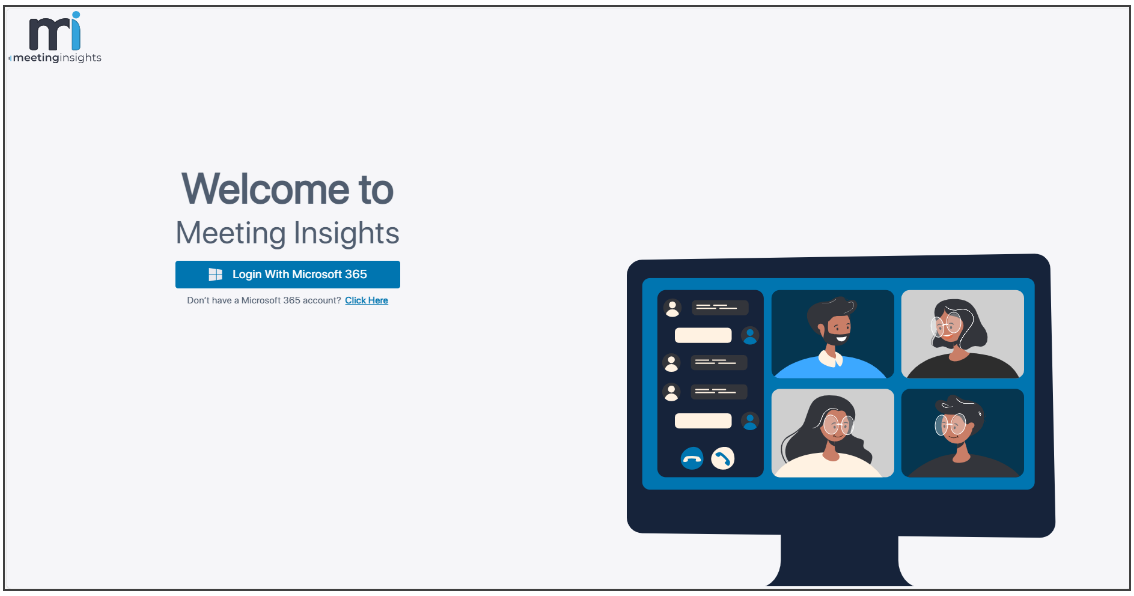
3 Signing in

Meeting Insights enables you to sign in as admin. Admin can perform management tasks which regular users cannot. Up to five admins are allowed.

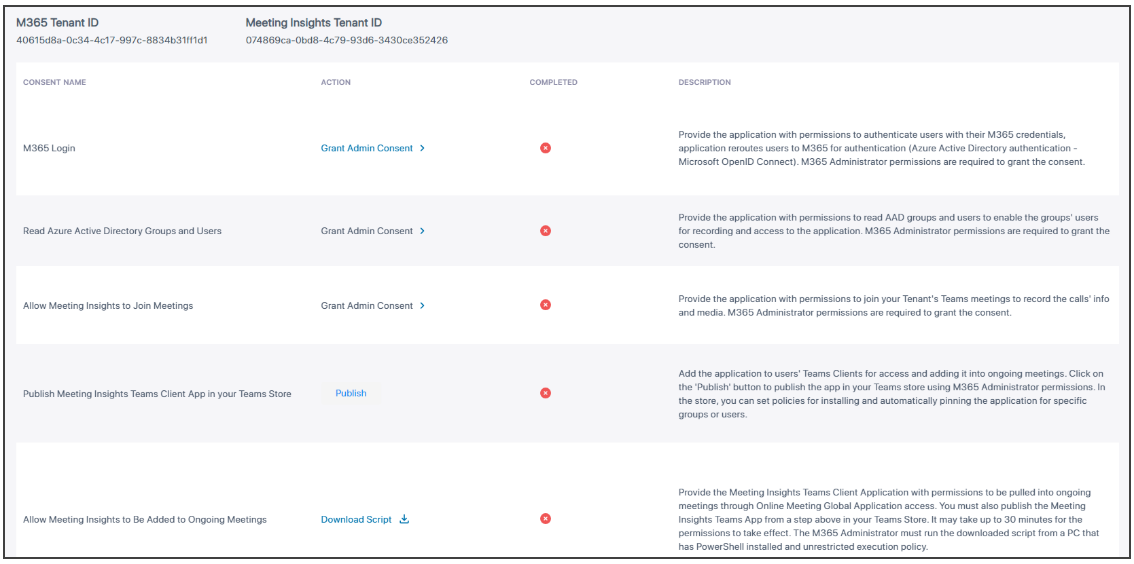
- Default admin is added when the customer application is created.
- Default admin receives an email when the app is ready for sign-in.
- Admin has full access permissions.
  - ✓ Admin has full access to system configuration and meetings.
  - ✓ Admin can act on behalf of the meeting owner and within the scope of the meeting owner's permissions, for example, admin can share a meeting externally if the meeting owner has permission to share externally.

➢ To sign in as admin:

1. Access the app at the link provided by AudioCodes in the email and paste it into your browser's address field. The link will be:
   - https://emea.meetinginsights.com/mi/login -OR-
   - https://americas.meetinginsights.com/mi/login



2. Click **Login with Microsoft 365** and then sign in with the default admin's UPN.



M365 Tenant ID
40615d8a-0c34-4c17-997c-8834b31ff1d1

Meeting Insights Tenant ID
074869ca-0bd8-4c79-93d6-3430ce352426

CONSENT NAME	ACTION	COMPLETED	DESCRIPTION
M365 Login	Grant Admin Consent ›		Provide the application with permissions to authenticate users with their M365 credentials, application reroutes users to M365 for authentication (Azure Active Directory authentication - Microsoft OpenID Connect). M365 Administrator permissions are required to grant the consent.
Read Azure Active Directory Groups and Users	Grant Admin Consent ›		Provide the application with permissions to read AAD groups and users to enable the groups' users for recording and access to the application. M365 Administrator permissions are required to grant the consent.
Allow Meeting Insights to Join Meetings	Grant Admin Consent ›		Provide the application with permissions to join your Tenant's Teams meetings to record the calls' info and media. M365 Administrator permissions are required to grant the consent.
Publish Meeting Insights Teams Client App in your Teams Store	Publish		Add the application to users' Teams Clients for access and adding it into ongoing meetings. Click on the 'Publish' button to publish the app in your Teams store using M365 Administrator permissions. In the store, you can set policies for installing and automatically pinning the application for specific groups or users.
Allow Meeting Insights to Be Added to Ongoing Meetings	Download Script		Provide the Meeting Insights Teams Client Application with permissions to be pulled into ongoing meetings through Online Meeting Global Application access. You must also publish the Meeting Insights Teams App from a step above in your Teams Store. It may take up to 30 minutes for the permissions to take effect. The M365 Administrator must run the downloaded script from a PC that has PowerShell installed and unrestricted execution policy.

3. You've successfully signed in. Next: Connect to Microsoft 365 as shown here.

4 Setting up Meeting Insights

Follow the three steps described here to set up Meeting Insights.

➢ **To set up the app:**

1. Configure an Azure Active Directory (AAD) group for Meeting Insights users as shown here.
2. Connect to your Microsoft 365 as shown here.
3. Assign a Meeting Insights license to your users group as shown here.

> After setting up Meeting Insights, test the setup as shown here.

Connecting to Microsoft 365

Connecting to Microsoft 365 requires admin to:

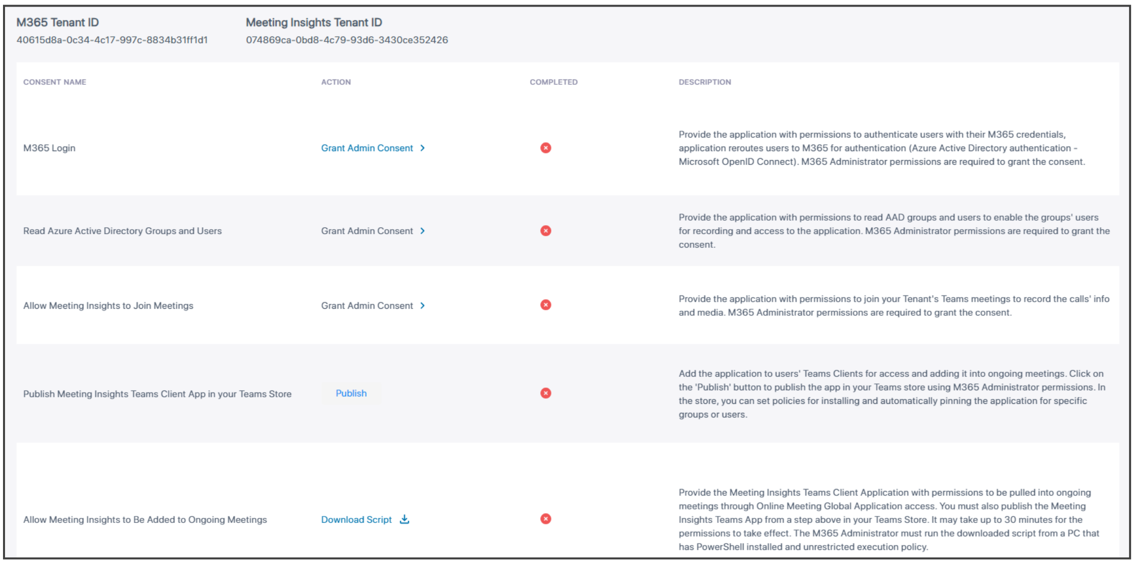
1. Grant three consents.
2. Publish the Meeting Insights Teams client app in the Teams Store.

> Optionally, admin can *manually* add the app to the Teams store *without needing to grant permissions*, as described in Adding Meeting Insights to Teams Client on page 41.

3. Download and run the script that allows the app to be added to ongoing meetings.

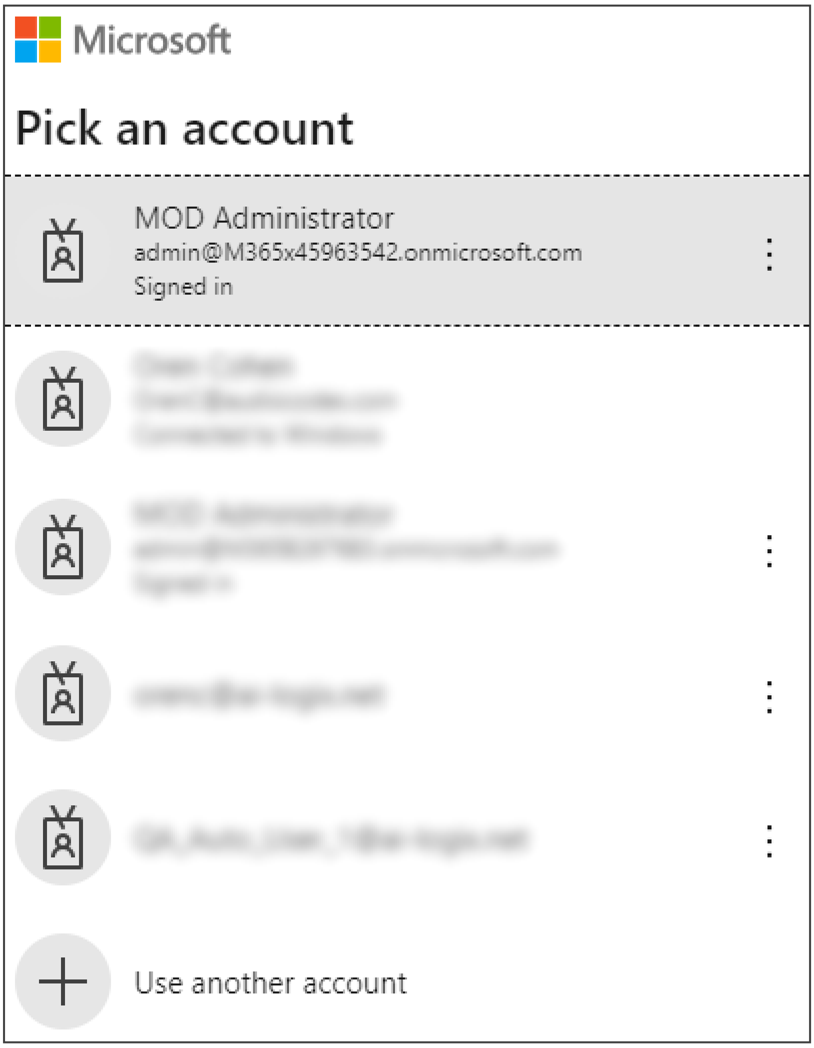
➢ **To connect to Microsoft 365:**

1. After signing in, the 'Connect to your M365' page is displayed (**Admin Settings** > **System Settings** > **Connect to your M365**).

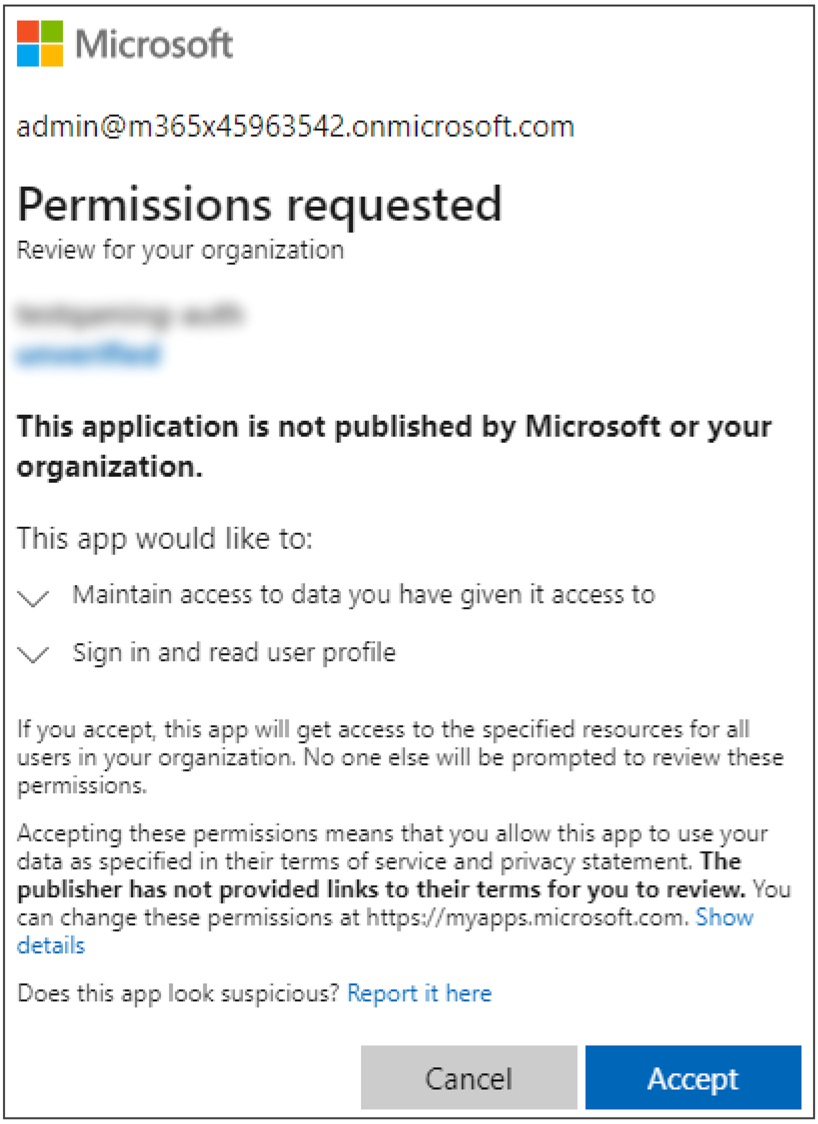


- Under the 'Completed' column, the icons indicate consent has not been granted yet and must be granted.
- The first consent is hyper linked indicating that this consent must be granted first.
- **Microsoft 365 Administrator permissions are required to grant each consent**.

2. Next to 'M365 Login', click **Grant Admin Consent**.

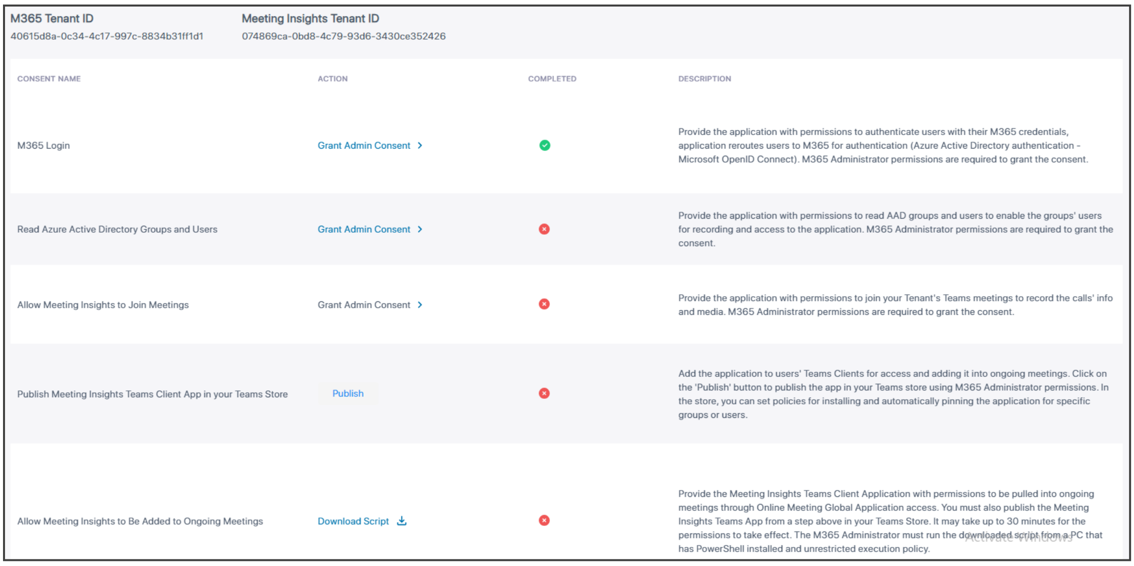


3. Click **+ Use another account** and in the prompts, enter the admin's email address and password.



- The consent provides the app with permission to authenticate users with your M365 credentials; the app reroutes users to M365 for authentication (Azure Active Directory authentication - Microsoft OpenID Connect).
- **M365 Administrator permissions are required to grant the consent.**

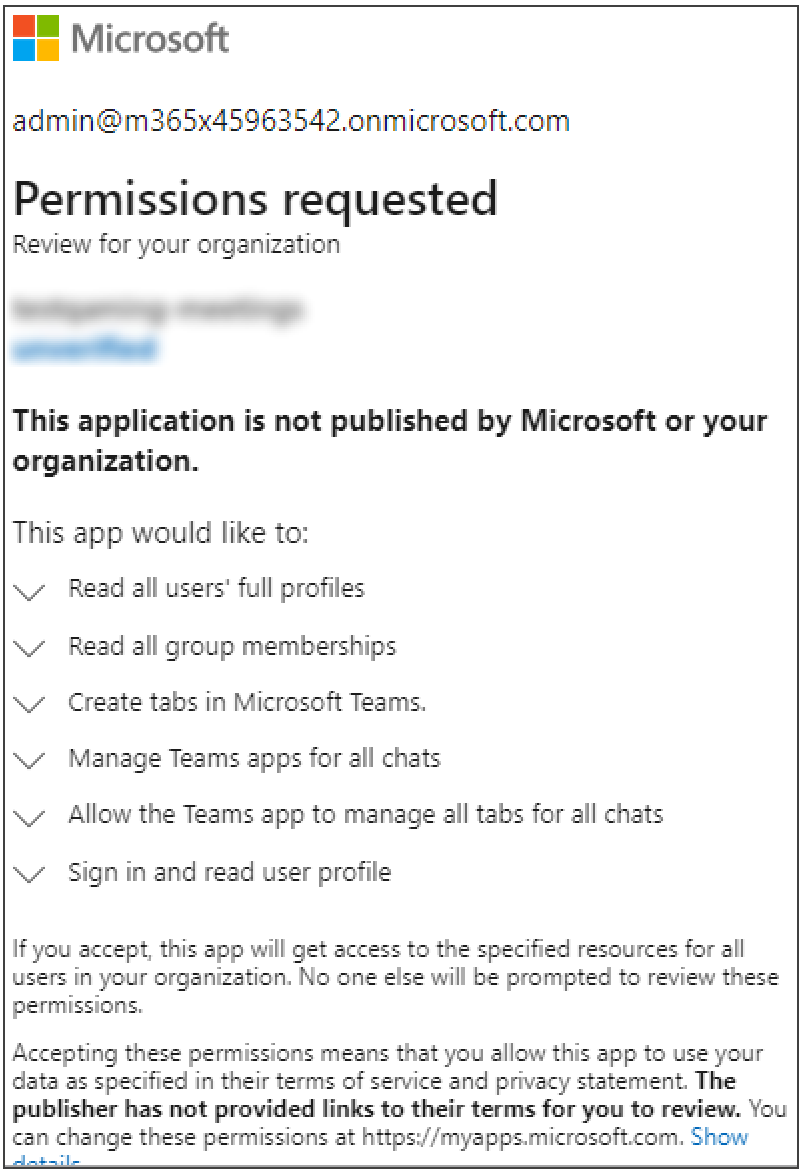
4. Click **Accept**.



5. View the icon under the 'Completed' column. It indicates you successfully granted consent (consent was successfully completed from this page for 'M365 Login'). You've successfully provided the app permission to authenticate users with your M365 credentials; the app reroutes users to M365 for authentication (Azure Active Directory authentication - Microsoft OpenID Connect).

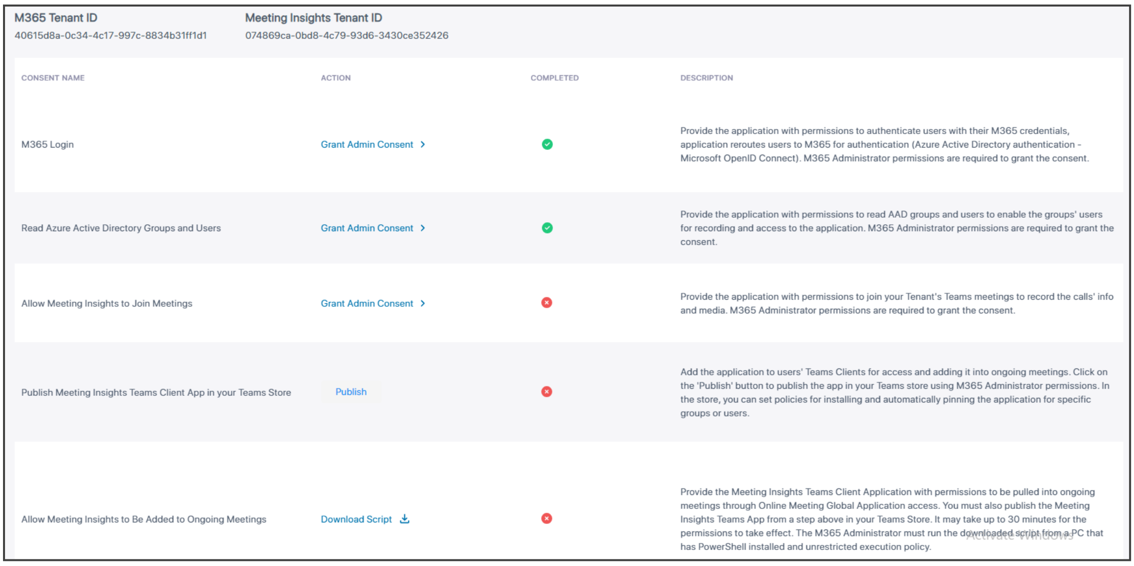
- Even if consent is later revoked, the icon stays green.
- The next consent down now becomes hyper linked for you to grant (Read AAD Groups and Users).
- **Microsoft 365 Administrator permissions are required to grant each consent**.

6. Next to ‘Read Azure AD Groups & Users’, click **Grant Admin Consent**, and then select the account.

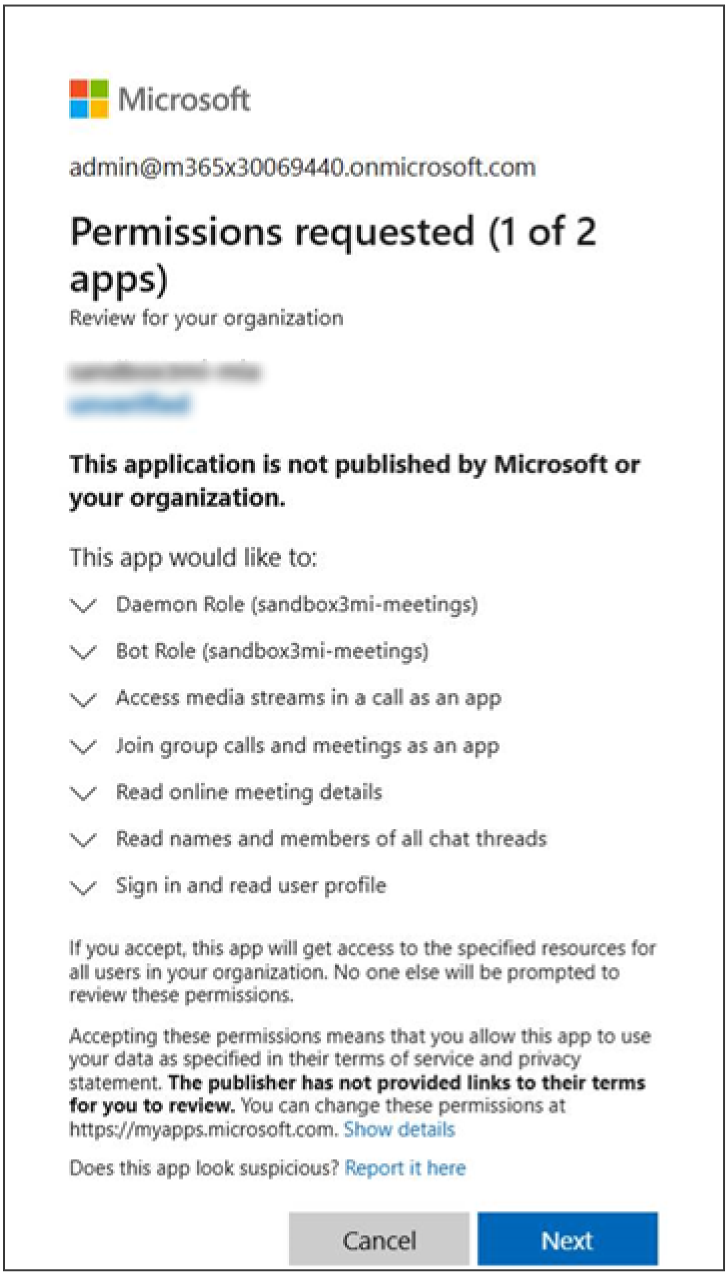


> ⚠ This consent provides the app with permission to read AAD groups and users, and permission for groups' users to access the app and record.

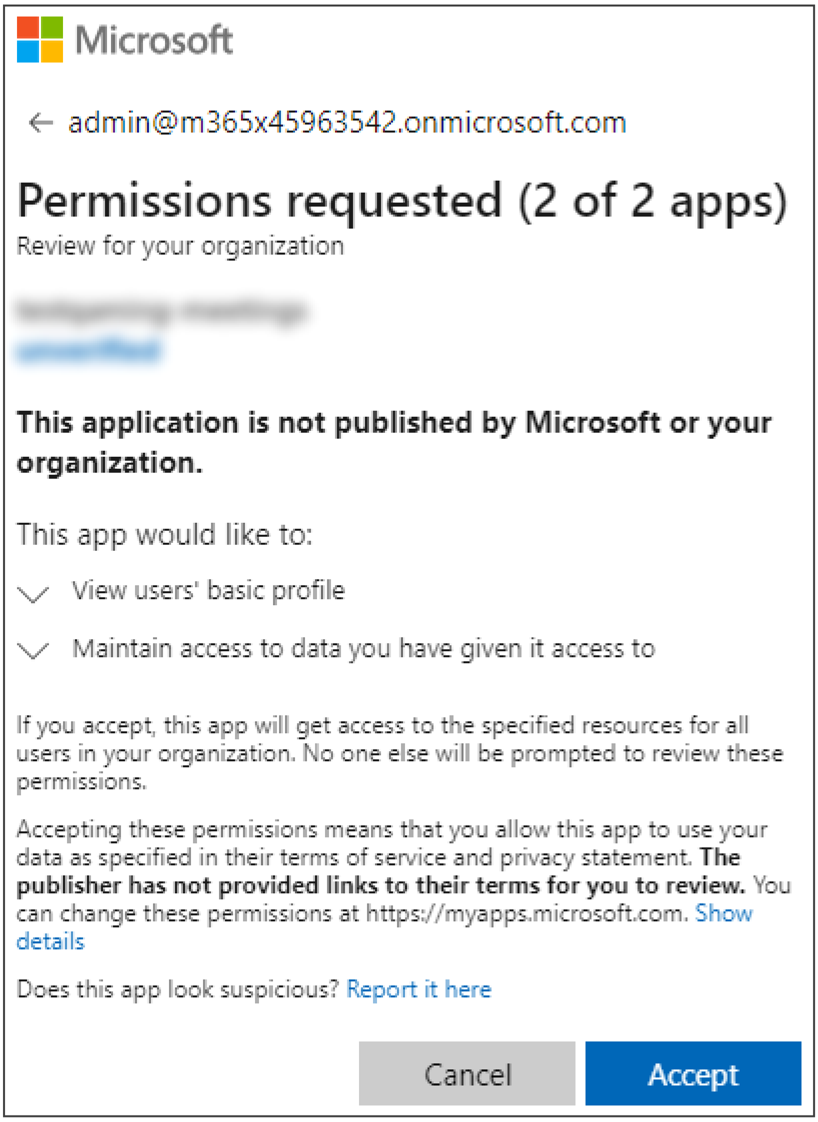
7. Click **Accept**.



8. Next to the consent ‘Allow Meeting Insights to Join Meetings’, click **Grant Admin Consent**, and then select the account.

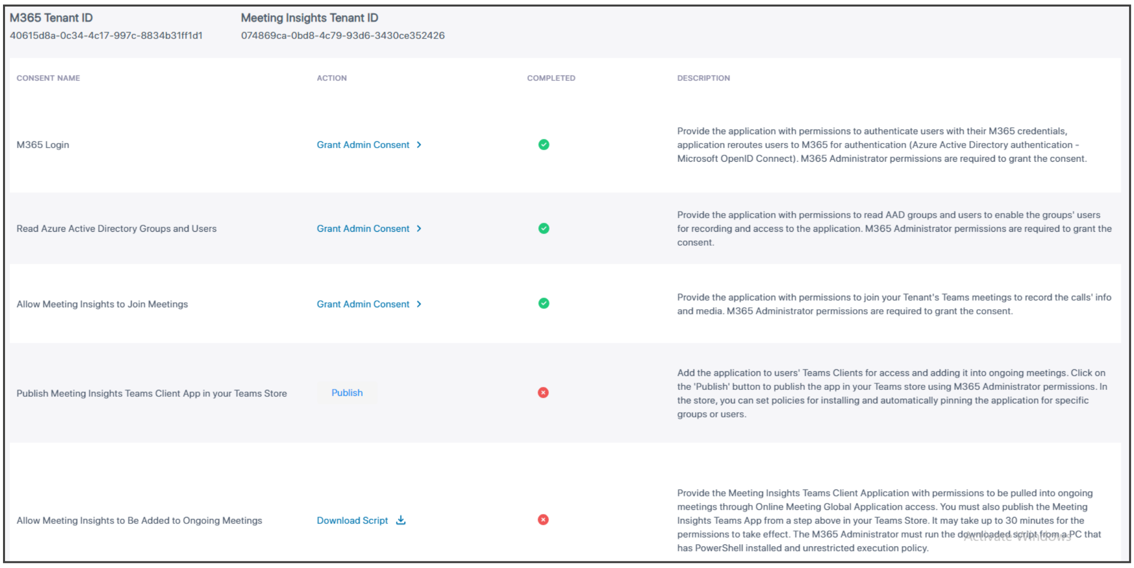

Microsoft
admin@m365x30069440.onmicrosoft.com
Permissions requested (1 of 2 apps)
Review for your organization
This application is not published by Microsoft or your organization.
This app would like to:
Daemon Role (sandbox3mi-meetings)
Bot Role (sandbox3mi-meetings)
Access media streams in a call as an app
Join group calls and meetings as an app
Read online meeting details
Read names and members of all chat threads
Sign in and read user profile
If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.
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
Cancel
Next

9. Click **Next**.



10. Click **Accept**.

> ⚠ The consent provides the app with permission to join your Tenant's Teams meetings to record calls' info and media.

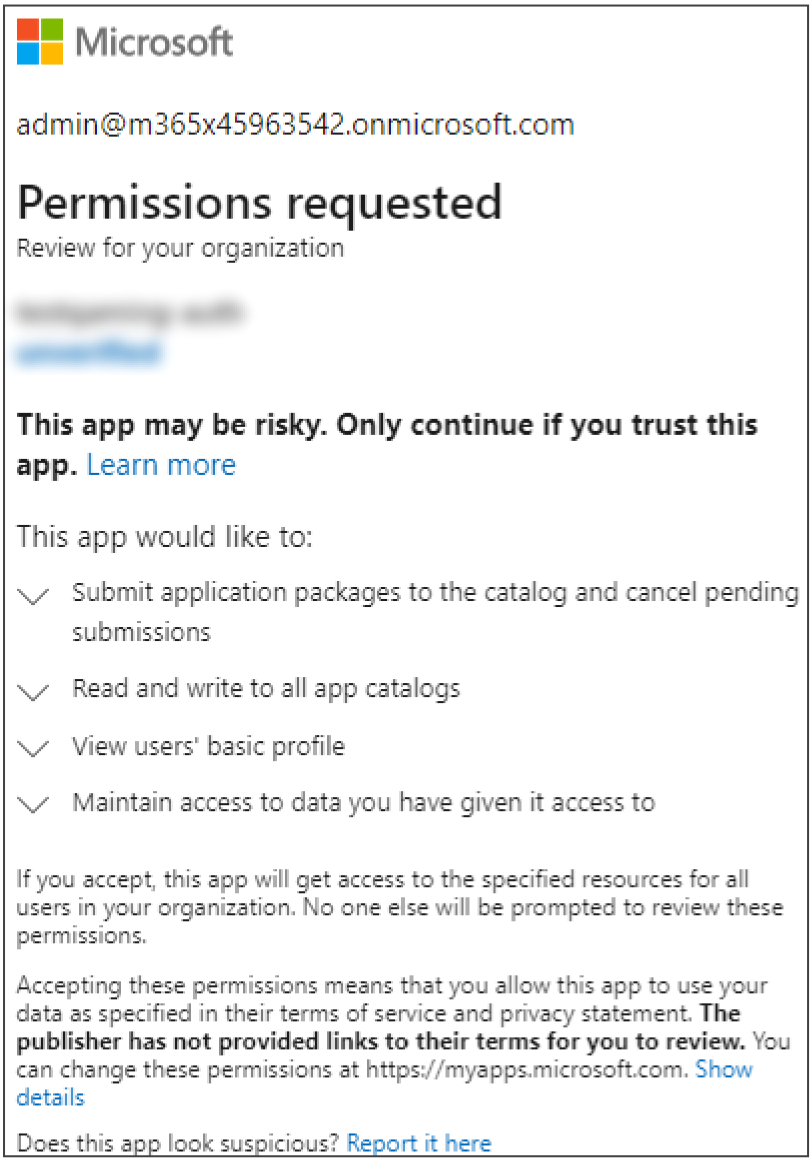


M365 Tenant ID 40615d8a-0c34-4c17-997c-8834b31f1d1

Meeting Insights Tenant ID 074869ca-0bd8-4c79-93d6-3430ce352426

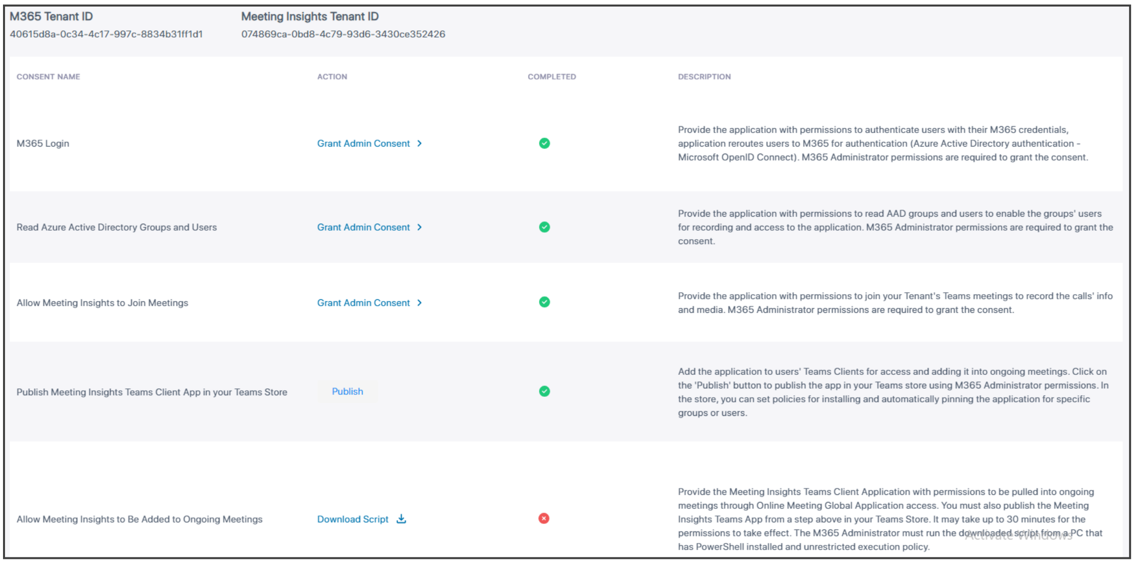
CONSENT NAME	ACTION	COMPLETED	DESCRIPTION
M365 Login	Grant Admin Consent ›	✔	Provide the application with permissions to authenticate users with their M365 credentials, application reroutes users to M365 for authentication (Azure Active Directory authentication - Microsoft OpenID Connect). M365 Administrator permissions are required to grant the consent.
Read Azure Active Directory Groups and Users	Grant Admin Consent ›	✔	Provide the application with permissions to read AAD groups and users to enable the groups' users for recording and access to the application. M365 Administrator permissions are required to grant the consent.
Allow Meeting Insights to Join Meetings	Grant Admin Consent ›	✔	Provide the application with permissions to join your Tenant's Teams meetings to record the calls' info and media. M365 Administrator permissions are required to grant the consent.
Publish Meeting Insights Teams Client App in your Teams Store	Publish	✖	Add the application to users' Teams Clients for access and adding it into ongoing meetings. Click on the 'Publish' button to publish the app in your Teams store using M365 Administrator permissions. In the store, you can set policies for installing and automatically pinning the application for specific groups or users.
Allow Meeting Insights to Be Added to Ongoing Meetings	Download Script	✖	Provide the Meeting Insights Teams Client Application with permissions to be pulled into ongoing meetings through Online Meeting Global Application access. You must also publish the Meeting Insights Teams App from a step above in your Teams Store. It may take up to 30 minutes for the permissions to take effect. The M365 Administrator must run the downloaded script from a PC that has PowerShell installed and unrestricted execution policy.

11. Click **Publish** next to 'Publish Meeting Insights Teams Client App in your Teams Store' to publish the app in your Teams store using M365 Administrator permissions, and then select the account.



12. Consent on behalf of your organization and click **Accept**.

- Alternatively, publish via the 'Tools' page as shown here.
- In the store, you can set policies for installing and automatically pinning the app for specific groups or users.
- The consent adds the app to users' Teams Clients for access and adding it into ongoing meetings.



M365 Tenant ID: 40615d8a-0c34-4c17-997c-8834b31ff1d1
Meeting Insights Tenant ID: 074869ca-0bd8-4c79-93d6-3430ce352426

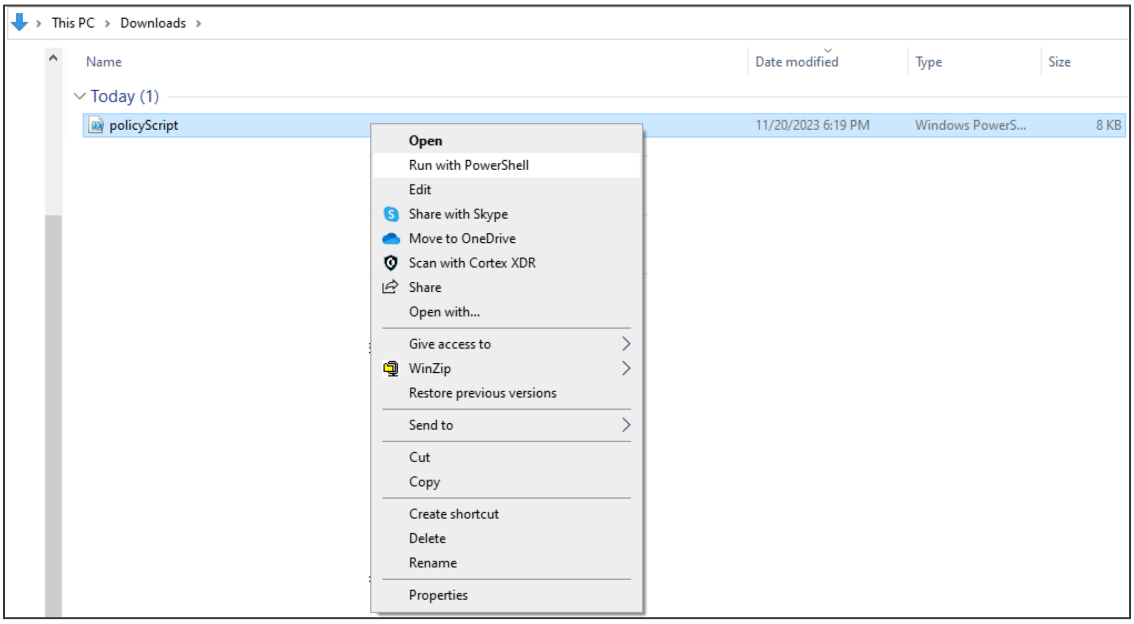
CONSENT NAME	ACTION	COMPLETED	DESCRIPTION
M365 Login	Grant Admin Consent ›		Provide the application with permissions to authenticate users with their M365 credentials, application reroutes users to M365 for authentication (Azure Active Directory authentication - Microsoft OpenID Connect). M365 Administrator permissions are required to grant the consent.
Read Azure Active Directory Groups and Users	Grant Admin Consent ›		Provide the application with permissions to read AAD groups and users to enable the groups' users for recording and access to the application. M365 Administrator permissions are required to grant the consent.
Allow Meeting Insights to Join Meetings	Grant Admin Consent ›		Provide the application with permissions to join your Tenant's Teams meetings to record the calls' info and media. M365 Administrator permissions are required to grant the consent.
Publish Meeting Insights Teams Client App in your Teams Store	Publish		Add the application to users' Teams Clients for access and adding it into ongoing meetings. Click on the 'Publish' button to publish the app in your Teams store using M365 Administrator permissions. In the store, you can set policies for installing and automatically pinning the application for specific groups or users.
Allow Meeting Insights to Be Added to Ongoing Meetings	Download Script		Provide the Meeting Insights Teams Client Application with permissions to be pulled into ongoing meetings through Online Meeting Global Application access. You must also publish the Meeting Insights Teams App from a step above in your Teams Store. It may take up to 30 minutes for the permissions to take effect. The M365 Administrator must run the downloaded script from a PC that has PowerShell installed and unrestricted execution policy.

In addition to the icon under the 'Completed' column indicating you successfully granted consent (consent was successfully completed from this page for 'Publishing Meeting Insights Teams Client App in your Teams Store'), the notification Application published in your Teams store successfully is displayed.

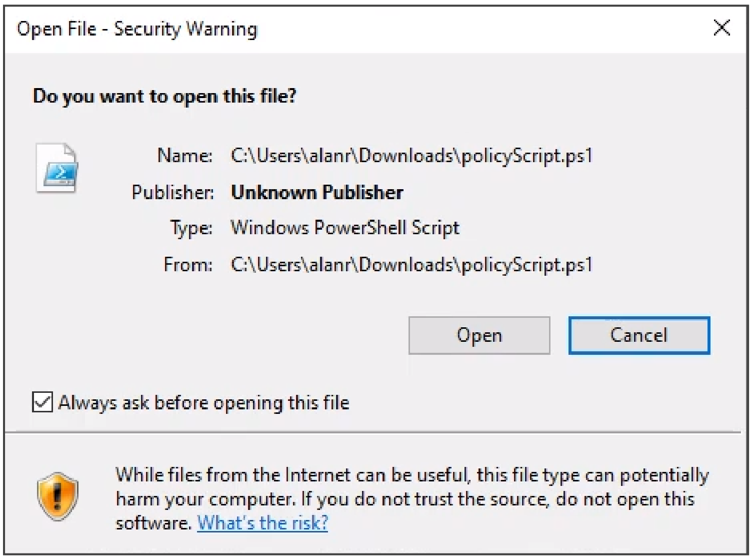
13. [Recommended] Install and pin the application for Meeting Insights users as shown here.

14. Next to the consent 'Allow Meeting Insights to be Added to Ongoing Meetings', click **Download Script**; the 'policyScript' file is downloaded to your PC.

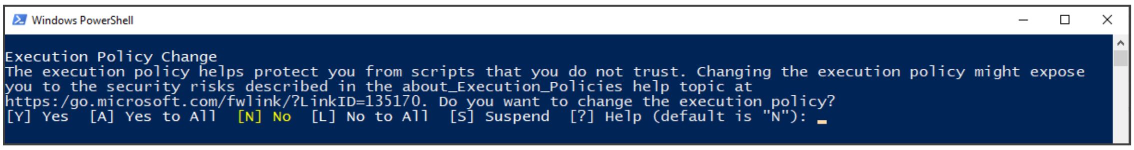
- **PowerShell must be installed on the PC and the PC must have an unrestricted execution policy for the Microsoft 365 admin to run the downloaded script.**
- Before running the downloaded script file, unblock it as the OS may block it. To unblock it, right-click the file and select **Properties**. If you're using Windows 11, first click **Show more options** to see the **Properties** option in the context menu. Select the **General** tab and check the **Unblock** option located lowermost under the 'Security' section.
- Run the script from the PC using PowerShell, with a 'Bypass' execution policy.
- The execution policy must be as follows:
  `Set-ExecutionPolicy -ExecutionPolicy Bypass -Scope LocalMachine`



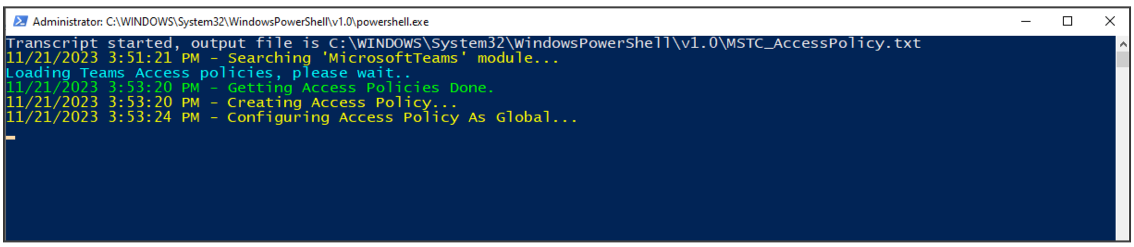
a. Right-click the file and select **Run with PowerShell**.



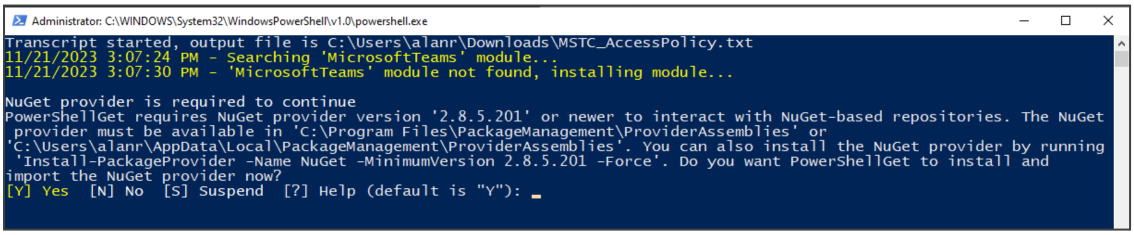
b. Click **Open**. PowerShell opens.



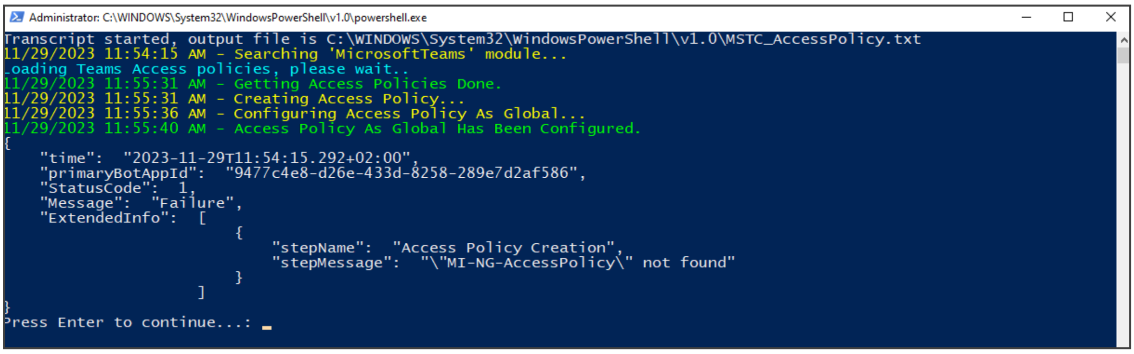
c. [Note that this screen is not always displayed after changing the execution policy the first time]. Type in **A** (Yes to All) and enter.



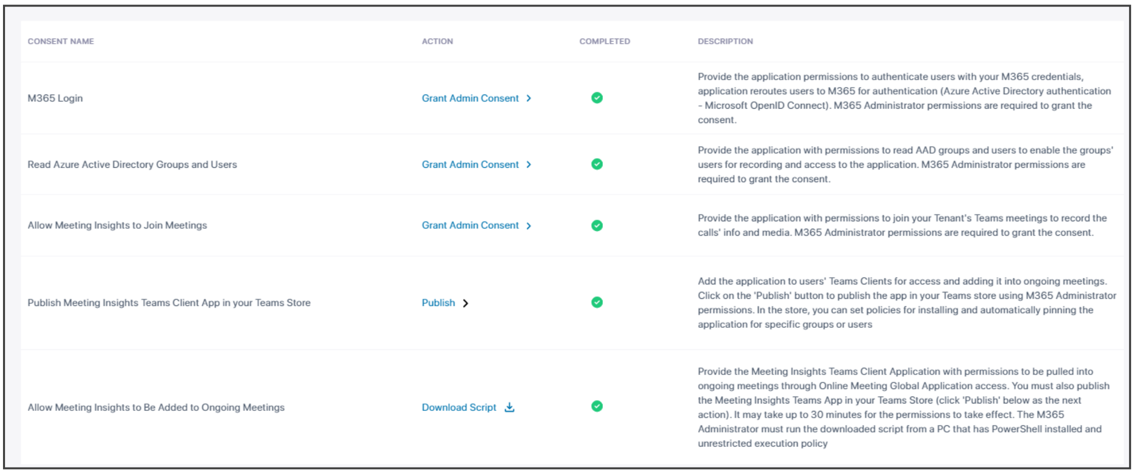
d. Type in **Y** (Yes) if the prompt below is displayed (it isn't always displayed), and enter.



e. Press Enter to continue...



You've successfully provided the Meeting Insights Teams client app with permissions to be pulled into ongoing meetings through Online Meeting Global Application access. It may take up to 30 minutes for the permissions to take effect. The M365 admin must run the downloaded script from a PC that has PowerShell installed and unrestricted execution policy.



CONSENT NAME	ACTION	COMPLETED	DESCRIPTION
M365 Login	Grant Admin Consent >	✔	Provide the application permissions to authenticate users with your M365 credentials, application reroutes users to M365 for authentication (Azure Active Directory authentication - Microsoft OpenID Connect). M365 Administrator permissions are required to grant the consent.
Read Azure Active Directory Groups and Users	Grant Admin Consent >	✔	Provide the application with permissions to read AAD groups and users to enable the groups' users for recording and access to the application. M365 Administrator permissions are required to grant the consent.
Allow Meeting Insights to Join Meetings	Grant Admin Consent >	✔	Provide the application with permissions to join your Tenant's Teams meetings to record the calls' info and media. M365 Administrator permissions are required to grant the consent.
Publish Meeting Insights Teams Client App in your Teams Store	Publish >	✔	Add the application to users' Teams Clients for access and adding it into ongoing meetings. Click on the 'Publish' button to publish the app in your Teams store using M365 Administrator permissions. In the store, you can set policies for installing and automatically pinning the application for specific groups or users
Allow Meeting Insights to Be Added to Ongoing Meetings	Download Script	✔	Provide the Meeting Insights Teams Client Application with permissions to be pulled into ongoing meetings through Online Meeting Global Application access. You must also publish the Meeting Insights Teams App in your Teams Store (click 'Publish' below as the next action). It may take up to 30 minutes for the permissions to take effect. The M365 Administrator must run the downloaded script from a PC that has PowerShell installed and unrestricted execution policy

You've successfully connected to Microsoft 365. **Next**: Assign licenses to Meeting Insights users as shown here.

The 'Auto can edit' feature takes effect on a meeting only if the user with this permission has joined the meeting. If the user hasn't joined, they will not be able to edit it automatically.

Permissions in Customers' Azure Enterprise Applications

Some customers must have Meeting Insights application permissions in flat form to run it through internal IT / Security approvals before onboarding. The following sections list the permissions that must be provided for customers' Azure enterprise applications. Provide permissions for the following customer Azure enterprise applications:

Azure AD Meeting Insights Web Application below

Azure AD Meeting Insights Application below

Azure AD Meeting Insights Bot Application on the next page

Azure AD Meeting Insights Teams Application on the next page

Azure AD Notifications Bot Application (Optional) on the next page

Allow Meeting Insights to Be Added to Ongoing Meetings – script needs to be executed (optional) on page 20

Azure AD Meeting Insights Web Application

Provide the application with permissions to authenticate users with their Microsoft 365 credentials, application reroutes users to Microsoft 365 for authentication (Azure Active Directory authentication - Microsoft OpenID Connect).

Microsoft 365 Administrator permissions are required to grant the consent.

Permissions description:

1. Microsoft Graph email - View users' email address (Delegated)
2. Microsoft Graph offline_access - Maintain access to data you have given it access to (Delegated)
3. Microsoft Graph openid - Sign users in (Delegated)
4. Microsoft Graph profile - View users' basic profile (Delegated)
5. Microsoft Graph User.Read - Sign in and read user profile (Delegated)

   For integration with MSFT Planner, when it is enabled by admin (optional):

6. Microsoft Graph Tasks.ReadWrite - Create, read, update, and delete user’s tasks and task lists (Delegated)

Azure AD Meeting Insights Application

Provide the application with permissions to read AAD groups and users to enable the groups' users for access to the application. Enable the application to add Meeting Insights Teams App to meetings.

Microsoft 365 Administrator permissions are required to grant the consent.

1. Microsoft Graph User.Read.All - Read all users' full profiles (Application)

2. Microsoft Graph TeamsTab.ReadWriteForChat.All - Allow the Teams app to manage all tabs for all chats (Application)
3. Microsoft Graph TeamsTab.Create - Create tabs in Microsoft Teams (Application)
4. Microsoft Graph TeamsAppInstallation.ReadWriteForChat.All - Manage Teams apps for all chats (Application)
5. Microsoft Graph GroupMember.Read.All - Read all group memberships (Application)

Azure AD Meeting Insights Bot Application

Provide the application with permissions to join your Tenant's Teams meetings to record the calls' info and media and read the participants of the meetings (chat permission).

Microsoft 365 Administrator permissions are required to grant the consent.

1. **Microsoft Graph Calls.JoinGroupCall.All:** Join group calls and meetings as an app (Application)
2. **Microsoft Graph OnlineMeetings.Read.All:** Read online meeting details (Application)
3. **Microsoft Graph Chat.ReadBasic.All:** Read names and members of all chat threads (Application)
4. **Microsoft Graph Calls.AccessMedia.All:** Access media streams in a call as an app (Application)

   Internal communication application roles permissions:

5. **BotRole:** Bot Role (Application)
6. **DaemonRole:** Daemon Role (Application)

Azure AD Meeting Insights Teams Application

Provide the application with permission to add and update Meeting Insights Teams app in Organizational Teams Store.

1. Microsoft Graph AppCatalog.Submit - Submit application packages to the catalog and cancel pending submissions (Delegated)
2. Microsoft Graph AppCatalog.ReadWrite.All - Read and write to all app catalogs (Delegated)
3. Microsoft Graph openid - Sign users in (Delegated)
4. Microsoft Graph email - View users' email address (Delegated)
5. Microsoft Graph profile - View users' basic profile (Delegated)

Azure AD Notifications Bot Application (Optional)

Provide the application with permissions to trigger Microsoft Teams recording notifications in your Tenant's Teams meetings when recorded by Meeting Insights.

Microsoft 365 Administrator permissions are required to grant the consent.

1. **Microsoft Graph Calls.JoinGroupCall.All:** Join group calls and meetings as an app (Application)
2. **Microsoft Graph OnlineMeetings.Read.All:** Read online meeting details (Application)
3. **Microsoft Graph Calls.AccessMedia.All:** Access media streams in a call as an app (Application)

   Internal communication application roles permissions.
4. **BotRole:** Bot Role (Application)
5. **DaemonRole:** Daemon Role (Application)

Allow Meeting Insights to Be Added to Ongoing Meetings – script needs to be executed (optional)

Provide the Meeting Insights Teams Client Application with permissions to be pulled into ongoing meetings through Online Meeting Global Application access.

The Microsoft 365 Administrator must run the downloaded script from a PC that has PowerShell installed and an unrestricted execution policy.

- Online Meeting Global Application access

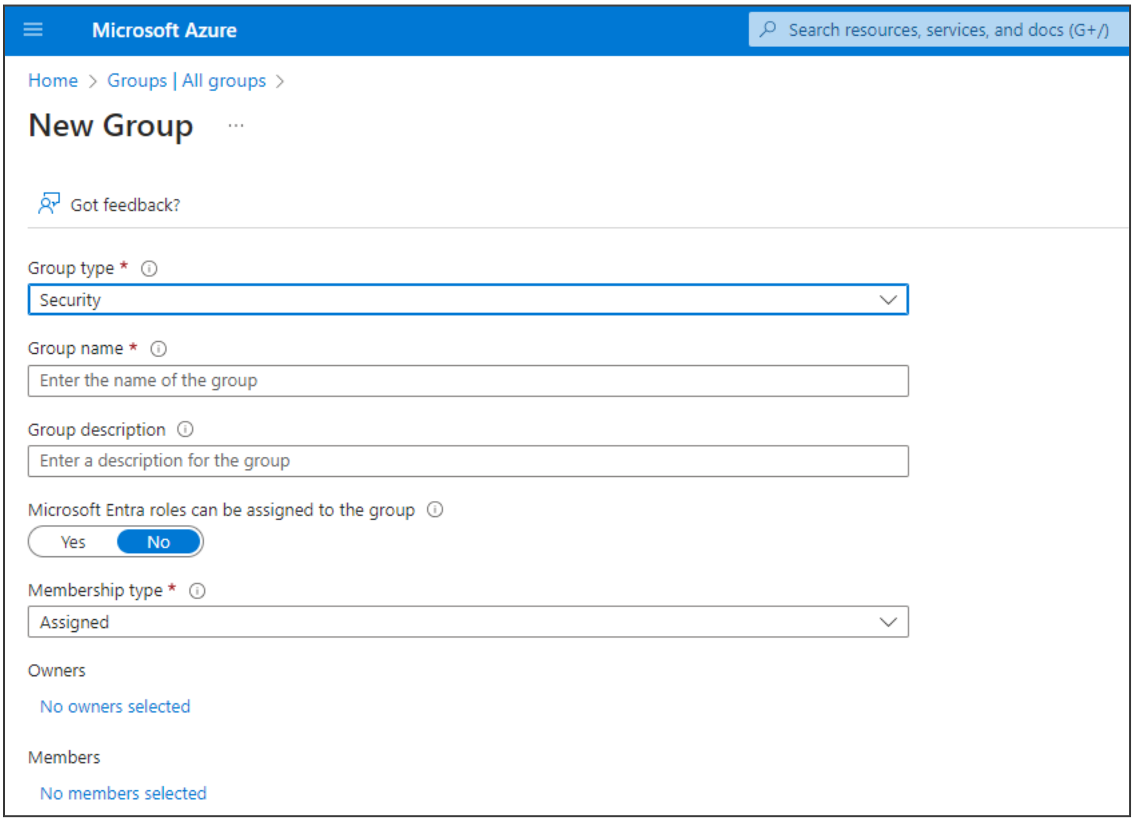
Defining a Group of Users in AAD

Before assigning a license, the enterprise admin must define a group of users in Azure Active Directory (AAD) for those users who'll be using Meeting Insights.

> If you later modify an AAD group, access the License Management page (see Assigning a Meeting Insights License to Users on page 22), and then click **Sync and Apply** for your changes to be reflected in Meeting Insights. For more information on the

➢ **To define a group of users in AAD:**

1. Sign in from here to Microsoft Azure portal with your admin credentials.
2. Locate the Groups | All Groups page and click **New group**.

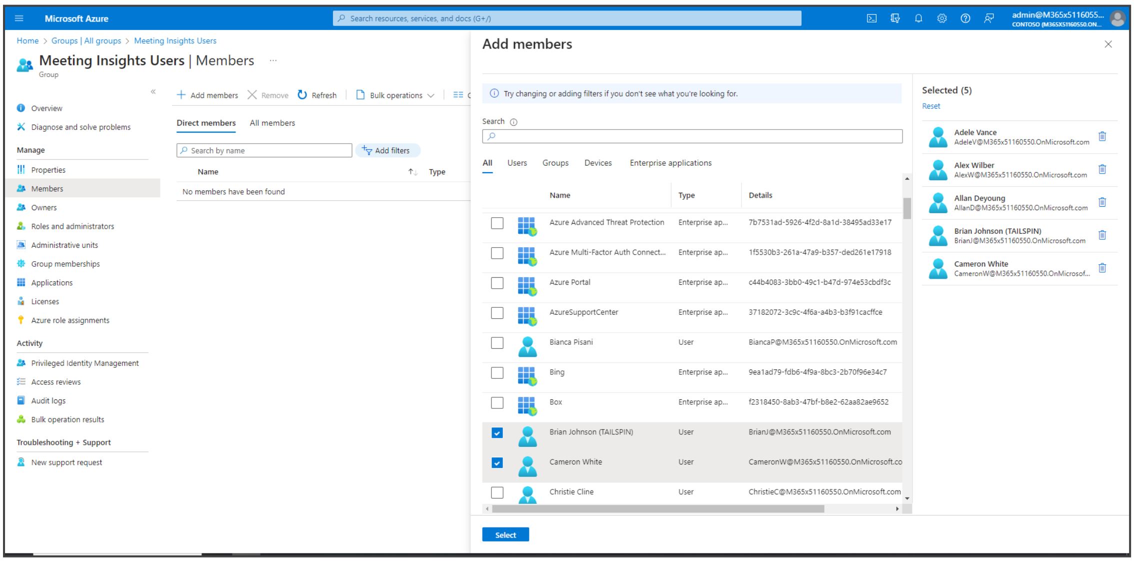


3. [Mandatory] From the 'Group type' drop-down, select **Security**.

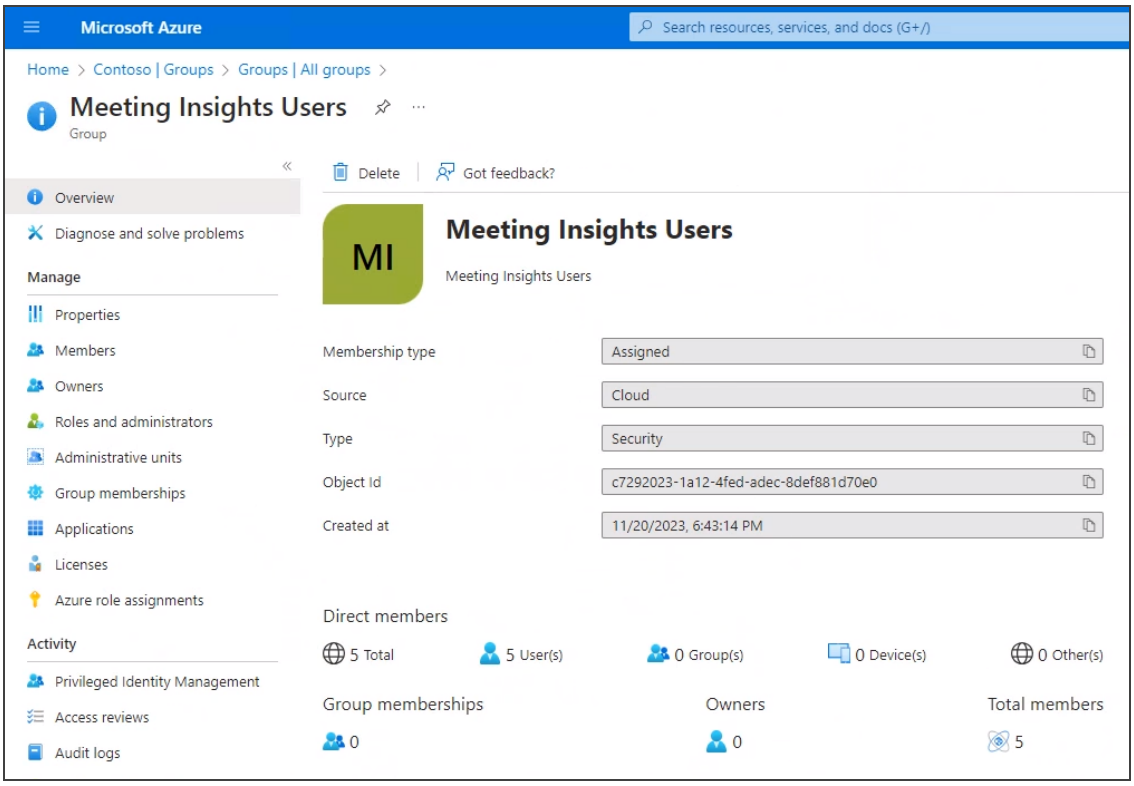
4. [Strongly recommended] Define the group name as **Meeting Insights Users**.

5. Assign owners to the group. Note that group owners have unique permissions to manage the group. They can add and remove members, change group settings, rename the group, update its description, and more.

6. Assign members (i.e., users or groups) to the group.



7. View the group details in Microsoft Azure portal.

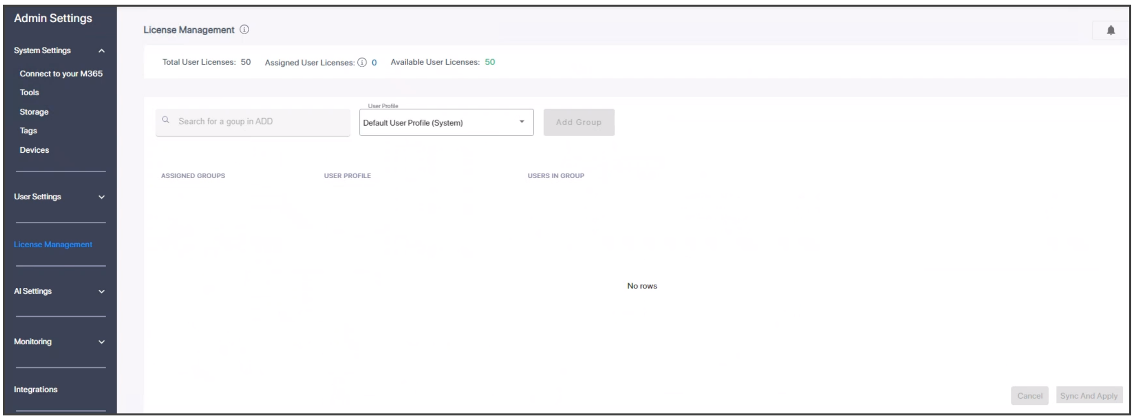


Assigning a Meeting Insights License to Users

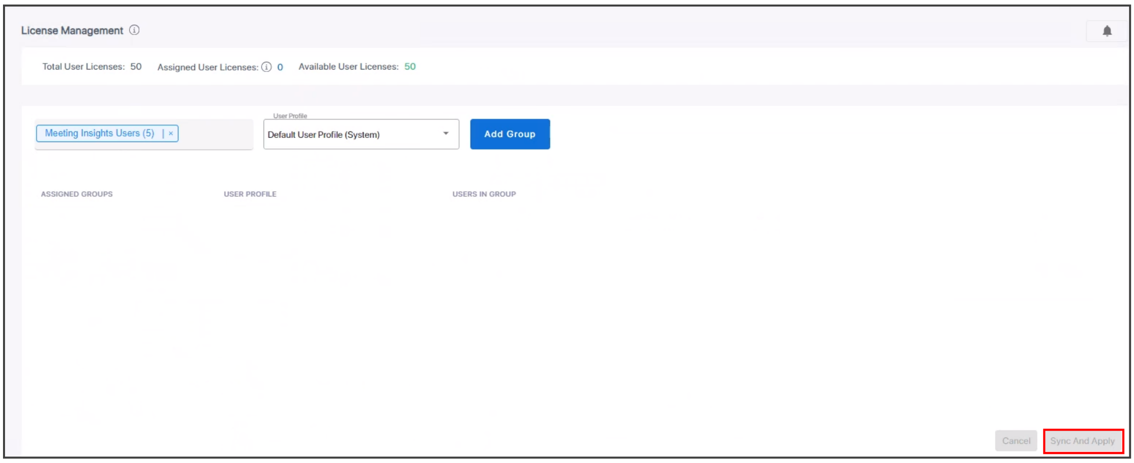
The License Management page in Meeting Insights enables the enterprise admin to assign a Meeting Insights license to a group of users.

➢ To assign a license to the group:

1. In Meeting Insights, click the **License Management** menu.

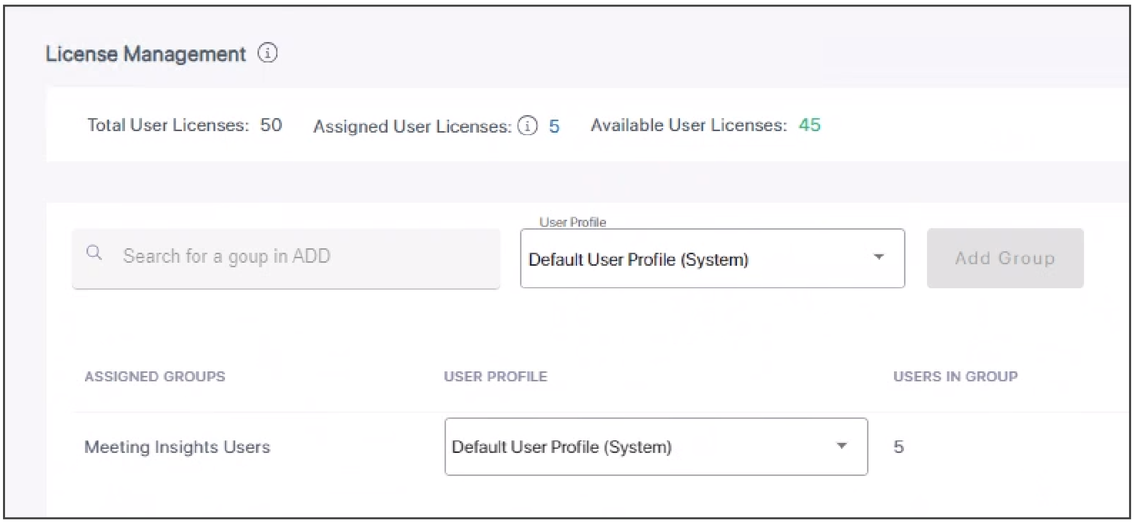


2. In the 'Search for a group in AAD' field, enter the first letters of the name of the group you defined in the previous procedure; the field is auto-populated, i.e., **Meeting Insights Users (5)**. Wait a few seconds for AAD to populate the field.



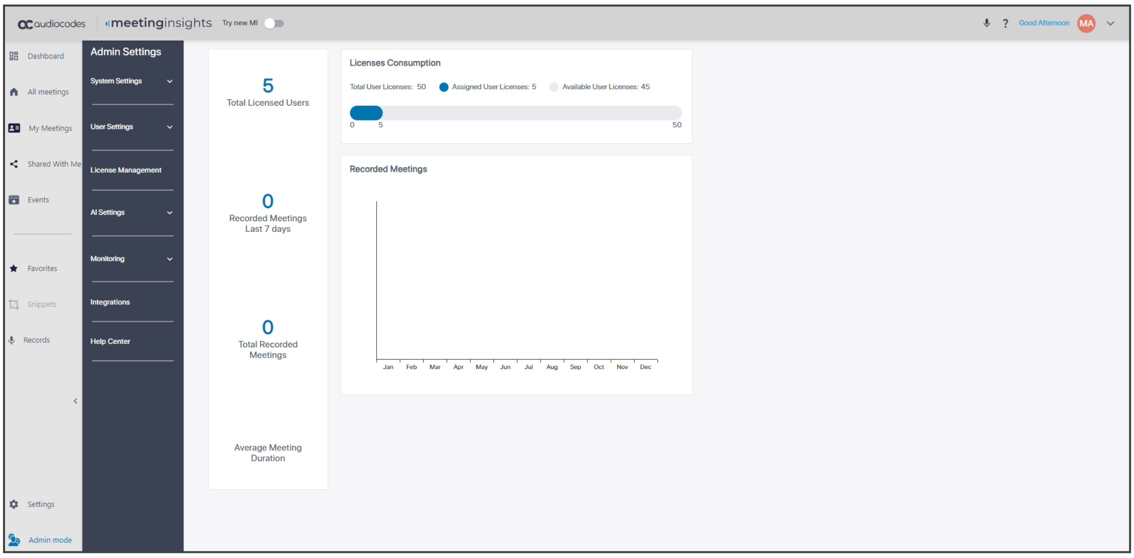
3. Leave the 'User Profile' field at its default, i.e., **Default User Profile (System)**, permitting users to access Meeting Insights and to record meetings. [See more information about User Profiles here].

4. Click **Add Group** and then **Sync and Apply**; a Meeting Insights license is assigned to the group; the users in the group can go ahead and use the app.



5. View the license assignment displayed uppermost in the License Management page. In the example shown in the preceding figure:
   - Total User Licenses: 50
   - Assigned User Licenses: 5
   - Available User Licenses: 45

6. [Optionally] View this information as well as usage on the Dashboard (Licenses Consumption) page.



In the example shown in the preceding figure, a license to a group of five Meeting Insights users was assigned, 0 meetings were recorded in the last 7 days and 0 meetings were held in total.

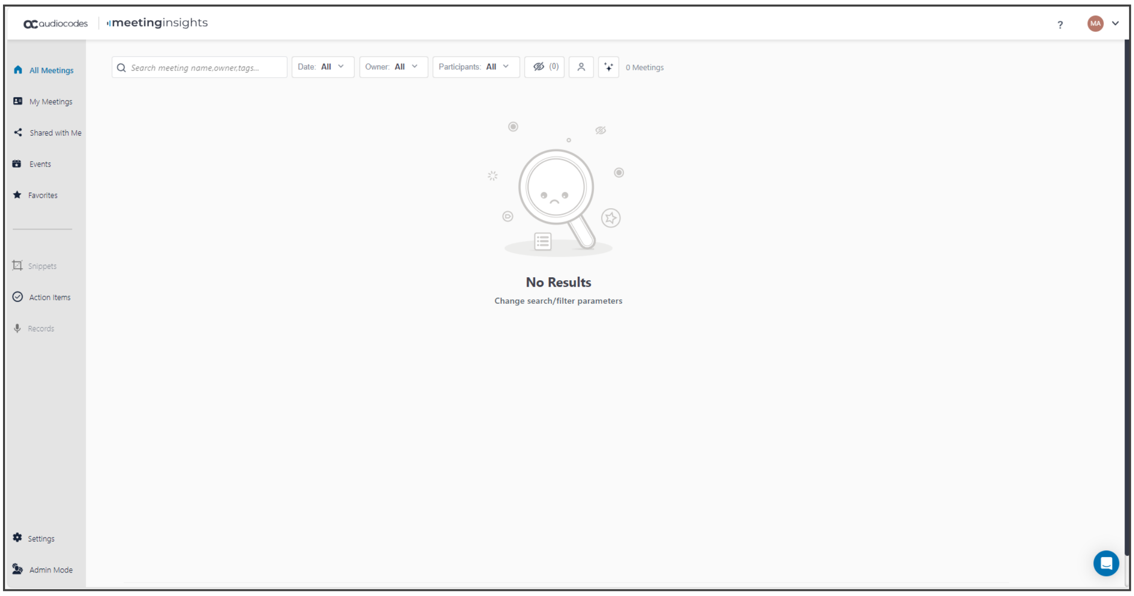
Switching from Admin to User Mode, and Back

Admin can optionally switch from Admin Mode to User Mode, and then back to Admin Mode.

- Admin mode located in the lowermost left corner of the page indicates you signed in as admin.
- The 'Admin Settings' menu bar also indicates you signed in as admin.
- Default admin must be a user who is logged in to the system (see here for related information).

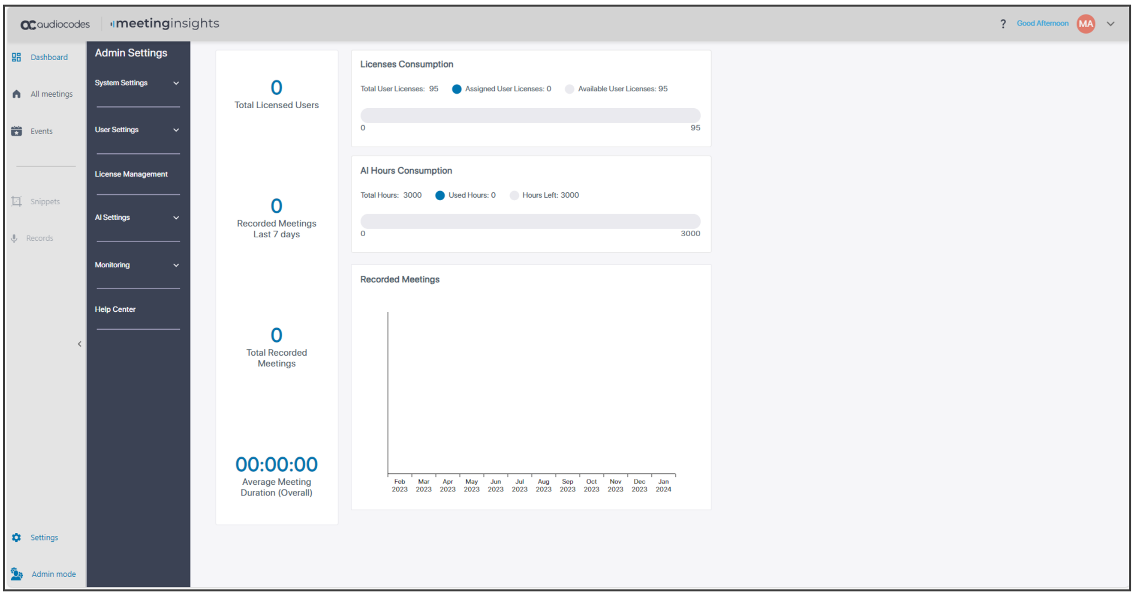
➢ To switch to user view:

- Click Admin mode; the link is deactivated and the user view is displayed. The figure below shows no meetings displayed following deployment.



➢ **To switch back to admin mode:**

■ Click Admin Mode; admin view is displayed and the link is reactivated.

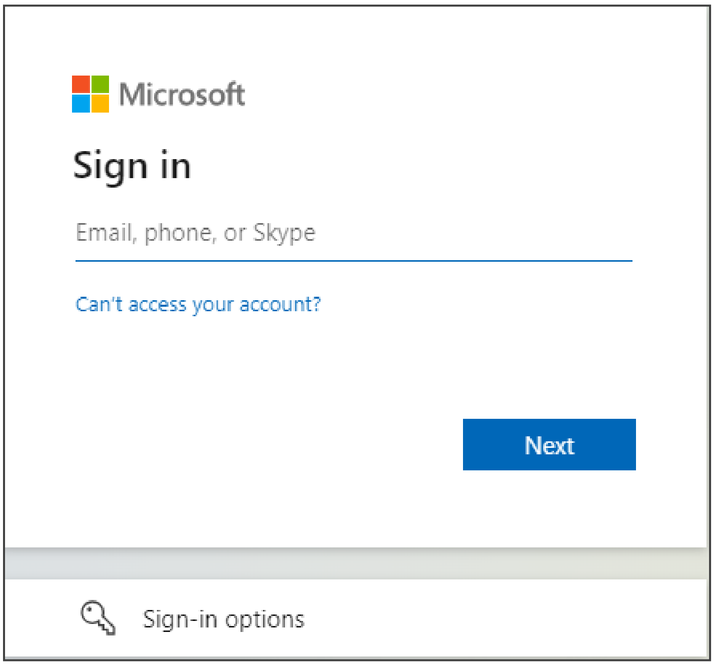


5 Testing your Meeting Insights App

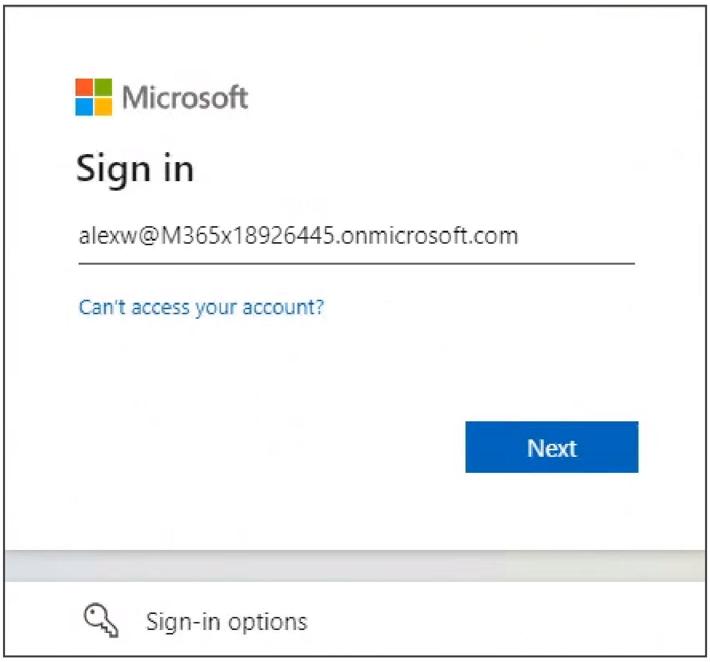
After setting up Meeting Insights, best practice is to test the app with one of the users that is in the Meeting Insights group.

➢ To test the app:

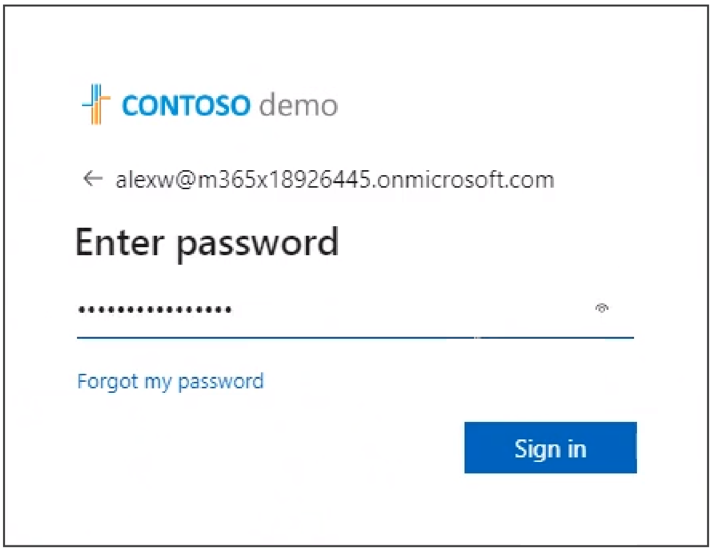
1. Click the Teams web app link.



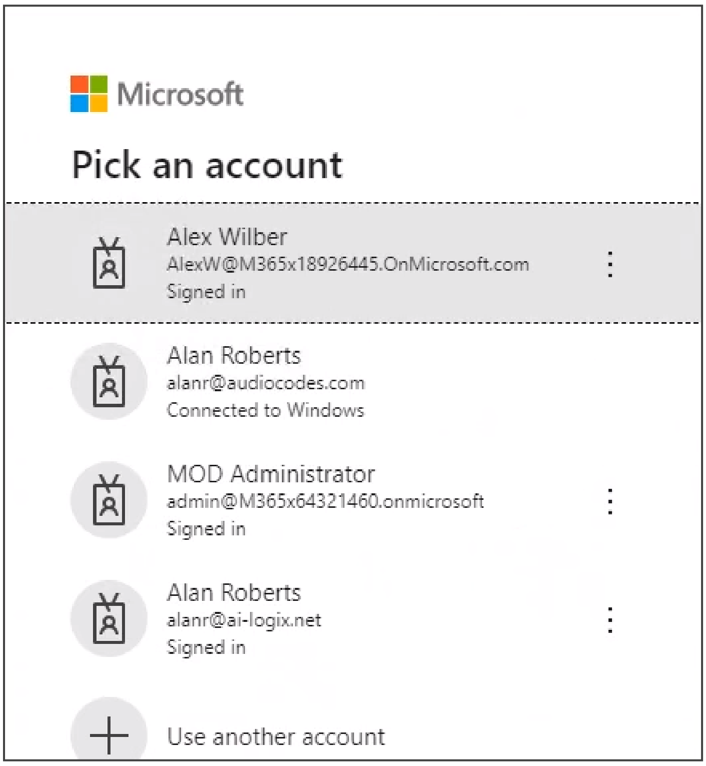
2. Enter the user's Teams client username.



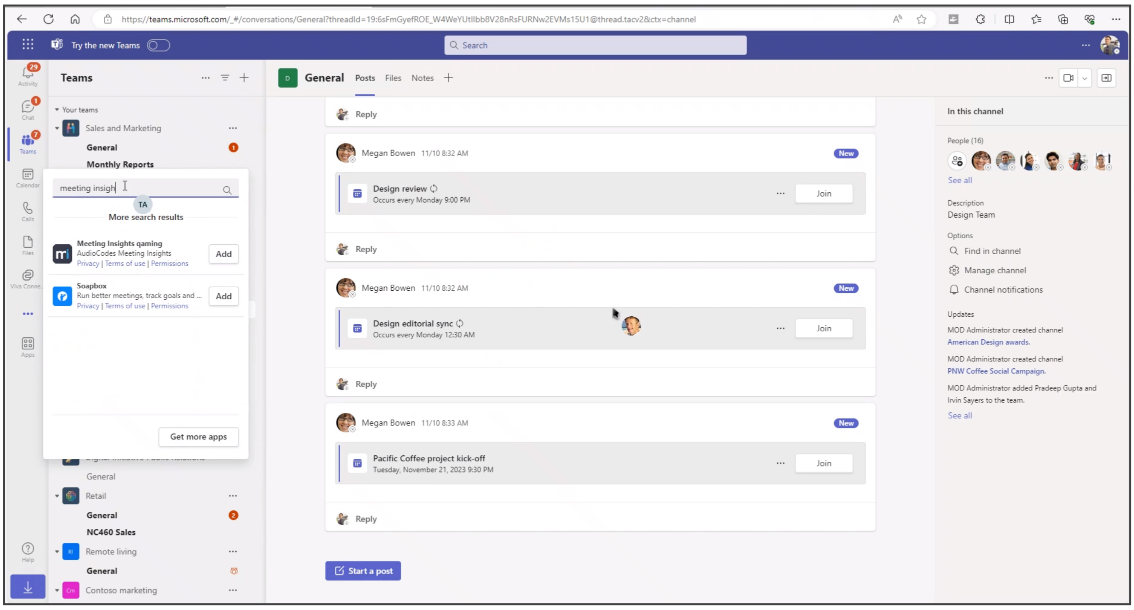
3. Click **Next**.



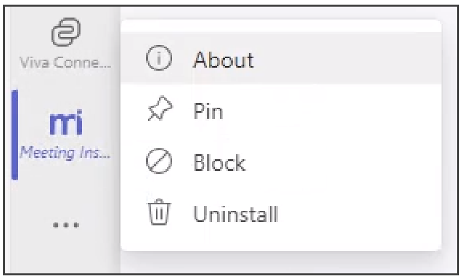
4. Enter the user's Teams client password and click **Sign in**.



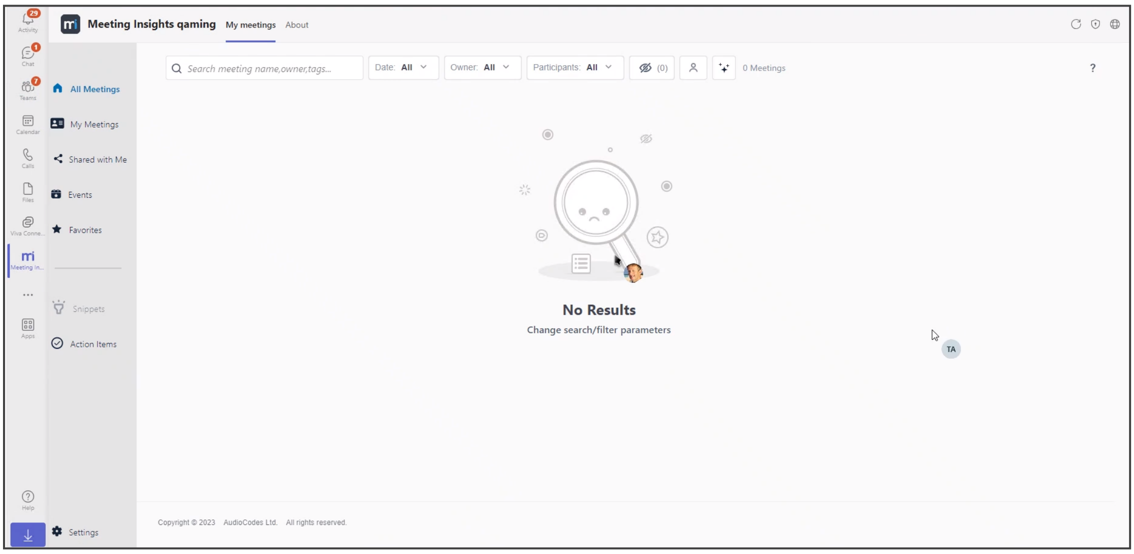
5. Click the account of the user.



6. In the Teams web app, click the **...** option in the left menu bar. In the 'Search for apps' field, enter Meeting Insights.
7. Select the **Meeting Insights** app and click the **Add** button next to it; Meeting Insights is added to the Teams client.
8. Right-click the newly added Meeting Insights icon in the left menu bar.

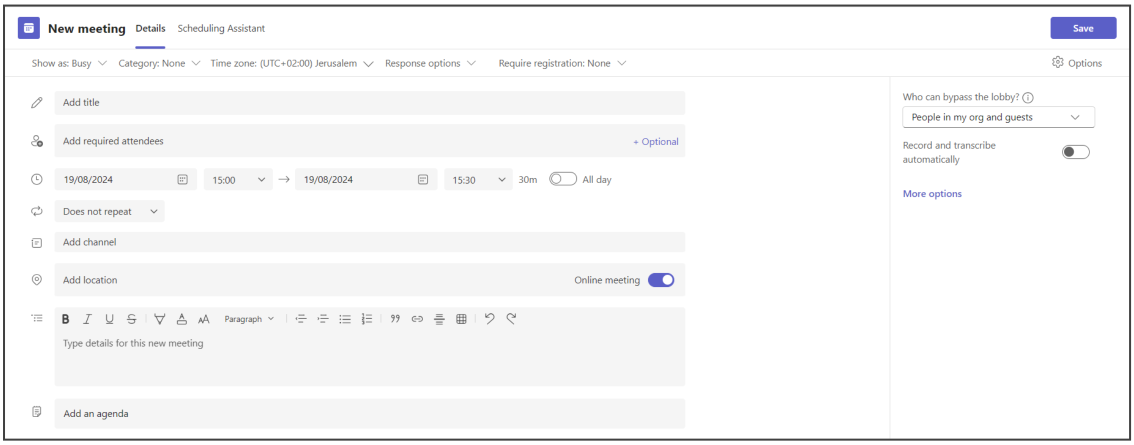


9. From the popup, select **Pin**.



The user has not used Meeting Insights before so no meeting recordings are displayed.

10. Click the **Calendar** icon in Teams and in the Calendar, click **New meeting**.



11. Schedule a meeting for at least five minutes before a start time to allow MIA (Meeting Insights Assistant) to join. Add MIA to the invitees' list using its email address (xx.mia@meetinginsights.com). Meeting Insights will join two minutes before the meeting.

12. Click **Start Meeting**. You've successfully tested the new user's ability to start a meeting and record it. Make sure the Meeting Insights app icon is displayed at the top of the meeting window and that MIA is one of the participants.

- The instructions above describe testing a *scheduled meeting*, with MIA *joining in*.
- If the meeting was *unscheduled*, go to **+ Apps** and select **Meeting Insights**; make sure MIA joins and that there's a **Meeting Insights** tab at the top of the screen.
- At the end of the meeting, go to 'List View' to play the recording. Note that it takes time for Meeting Insights to process a meeting but the video recording can be viewed and the audio can be played almost immediately.

6 Determining Who has Permission to Perform What Action

The table below shows who has permission to perform what actions for highlights, bookmarks, snippets, etc., with Meeting Insights.

	Actions	Admin	Owner	Delegate	Auto Can Edit	Participant
Highlight	Add	X	√	√	√	√
	Edit	X	OWN	OWN	OWN	OWN
	Delete	X	OWN	OWN	OWN	OWN
	View	√	OWN	OWN	OWN	OWN
Bookmark	Add	X	√	√	√	√
	Edit	X	OWN	OWN	OWN	OWN
	Delete	X	OWN	OWN	OWN	OWN
	View	√	OWN	OWN	OWN	OWN
Snippet	Add	X	√	√	√	√
	Edit	X	OWN	OWN	OWN	OWN
	Delete	X	OWN	OWN	OWN	OWN
	View	√	OWN	OWN	OWN	OWN
Snippet Sharing	Restricted	X	√	√	√	√
	Shareable	X	√	√	√	X
	Organization	X	√	√	√	X
Notes Private	Add	X	√	√	√	√
	Edit	X	OWN	OWN	OWN	OWN
	Delete	X	OWN	OWN	OWN	OWN
	View	X	OWN	OWN	OWN	OWN

	Actions	Admin	Owner	Delegate	Auto Can Edit	Participant
Notes Public	Add	X	√	√	√	√
	Edit	X	√	√	√	OWN
	Delete	√	√	√	√	OWN
	View	√	√	√	√	√
Recap	Add	√	√	√	√	X
	Edit	√	√	√	√	X
	Delete	√	√	√	√	X
	View	√	√	√	√	√
	AI trigger	√	√	√	√	If everyone can trigger, enabled by admin
Transcription	Edit	√	√	√	√	X
	Delete	√	√	√	√	X
	View	√	√	√	√	√
	Trigger	√	√	√	√	If everyone can trigger, enabled by admin
Delete		√	√	√	√	X
Download		√	√	√	√	X
Meeting info	Edit	√	√	√	√	X
	View	√	√	√	√	√
External Share	Only when both the owner and the other	√	√	√	√	X

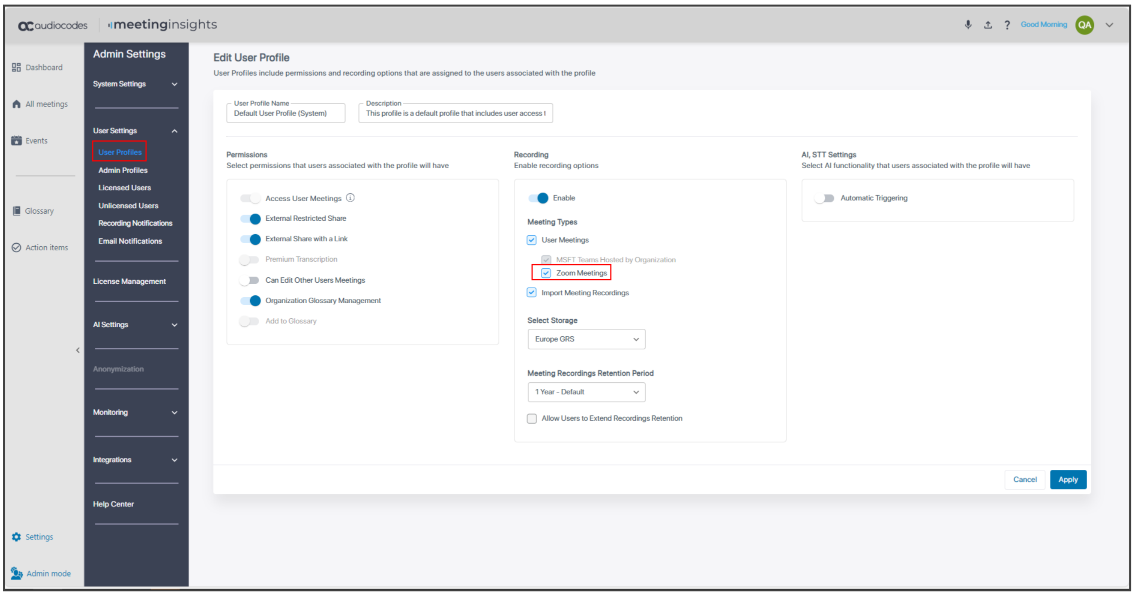
	Actions	Admin	Owner	Delegate	Auto Can Edit	Participant
	party have permission to share (this is due to the sensitivity of the external share).					
Internal Share		√	√	√	√	X

7 Enabling Users to Record Zoom Meetings

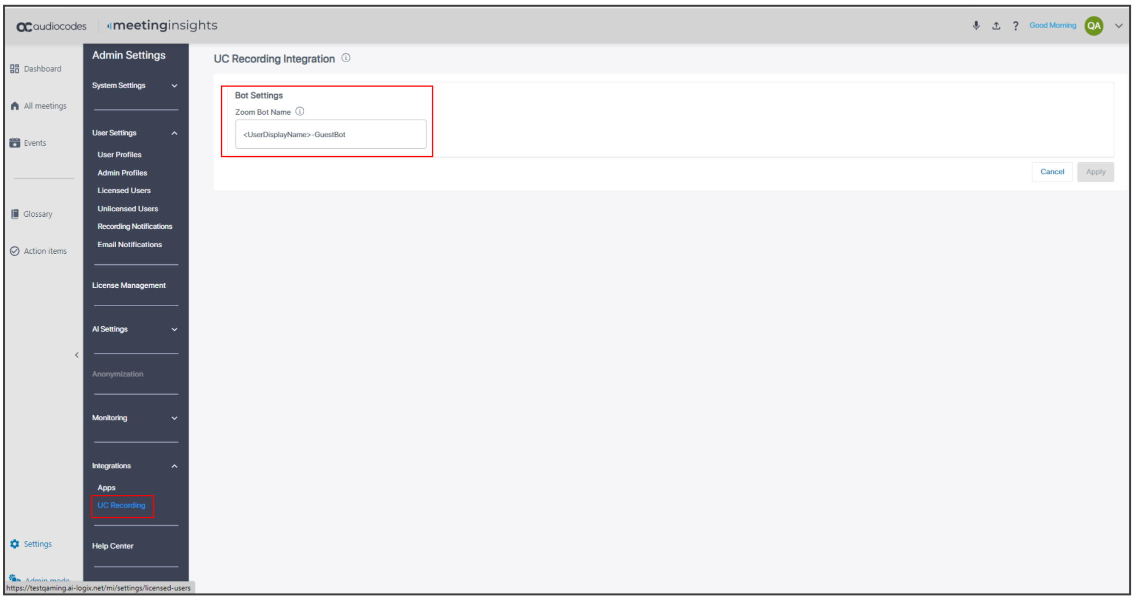
The instructions below show how to enable users (associated with a specific User Profile) to record their Zoom meetings.

➢ To enable users to record Zoom meetings:

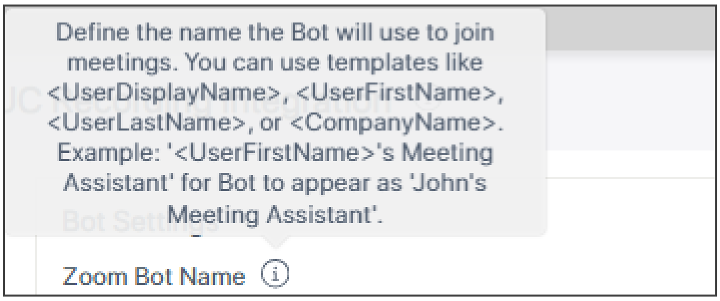
1. Select a User Profile with which the users for whom you want to enable Zoom are associated.



2. [Optional] In the UC Recording Integration page (**Admin Settings** > **Integrations** > **UC Recording**) in the 'Zoom Bot Name' field under 'Bot Settings', configure a Zoom Bot name.



3. Click the **i** icon adjacent to 'Zoom Bot Name' and use the tooltip as reference:



- The 'Zoom Bot Name' field includes <UserDisplayName> in brackets.
- This is the name the Zoom Bot will use to join meetings.

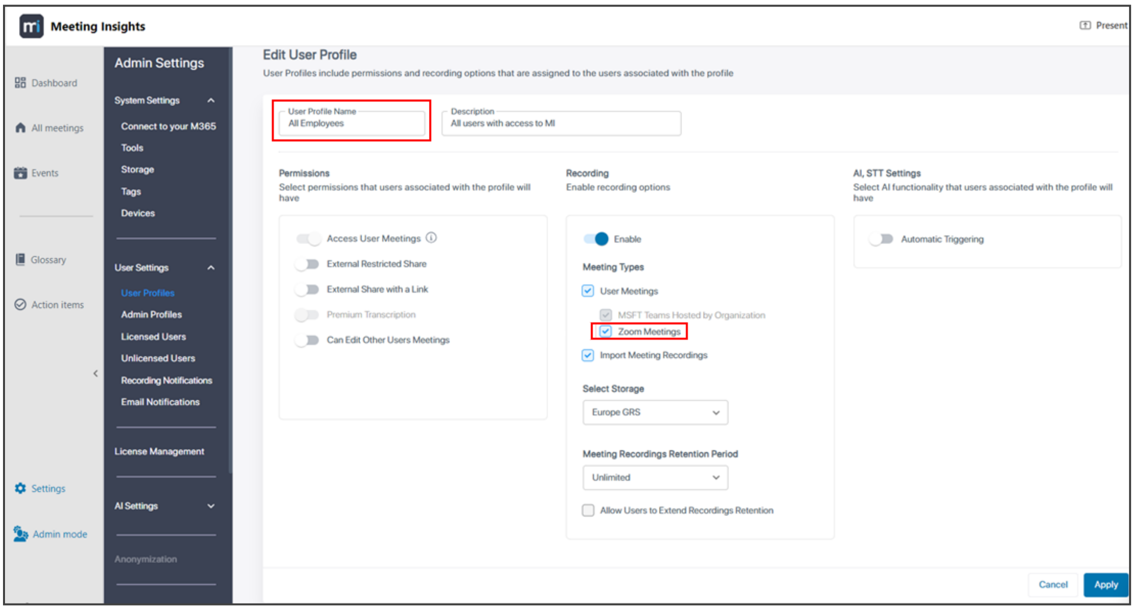
4. Click **Apply**.

Enabling Zoom for All Employees

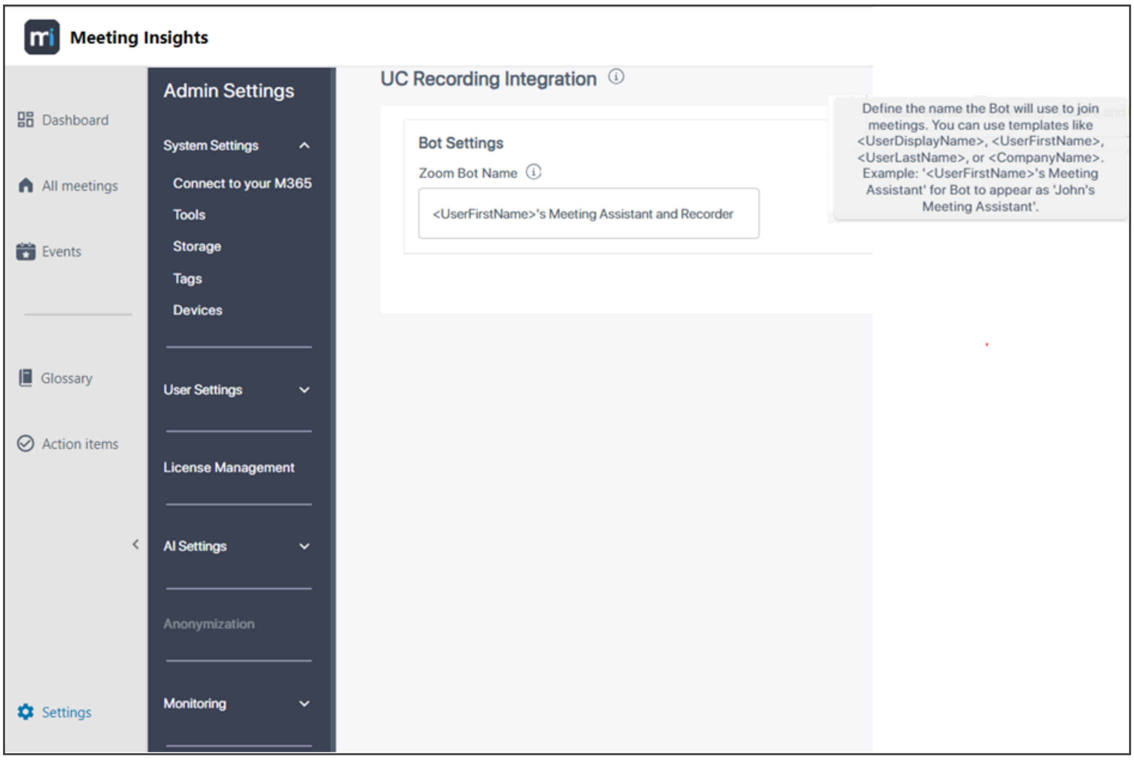
This section shows how to enable Zoom for all employees in the enterprise with access to Meeting Insights. Admin can configure enabling Zoom for all users in the enterprise, or for a group of users, in the User Profiles page. Additionally, admin can customize the Zoom Bot name.

➢ To enable Zoom for all enterprise employees with access to Meeting Insights:

1. Select the User Profile with which all users in the enterprise, for whom you want to enable Zoom, are associated. In the figure below, the User Profile Name is 'All Employees'.



2. [Optionally] In the UC Recording Integration page (**Admin Settings** > **Integrations** > **UC Recording**) in the 'Zoom Bot Name' field under 'Bot Settings', configure a Zoom Bot name.


Meeting Insights
Dashboard
All meetings
Events
Glossary
Action items
Settings
Admin Settings
System Settings
Connect to your M365
Tools
Storage
Tags
Devices
User Settings
License Management
AI Settings
Anonymization
Monitoring
UC Recording Integration
Bot Settings
Zoom Bot Name
<UserFirstName>'s Meeting Assistant and Recorder
Define the name the Bot will use to join meetings. You can use templates like <UserDisplayName>, <UserFirstName>, <UserLastName>, or <CompanyName>. Example: '<UserFirstName>'s Meeting Assistant' for Bot to appear as 'John's Meeting Assistant'.

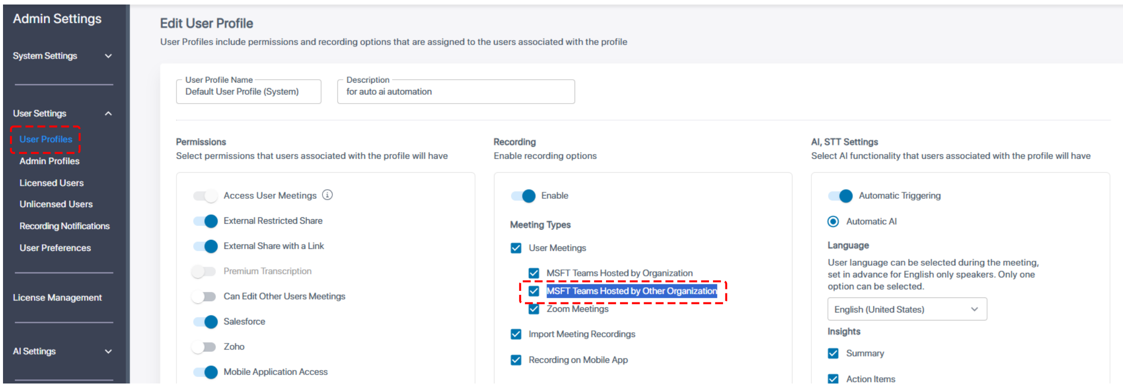
8 Enabling Users to Record External Teams Meetings

You can enable users (associated with a specific User Profile) to record Microsoft Teams meetings that are hosted by other organizations (external Teams meetings).

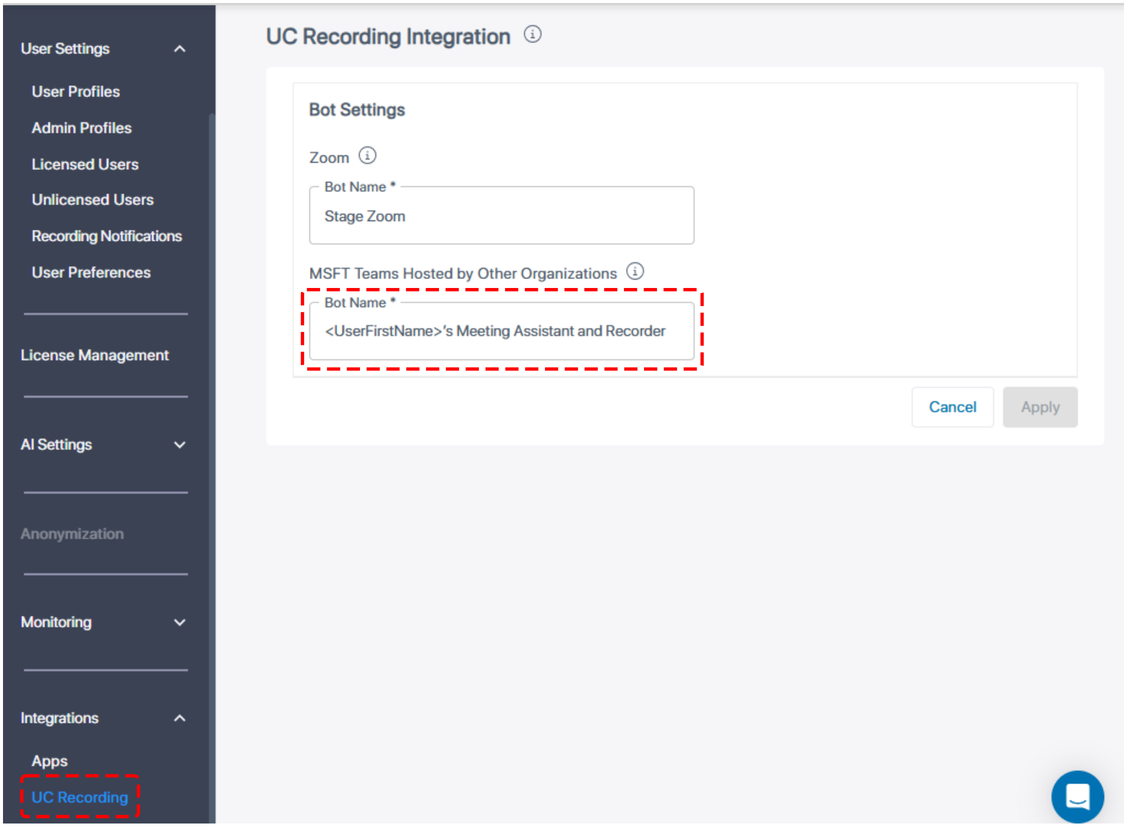
You can also customize the name of the Meeting Insights bot that joins external Teams meetings to record them.

➢ To enable users to record external Teams meetings:

1. In the Admin Settings navigation pane, expand **User Settings** and then click **User Profiles**.
2. Select a User Profile that contains the users for whom you want to enable recording of external Teams meetings; the Edit User Profile page appears.
3. In the **Recording** section, under the **Metering Types** group, select the 'MSFT Teams Hosted by Other Organization' check box:



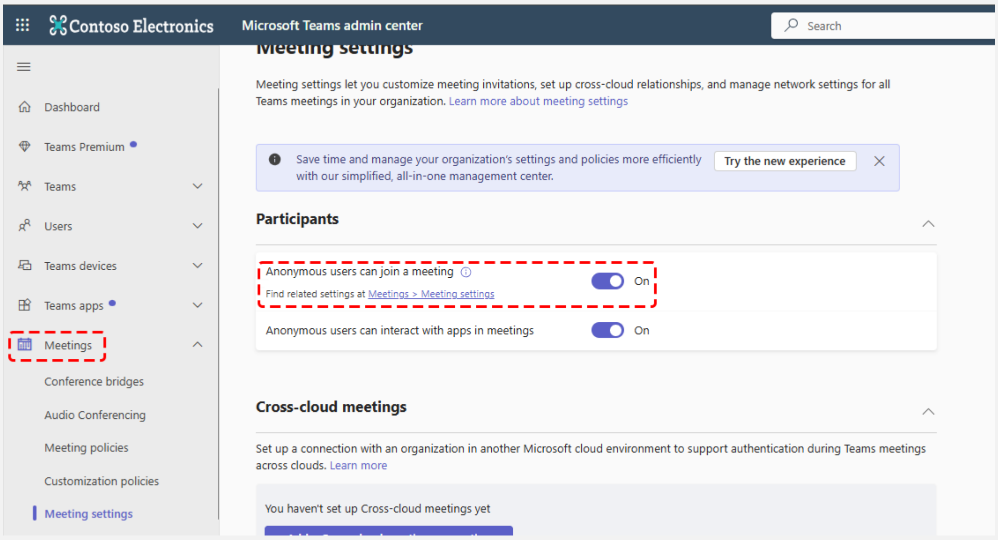
4. Click **Apply**.
5. (Optional) To customize the name of the Meeting Insights bot (detailed information in Customizing Bot Names for Recording Zoom and External Teams Meetings on page 104):
   a. In the Admin Settings navigation pane, expand **Integrations**, and then click **UC Recording**.
   b. Under **MSFT Teams Hosted by Other Organizations**, in the 'Bot Name' field, configure a bot name. To view the placeholders that you can use, click the **i** icon.



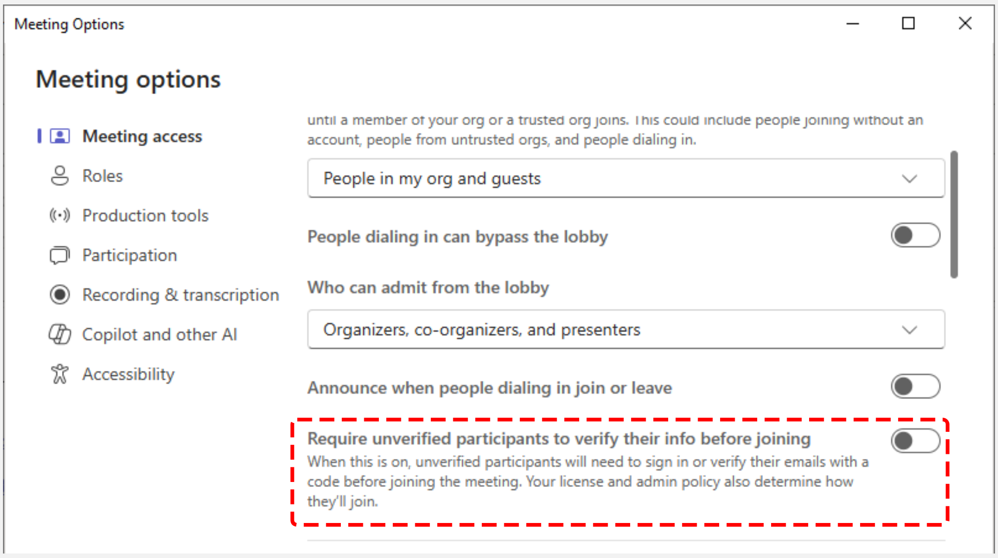
c. Click **Apply**.

For Meeting Insights to record external Teams meetings, the administrator of the **other** organization needs to allow anonymous users to join their Teams meetings. The administrator of the other organization has various ways to manage anonymous users (detailed information is in Microsoft's documentation on managing anonymous participants):

- **Organization-wide policy:** The 'Anonymous users can join a meeting' setting must be enabled (default) in Teams admin center:



- **Specific meeting policy:** The organizer of the meeting must make sure that the meeting's policy allows anonymous users to join. By default, this is allowed ('Require unverified participants to verify their info before joining' is disabled):



9 Recording Teams Live Events or Webinars

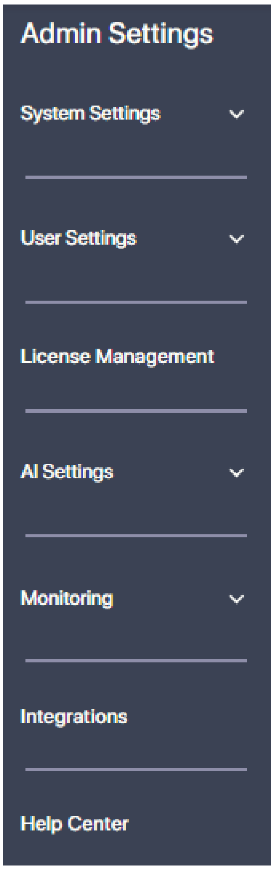
➢ **To record Teams Live Events or Webinars:**

- Make sure to add the Meeting Insights Assistant (MIA) email address to the invitation or forward the invitation to MIA.

> ⚠ MIA can’t be added as a presenter | producer.

10 Configuring System Settings

Regular users cannot perform management tasks. Only enterprise admins can. After logging in as admin, view 'Admin Settings' displayed.



Tools

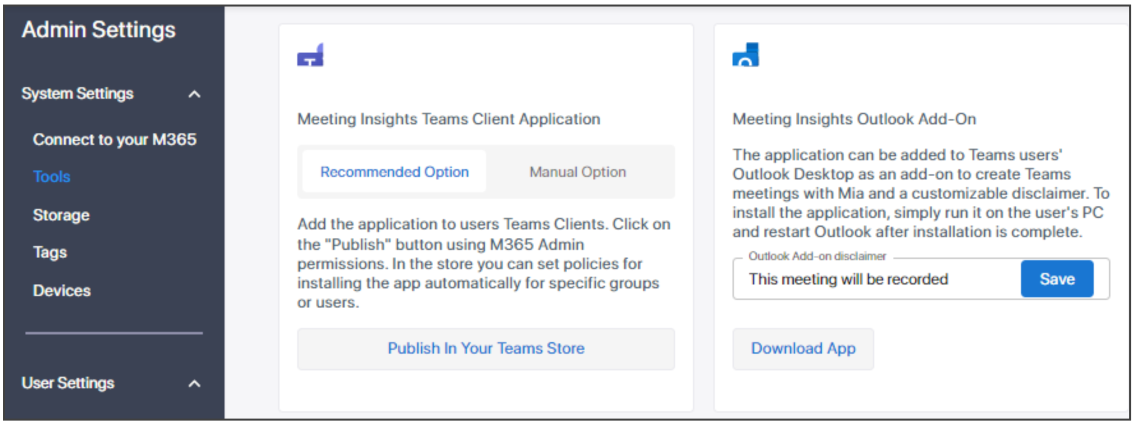
Two supplementary apps are provided by AudioCodes as installation additions:

- Meeting Insights Teams add-on provided by AudioCodes for accessing the portal from within the Teams client.
- Meeting Insights Outlook add-on provided by AudioCodes to make scheduling of recorded meetings easier | meetings with MIA.

The Tools page enables admins to add the Meeting Insights app to the Teams client and/or to Outlook.

➢ **To add the app to Teams client| Outlook:**

1. Under the 'System Settings' menu, click the **Tools** option.



2. (Optionally) Add the Meeting Insights app to users':
   - Teams client - go here
   - Outlook - go here

Adding Meeting Insights to Teams Client

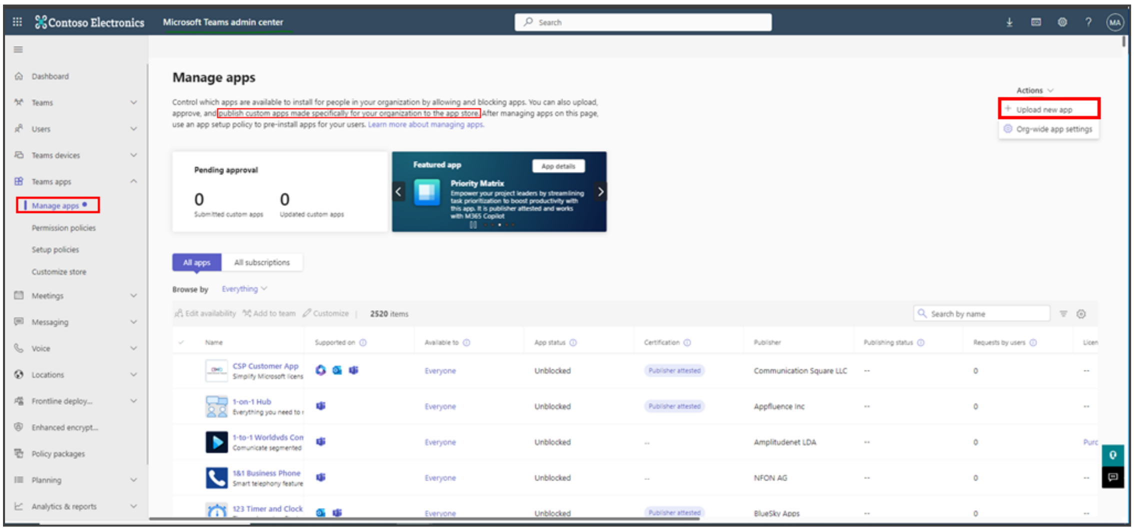
The Tools page enables the admin to add the Meeting Insights app to Teams users' Teams clients.

- This step is usually performed during the initial setup in the 'Connect to your M365' page as shown here (last step).
- Optionally, admin can *manually* add the app to the Teams store *without needing to grant permissions*, as described below.

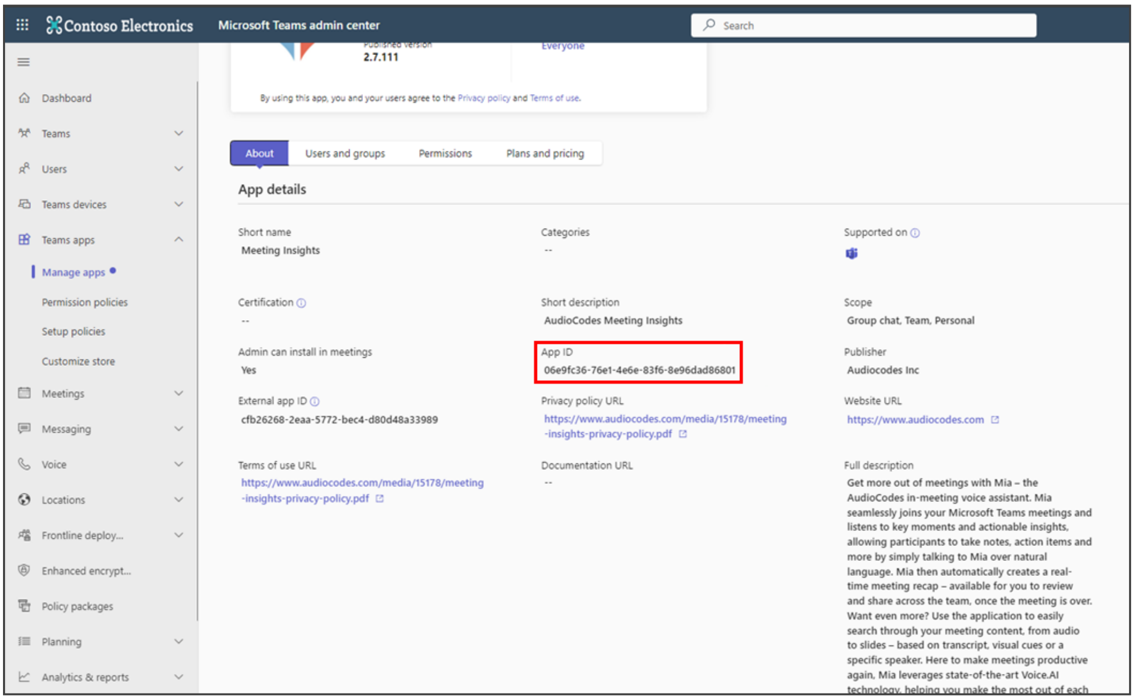
➢ To add the Meeting Insights app:

1. Under the 'System Settings' menu, click the **Tools** option.
2. Under 'Meeting Insights Teams Client Application' either:
   - Click **Recommended Option** and then click **Publish in your Teams Store**

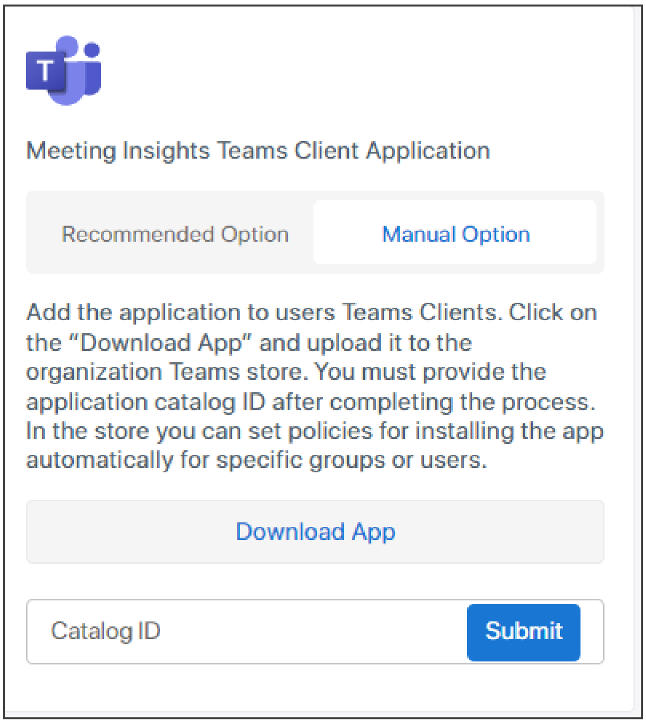
     -OR-
   - Manually add the Meeting Insights app to the Teams client (if for example it has been customized for your organization and you harbor concerns about Meeting Insights requesting permissions for Teams app publishing):
     i. Download the app package.
     ii. Add it manually to the Teams store: In Teams admin center, open the 'Manage apps' page and upload it as shown in the figure below:



iii. Locate the Catalog ID that is generated and allocated to the app:



iv. Update it in Meeting Insights under **Tools** > **Manual Option**:



v. Enter it in the 'Catalog ID' field and then click **Submit**.

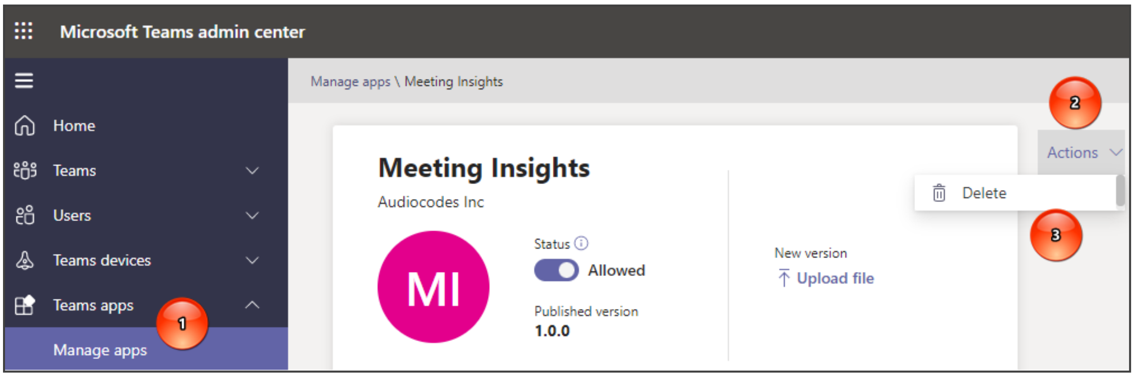
Alternatively, add the app during the initial setup in the 'Connect to your M365' page as shown here (last step).

Adding App to Organization's Teams Store via TAC

This section describes how to add the Meeting Insights app to your organization's Microsoft Teams Store via Microsoft's Teams admin center (TAC).

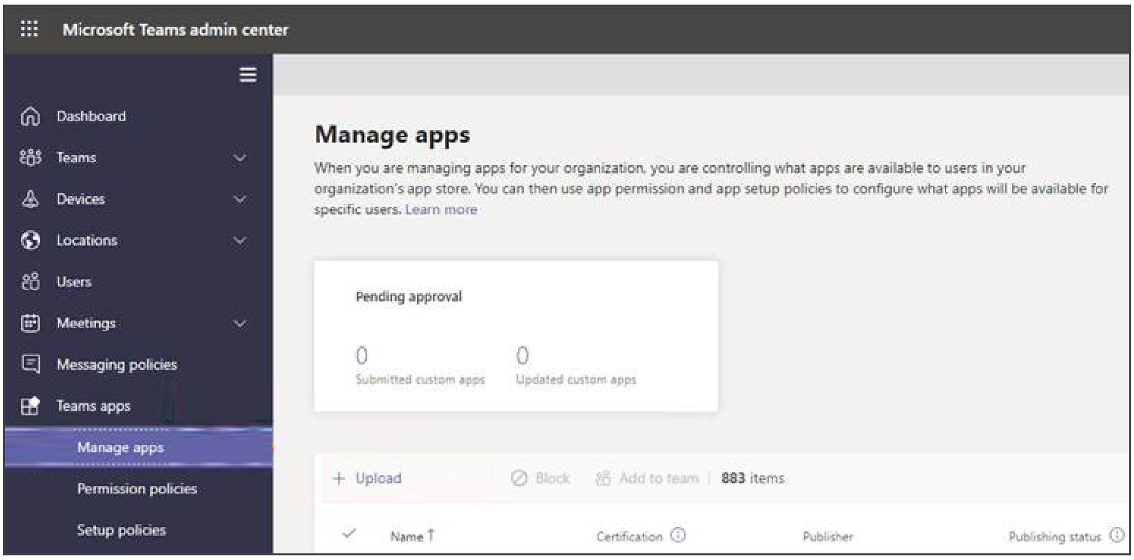
➢ **To add Meeting Insights app to Teams store via Teams admin center:**

1. Sign in to your organization's Teams admin center with your Office 365 admin account.
2. If the Teams store has the previous version of Meeting Insights Teams app, you need to remove it:
   a. From the left navigation menu, navigate to **Teams apps** > **Manage apps**.
   b. Search for the Meeting Insights app, and then from Actions drop-down menu, choose **Delete**:



3. Upload the installation file for the Meeting Insights Teams app:

   a. From the left navigation menu, navigate to **Teams apps** > **Manage apps**, and then click **Upload**:



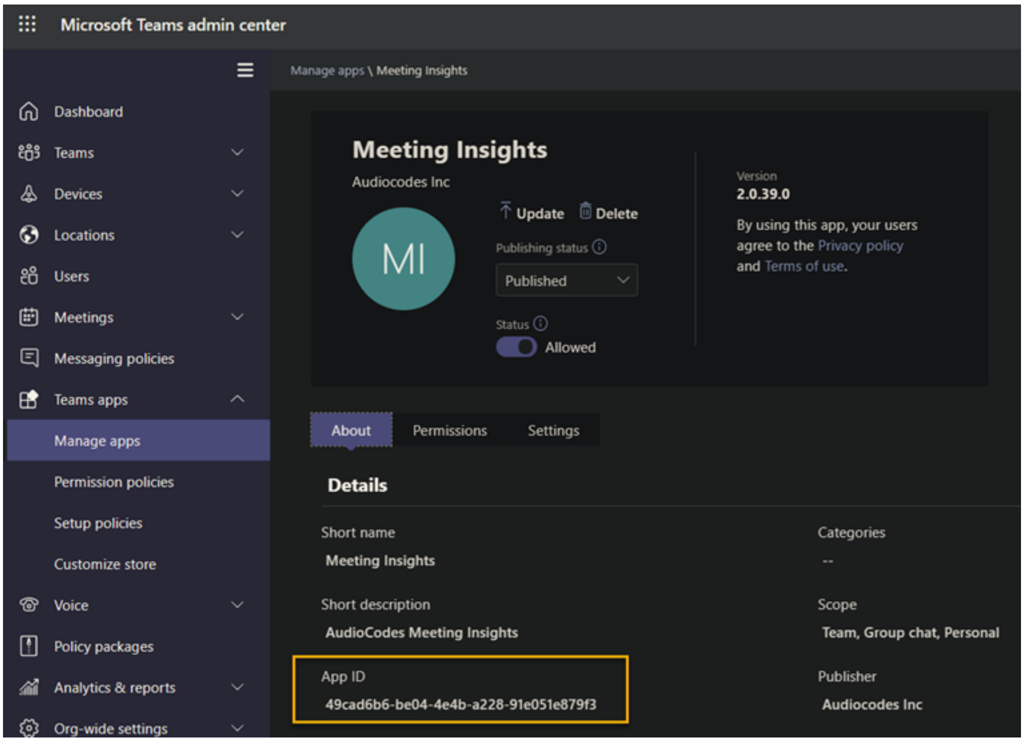
   b. In the displayed dialog box, click **Select a file**, and then browse to and select the Meeting Insights Teams app installation file (*TeamsApp.zip*) that you received from AudioCodes.

4. Provide AudioCodes with the app ID:

   a. From the left navigation menu, navigate to **Teams apps** > **Manage apps**.

   b. Locate the newly installed Meeting Insights Teams app in the list of apps, and then select it.

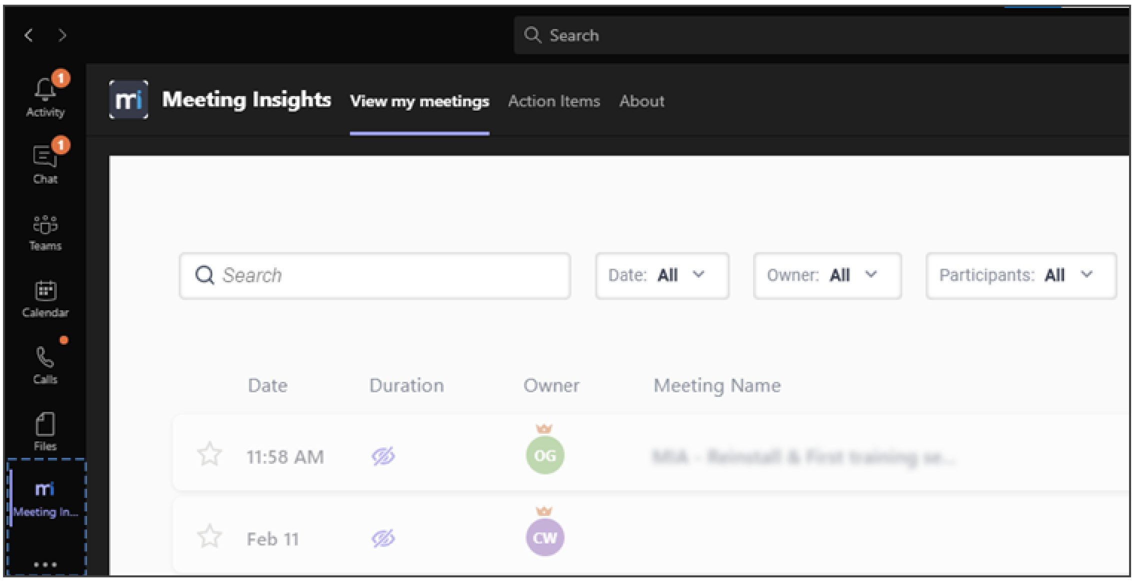
   c. Under the **About** tab, copy the 'App ID' field value:



d. Enter the app ID in the 'Catalog ID' field in Meeting Insights' Tools page as shown here.

5. Pin the Meeting Insights app to the Teams client navigation bar:

   In the Teams client left navigation bar, click the 3-dot (...) button, and then choose the newly installed Meeting Insights app; a Meeting Insights icon is added to the navigation bar:



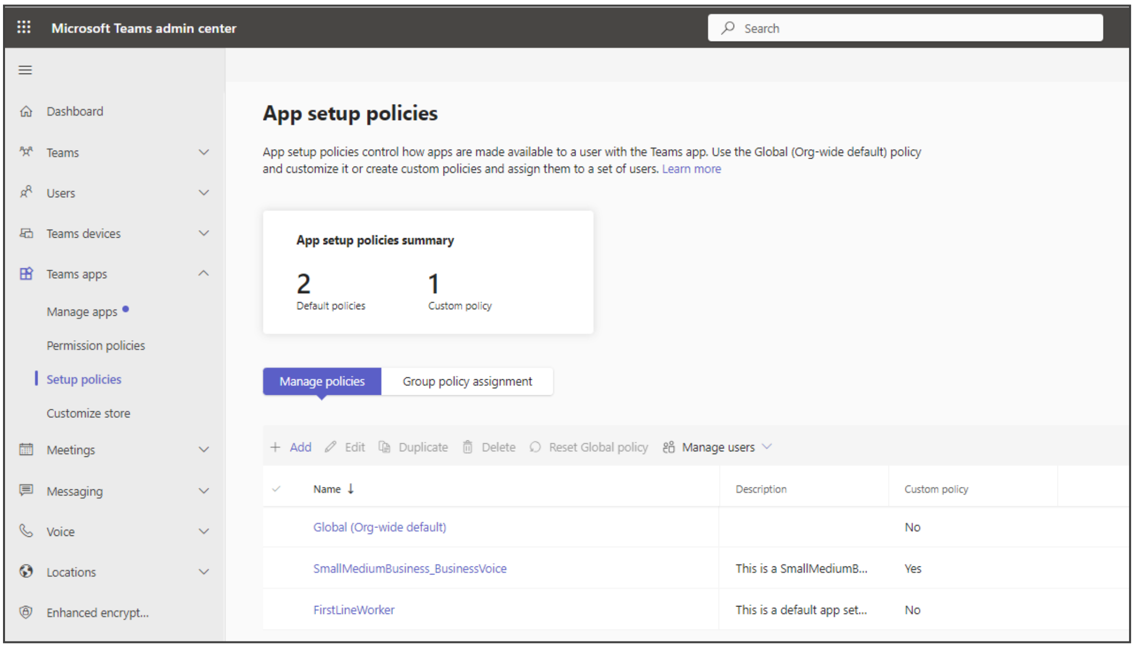
Admins are recommended to add and pin Meeting Insights Teams app to the whole organization or to user group(s) that will be using the application. See here for more information.

Add and Pin Meeting Insights Teams App to the Entire Organization or to User Group(s)

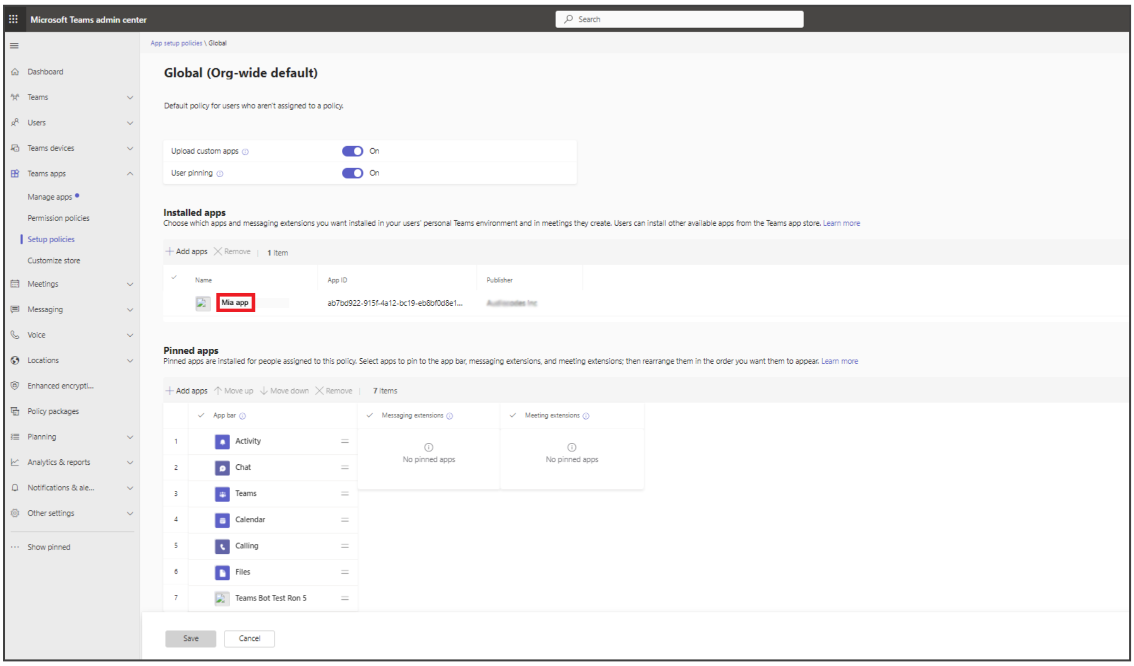
Admins are recommended to add and pin the Meeting Insights Teams app to the whole organization or to user group(s) that will be using the app.

➢ To add and pin the Meeting Insights Teams app to the whole organization or to user group(s):

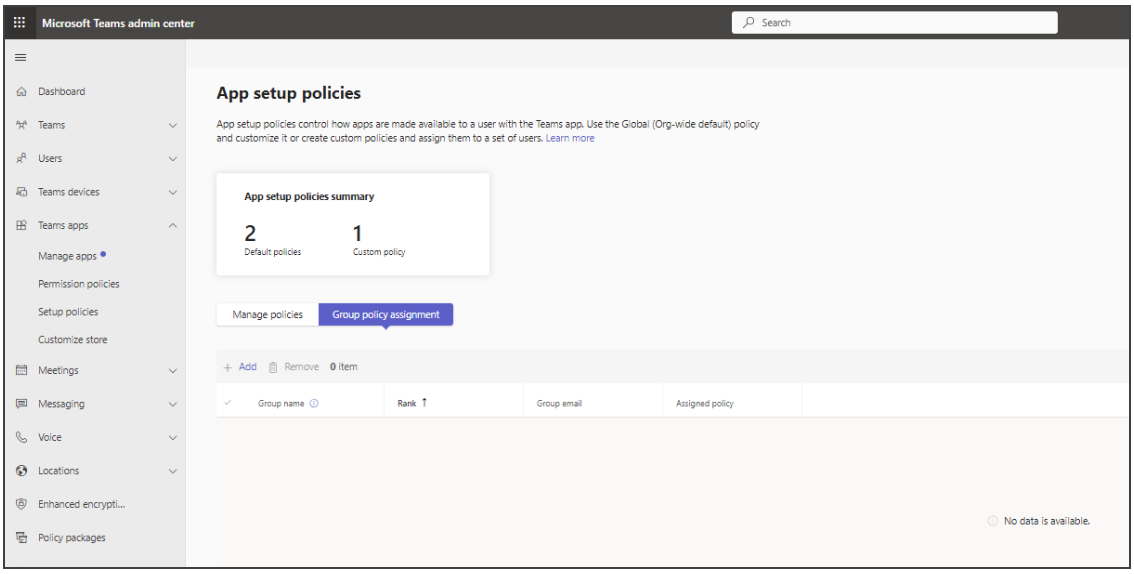
1. Open Microsoft Teams admin center (TAC) and add to the organizational policy or create a new policy and assign it to the users or groups.



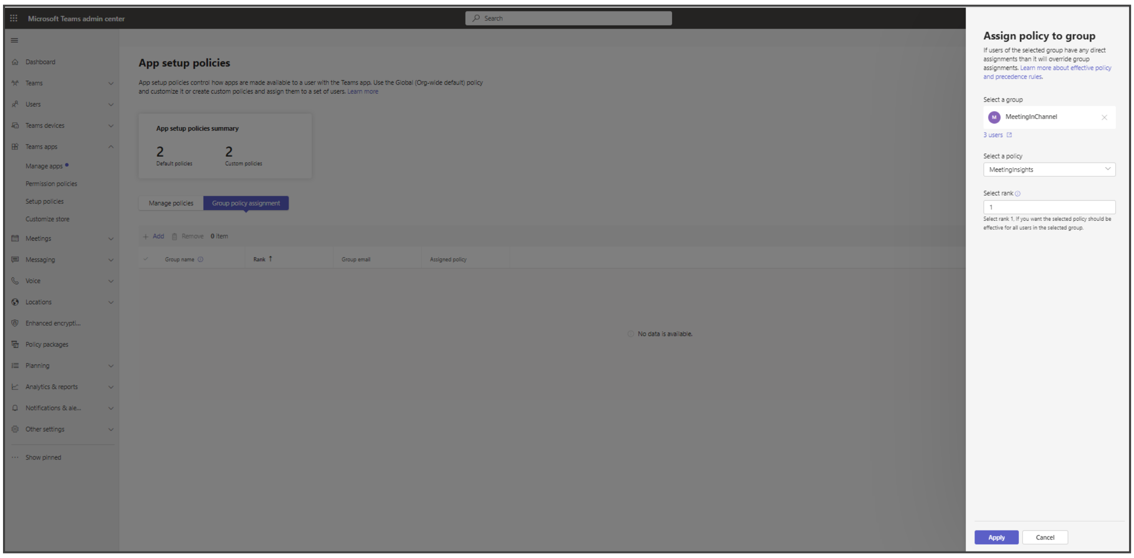
2. Add Meeting Insights Teams app to the installed apps and to the pinned apps (recommended) so that it'll be displayed for users by default.



3. To apply to a group, create a separate policy, add the Meeting Insights Teams app to the installed and pinned apps, and then assign group(s) as shown below.
4. To assign to a group, click **Group policy assignment** under the setup policy option.



5. To assign groups, click **Apply**.

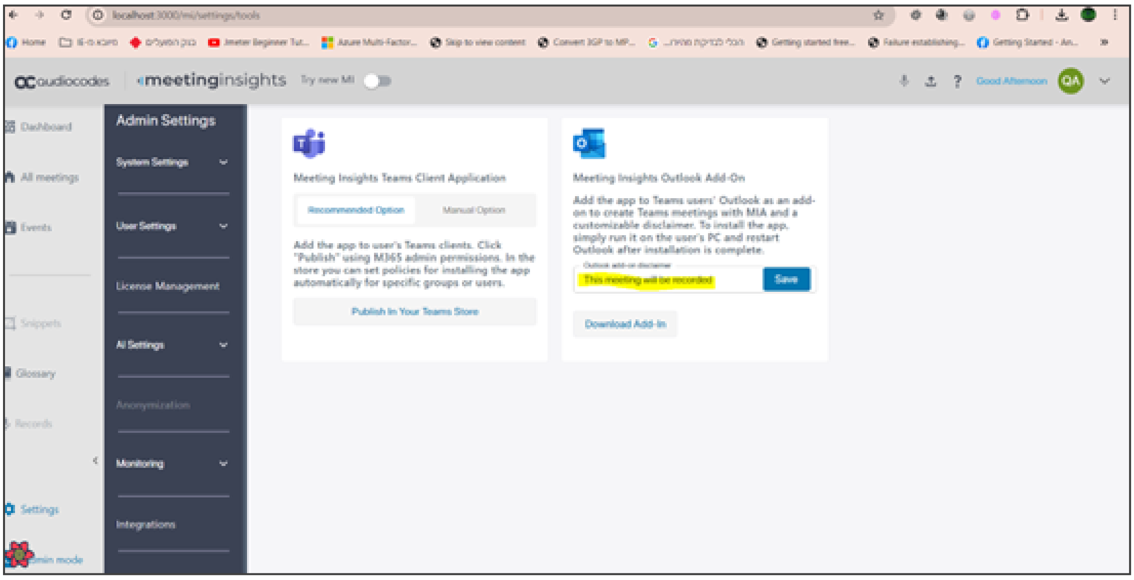


Setting up Outlook Add-In

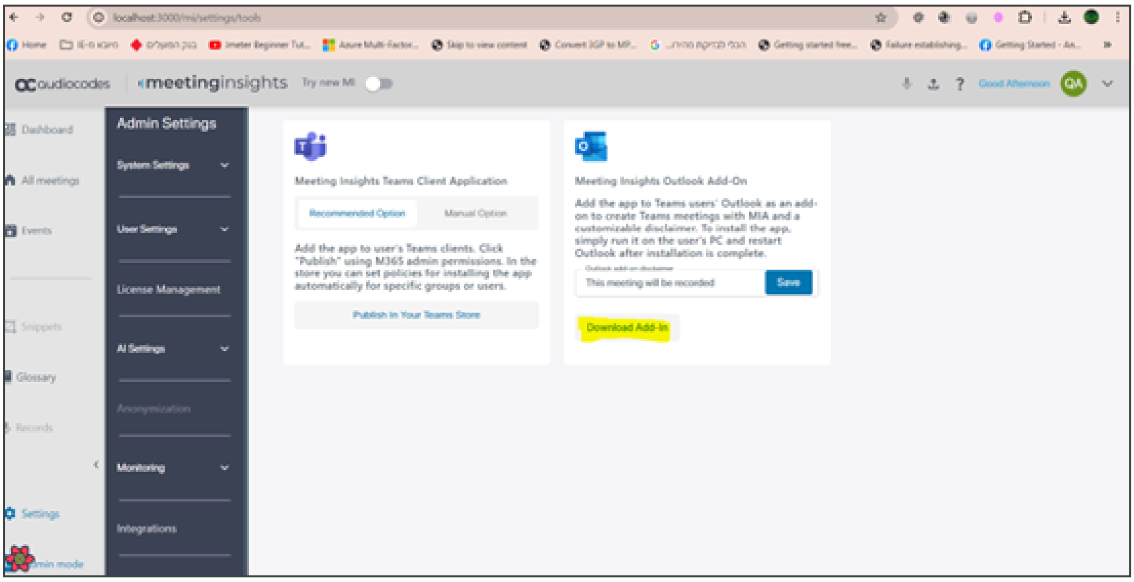
The Tools page enables admin to add the Meeting Insights app to Teams users' Outlook as an add-on to create Teams meetings with MIA. The instructions below show how to set up the Microsoft Outlook add-in.

➢ To set up Outlook add-in:

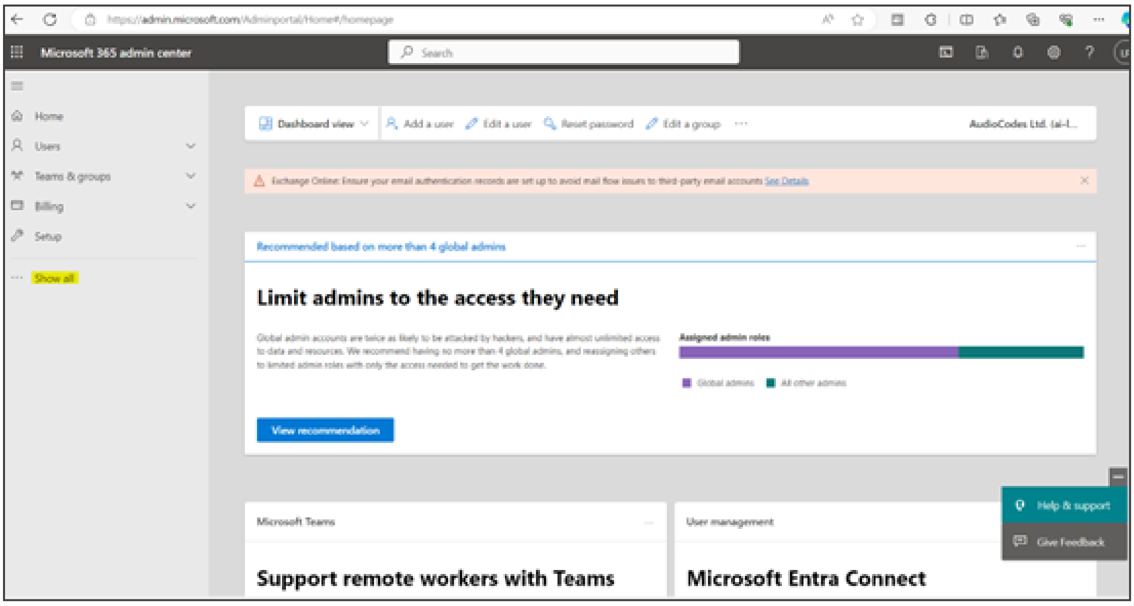
1. [Recommended] Set a disclaimer in the Meeting Insights 'Tools' page (**Admin Settings** > **System Settings** > **Tools**), as shown here:



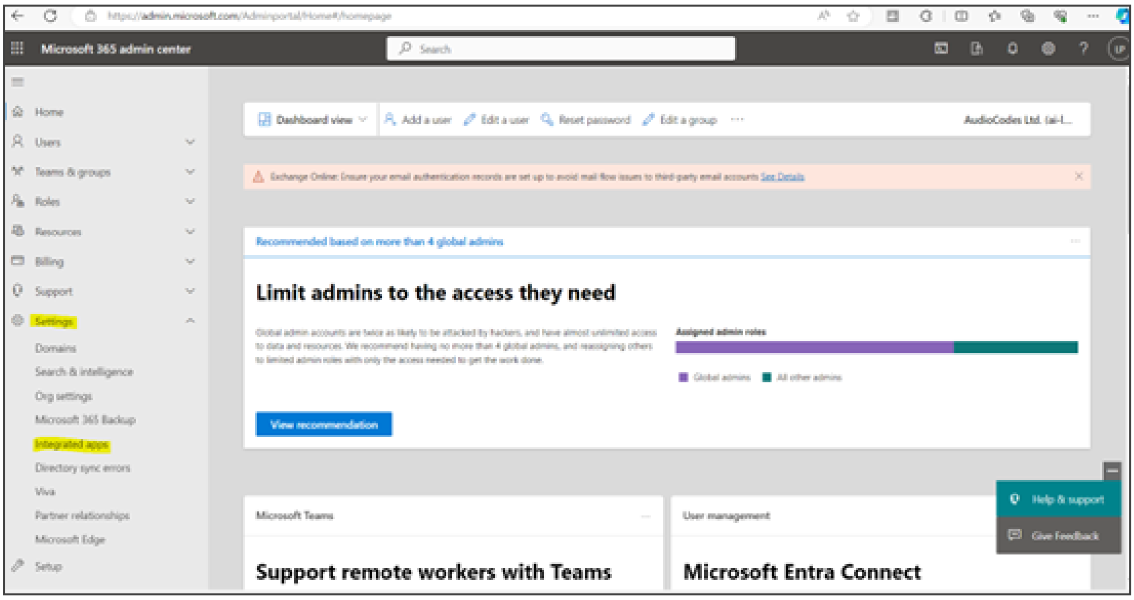
2. Download the add-in by clicking the **Download Add-In** button



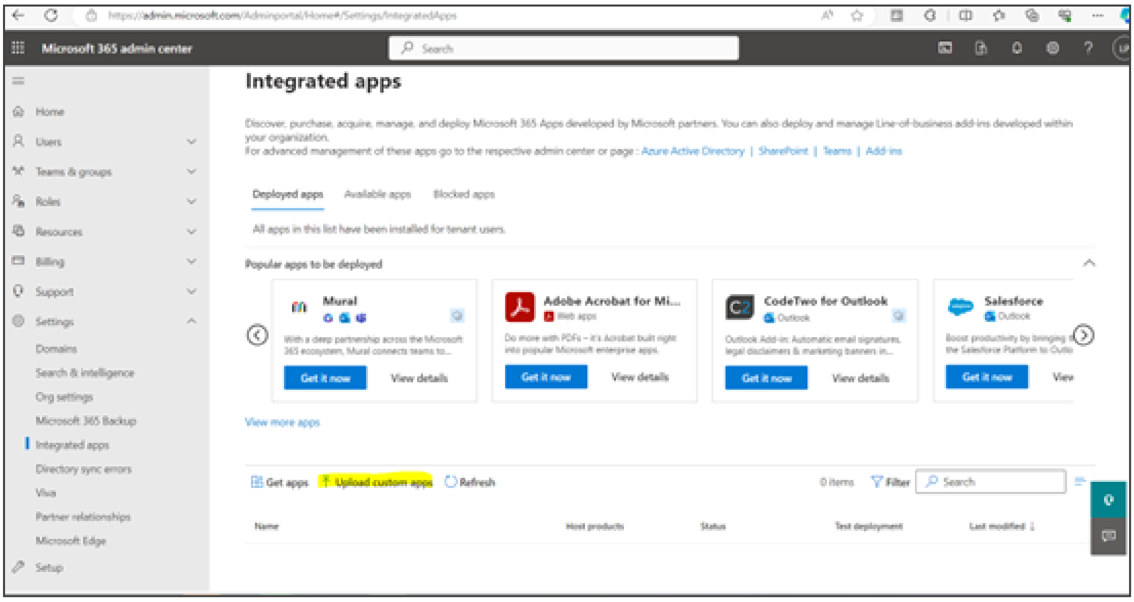
3. Log in to https://admin.microsoft.com/ to view the Microsoft 365 admin center.



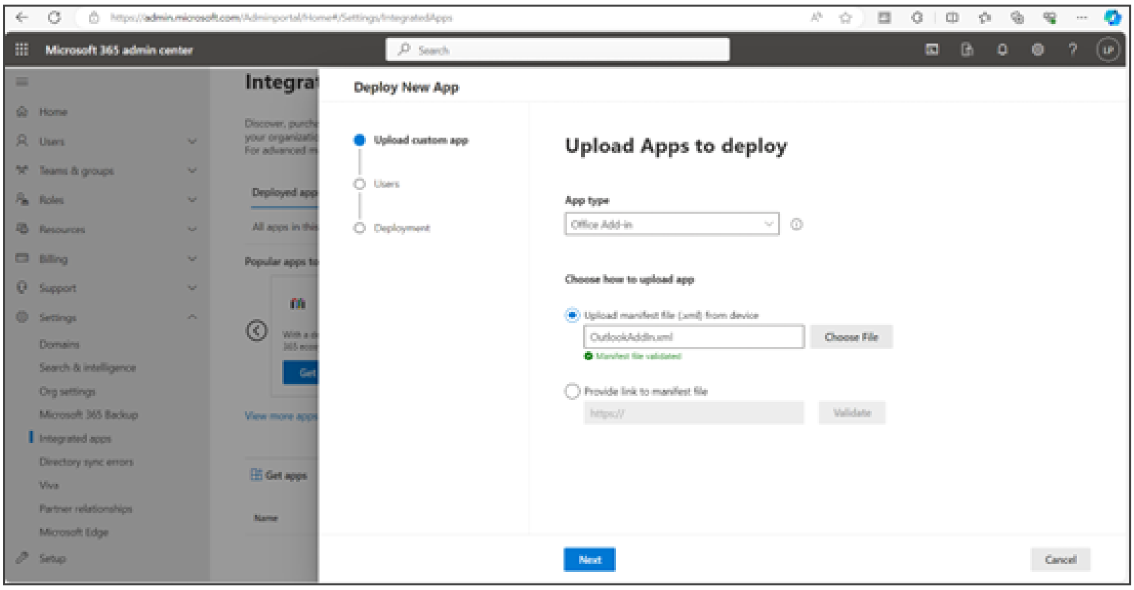
4. Click **Show All** as shown in the preceding figure.



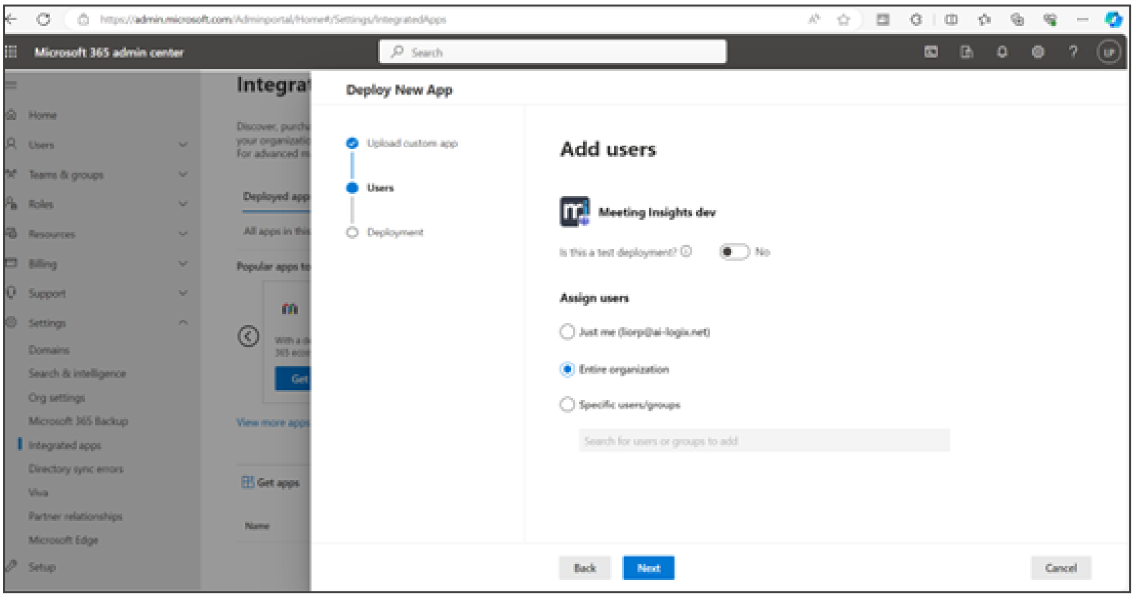
5. Expand the **Settings** menu as shown in the preceding figure and click the **Integrated apps** option.



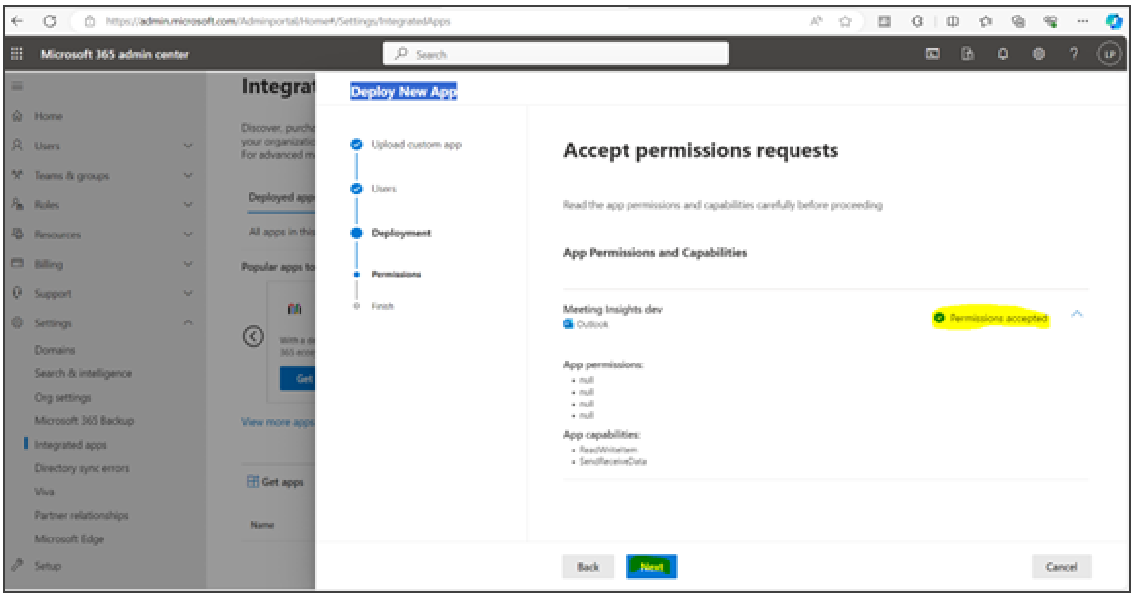
6. Click the **Upload custom apps** option.



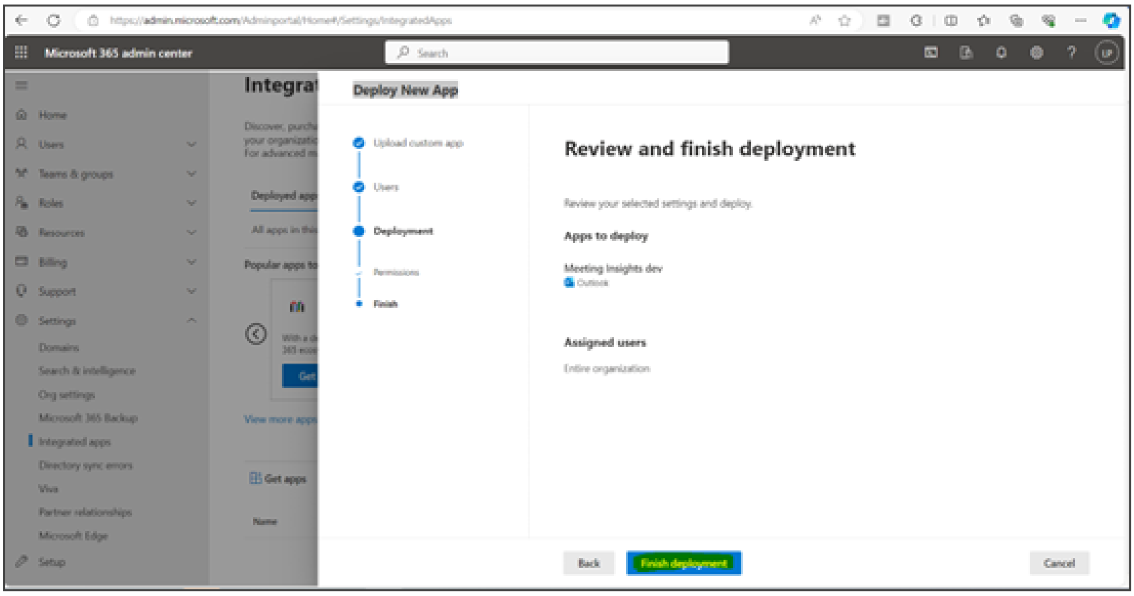
7. From the 'App type' drop-down, select **Office Add-in**, select the **Upload manifest (.xml) from device** option and then click **Choose File**. Click **Next** after xml validation.



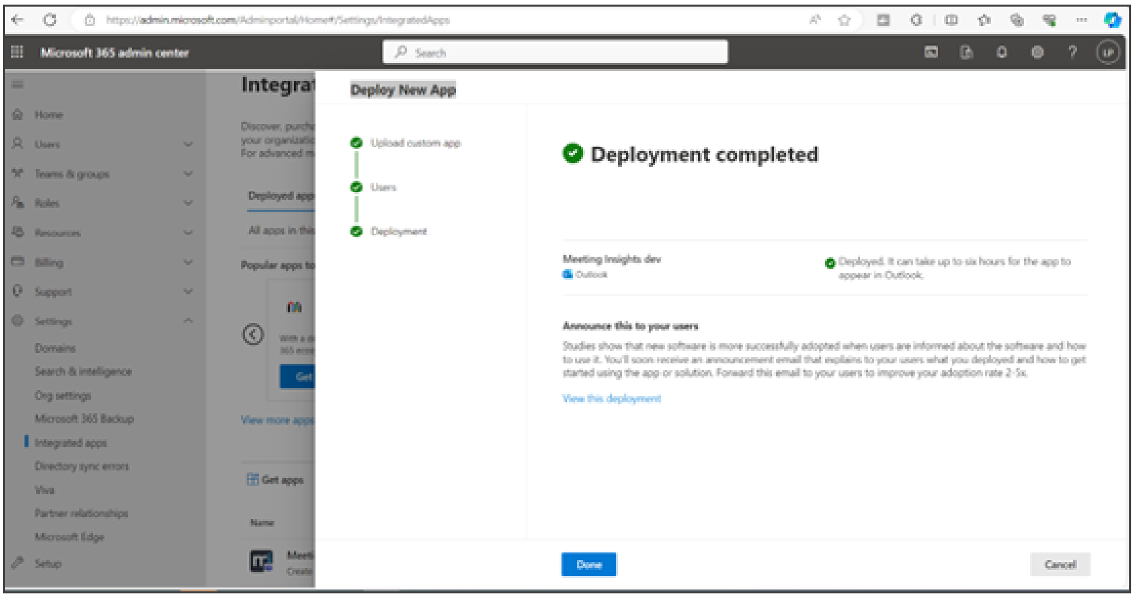
8. Select who can use the add-in and then click **Next**.



9. Accept the required permissions the application requires by clicking on the permissions and then click **Next**.



10. Review the deployment and then click **Finish deployment**.



View the screen shown in the preceding figure after the deployment is completed.

Storage

By default, Meeting Insights stores meeting recording audio, screen sharing content, generated images, transcriptions, and AI insights in separate Azure Blob storage, tailored to regional preferences, and hosted in AudioCodes data centers. For more information, see Storage Hosted on AudioCodes Azure Blob on page 54.

However, Customers who need control and ownership of their stored data can add their Azure Blob Storage accounts for various locations (Bring Your Own Blob Storage or BYOS). Once the BYOS locations are configured, they can be assigned to user profiles, enabling recordings for users assigned to these profiles to be stored in the designated storage. For more information on BYOS, see Storage Hosted on Customer Azure Blob on page 55.

Meeting Insights supports the following Azure storage options:

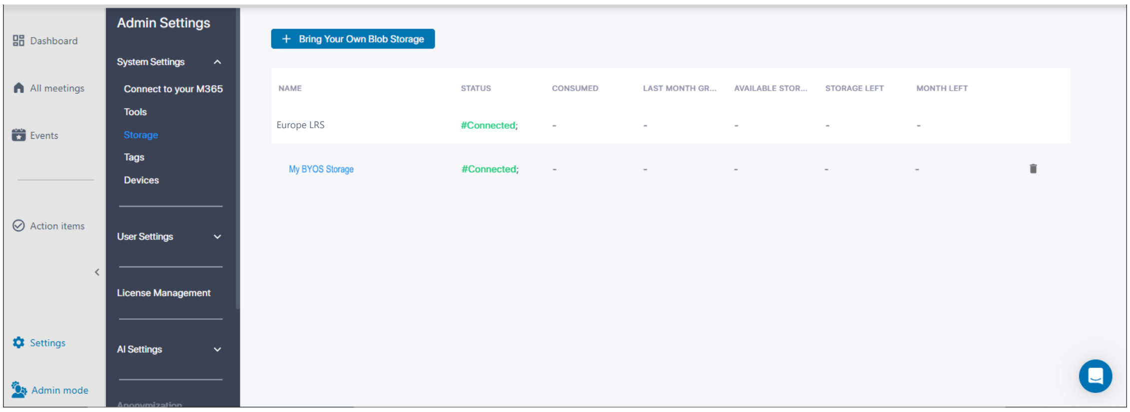
- **Local redundant storage (LRS):** This is a local, redundant storage, whereby data is replicated in the same region.
- **Geo-redundant storage (GRS):** This is a geographically, redundant storage, whereby data is replicated across two regions (primary and secondary). The benefit of GRS is that it protects the recordings in case of a regional outage.

Meeting Insights also allows you to monitor the storage services, by displaying maximum storage, storage utilization, and remaining storage.

- Meeting Insights default storage is LRS.
- GRS is a feature available for purchase from AudioCodes.
- Bring Your Own Blob Storage requires the BYOS feature key.

➢ To view Meeting Insights storage accounts:

1. Under the 'System Settings' menu, click the **Storage** option; the default storage account is displayed (e.g., Europe LRS).



The following table describes the table columns:

Table Column	Description
Name	Displays the region in which the storage (LRS) is located (e.g., 'Canada LRS').
Status	Displays the status of connection to storage account: ■ "Connected" ■ "Disconnected" ■ "Failed"
Consumed	Displays the storage space (in GB) that has been utilized. **Note:** This column is applicable to Locally-Redundant Storage (LRS) and

Table Column	Description
	Geo-Redundant Storage (GRS).
Last Month Growth	Displays the change of storage for the last month. This typically shows an increase (growth), but if more meeting recordings are deleted than created, then it shows a decrease.
Available Storage	Displays the total available storage space (in GB). **Note:** This column is applicable only to GRS.
Storage Left	Displays the remaining storage space (in GB). **Note:** This column is applicable only to GRS.
Month Left	Displays the estimated number of months remaining before the storage is full.

Storage Hosted on AudioCodes Azure Blob

The Meeting Insights application stores the recorded media (audio, screen sharing content, generated images) and recaps (transcription, summary, action items, and AI-generated insights) in separate Azure Blob storage containers, tailored to regional preferences and hosted in AudioCodes data centers.

Meeting Insights supports the following Azure storage options:

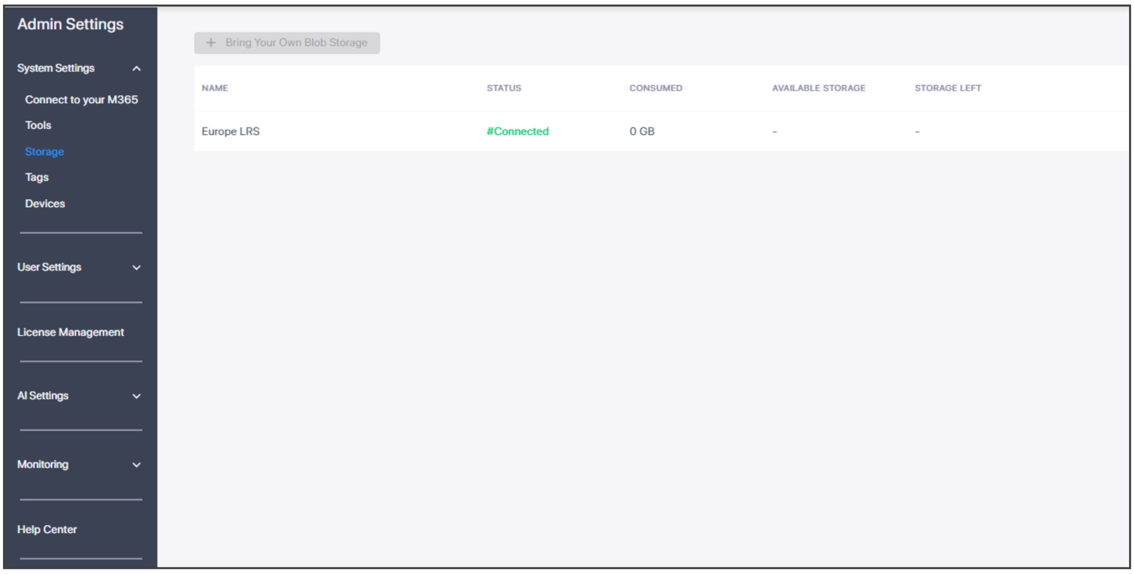
- **Local redundant storage (LRS):** This is a local, redundant storage, whereby data is replicated in the same region. By default, Meeting Insights provides you with a single storage LRS platform in AudioCodes data center. This storage platform doesn't include storage monitoring.
- **Geo-redundant storage (GRS):** This is a geographically, redundant storage, whereby data is replicated across two regions (primary and secondary). The benefit of GRS is that it protects the recordings in case of a regional outage. If you require GRS, you can purchase this feature from AudioCodes. GRS is enabled by a feature key, which also specifies the storage capacity (GB). This storage platform allows you to monitor storage.

For monitoring the storage connectivity status and capacity, see Monitoring Storage Connectivity Status and Capacity on page 59.

Meeting Insights doesn't limit storage when hosted by AudioCodes.

➢ To view storage hosted by AudioCodes:

- Under the 'System Settings' menu, click the **Storage** option; the default storage account is displayed (e.g., Europe LRS).



Storage Hosted on Customer Azure Blob

If you require control and ownership of your stored Meeting Insights data, you can use Meeting Insights *Bring Your Own Blob Storage* (BYOS) feature to use your Azure Blob Storage account across different locations (regions). After configuring BYOS for each location (region), you can assign these storage accounts to specific User Profiles, ensuring that recordings for users associated with these profiles are stored in the designated storage locations.

Adding BYOS storage includes the following main steps:

1. Setting up your Azure Blob storage account.
2. Configuring Meeting Insights with your storage account (BYOS).

- Bring Your Own Blob Storage requires the BYOS feature key. Contact your Service Provider if it's not available in your Meeting Insights application.
- Make sure that your BYOS accounts are registered on your Microsoft 365 tenant.
- Performance latency may occur if the storage location is geographically distant from the Meeting Insights deployment instance.
- The customer's user information such as Display name, email, Azure OID, and recorded meeting metadata such as time, duration, subject, participants, and invitees are stored in the Meeting Insights separate database per customer.
- When a user is assigned to multiple user profiles, all profiles must be configured with the same storage. User recordings will be stored in arbitrary storage locations if the user is assigned to user profiles with distinct storage locations.
- You can delete an added BYOS storage only when there are no active meeting recordings.

Defining Your Azure Blob Storage Account

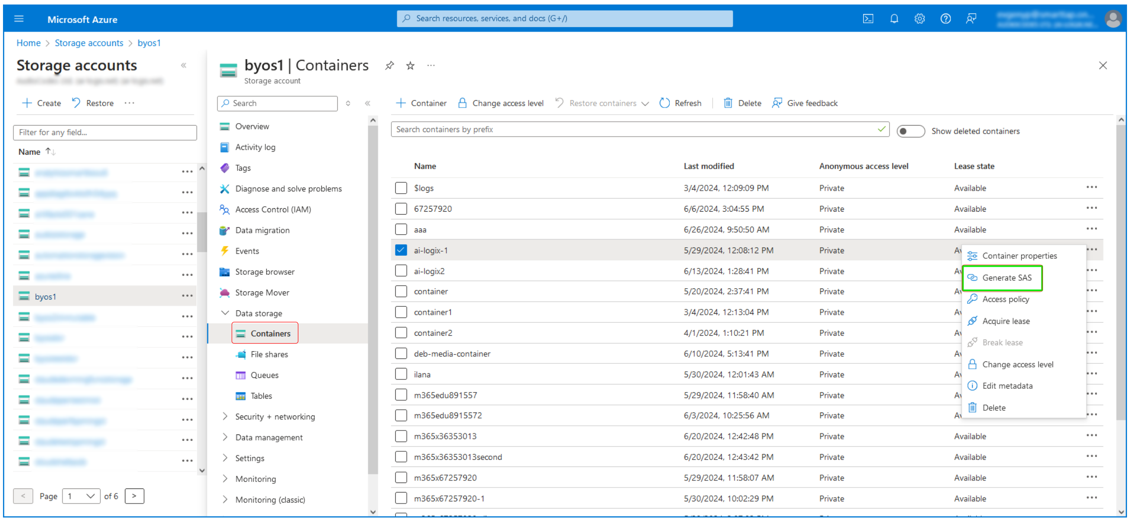
Before you can configure Meeting Insights with BYOS, the first step is to configure a storage container in your Azure Blob Storage account. This process includes generating a Shared Access Signature (SAS) token and URL, which you'll need later when configuring BYOS in Meeting

Insights. In addition, this process includes specifying a start date and time, as well as an expiry date and time for the SAS token.

> ⚠ This section assumes that you have an Azure Blob Storage account with a storage container.

➢ Set up Azure Blob Storage account:

1. Log in to your (customer tenant) Microsoft Azure portal account.
2. Access the Storage accounts page, and then select the relevant Blob Storage account.
3. Navigate to **Data storage** > **Containers**, and then select the container where you want to store media.
4. Right-click the container, and then from the drop-down menu, choose **Generate SAS**; the Generate SAS dialog box opens.

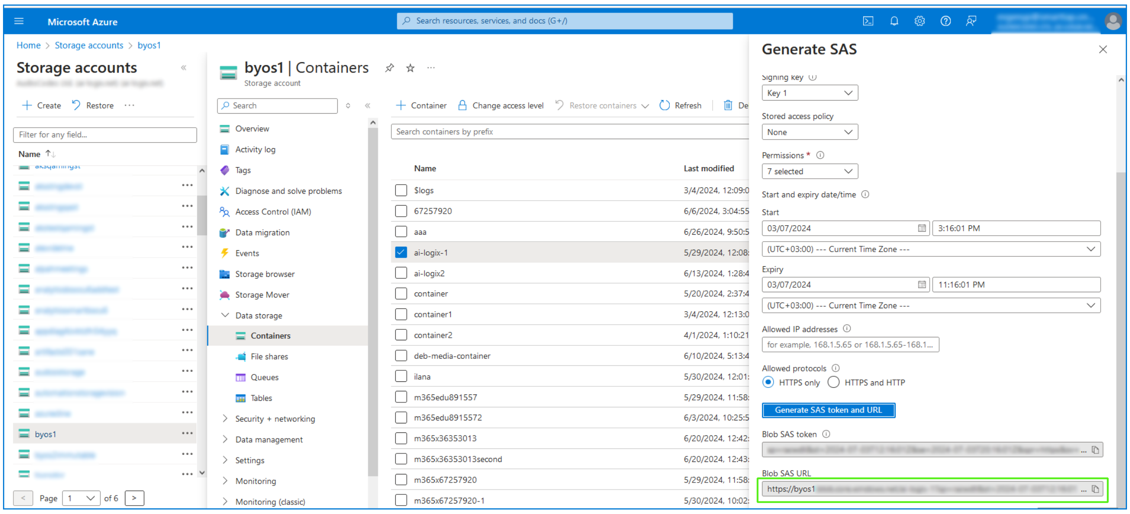


5. In the Generate SAS dialog box, configure access settings to the storage:
   a. Under the Signing method group, select the **Account key** option.
   b. From the 'Signing key' drop-down list, select **Key 1**.
   c. From the 'Stored access policy' drop-down list, select a shared access policy.
   d. From the 'Permissions' drop-down list, select (check) all the listed permissions check boxes.
   e. In the 'Start' and 'Expiry' fields, define the start and expiry time-date of the signed key, respectively.

> ⚠ For Meeting Insights' BYOC, the SAS token expiration period must be **at least three months**.

f. Under the Allowed protocols group, select the **HTTPS only** option to allow only requests using the HTTPS protocol.

g. Click the **Generate SAS token and URL** button; a shared access signature (SAS) token and URL are generated and displayed in the fields below the button:



6. Copy and paste the Blob SAS URL in a secure location (e.g., in Notepad). You'll need this URL (which includes the SAS token key) when configuring this BYOS storage in Meeting Insights (see Configuring Meeting Insights with BYOS below).

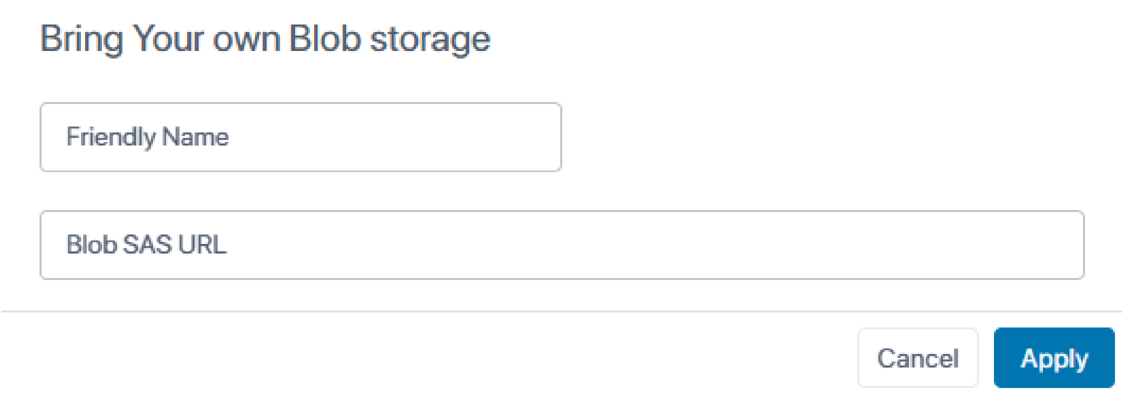
Configuring Meeting Insights with BYOS

Once you have configured your Azure Blob Storage account and generated a SAS URL, you can configure Meeting Insights with a BYOS.

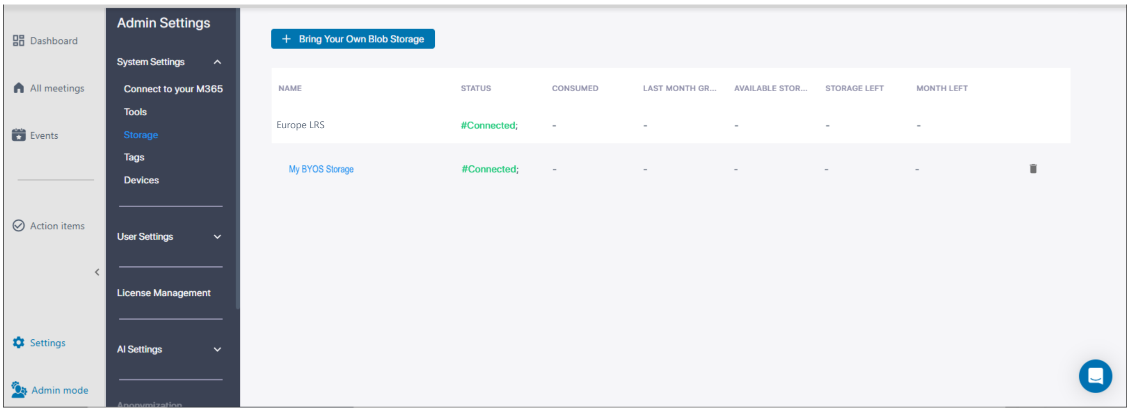
> ⚠ Meeting Insights doesn't display BYOS storage capacity. Storage monitoring can only be done through your Azure Blob storage account.

➢ To configure Meeting Insights with BYOS:

1. Under the 'System Settings' menu, click the **Storage** option; the default storage account is displayed (e.g., Europe LRS).
2. Click the **Bring Your Own Blob Storage** button; the following dialog box appears:



3. In the 'Friendly Name' field, type a meaningful name for your Blob storage container so that you can easily identify it later, especially useful if add multiple Blob storage containers (e.g., "West US BYOS" or "North Europe BYOS").
4. In the 'Blob SAS URL' field, paste the Blob SAS URL (also contains the SAS token key) that you copied from your Azure Blob Storage account (see Defining Your Azure Blob Storage Account on page 55).
5. Click **Apply**; the BYOS is added to Meeting Insights:



6. Associate the BYOS account to a Users Profile, by selecting it from the 'Select Storage' drop-down list, as described in User Profiles on page 64.

For monitoring the storage connectivity status, see Monitoring Storage Connectivity Status and Capacity on the next page.

Connectivity Issues to BYOS Storage

If Meeting Insights is unable to access the BYOS storage, it deletes the recording after several retry attempts. Loss of connectivity to the BYOS storage can occur for several reasons, such as:

- Storage no longer exists
- Network issues
- SAS token key expired

Meeting Insights notifies you about the upcoming token key expiration at 30 days, 7 days, and on expiration day, both via email and in the system activity logs. In addition, Meeting Insights triggers an alarm if the connection to the storage is lost or the token key expires.

- The SAS token key expiration period must be at least three months.
- To prevent outages and the potential loss of recordings, it's essential that you generate a new SAS token key before it expires and update Meeting Insights with the new key.

Monitoring Storage Connectivity Status and Capacity

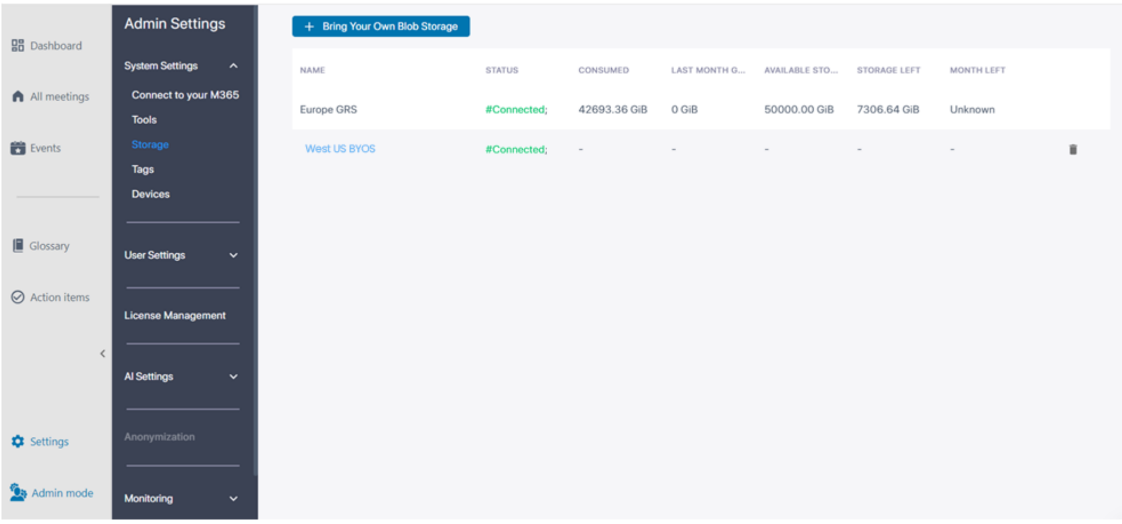
Meeting Insights allows you to monitor the storage connectivity status as well as storage capacity (depending on storage platform). The support for monitoring storage per platform is shown below:

Storage Platform	Monitoring of Storage Capacity
Storage hosted by AudioCodes Azure Blob storage account	Storage monitoring depends on Blob storage option: ■ **LRS:** No monitoring provided. ■ **GRS:** Monitoring is through Meeting Insights (described below).
Storage hosted by Customer's Azure Blob storage account	Monitoring is through Customer's Azure Blob storage account (not through Meeting Insights).

The following describes how to monitor storage connectivity status and storage capacity through Meeting Insights.

➢ To monitor storage connectivity and capacity:

- Under the ‘System Settings’ menu, click the **Storage** option; the storage account(s) are displayed:



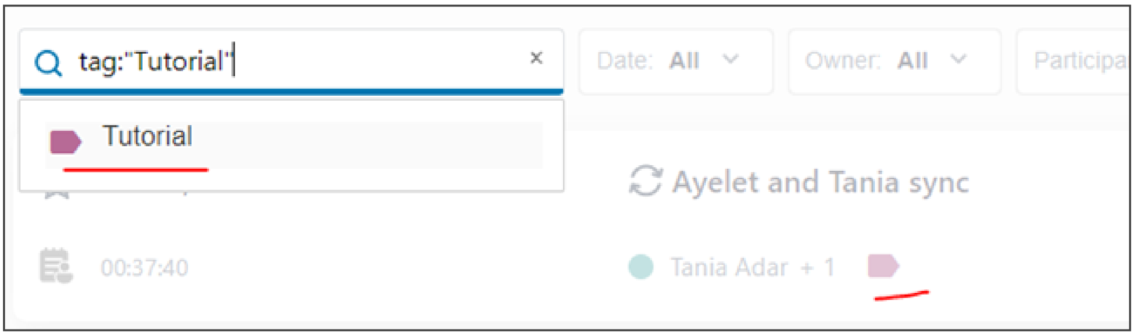
The storage connectivity status and capacity are monitored using and following fields on the page:

<table>
<tr><th>Table Column</th><th>Description</th></tr>
<tr><td>Name</td><td>Displays the region in which the storage is located (e.g., "Canada LRS", "Europe GRS", or "West US BYOS").</td></tr>
<tr><td>Status</td><td>Displays the status of connection to storage platform:
"Connected"
"Disconnected"
"Failed"
"Pending"</td></tr>
<tr><td>Consumed</td><td>Displays the storage space (in GB) that has been utilized.
Note: This column is applicable only to AudioCodes hosted storage for GRS.</td></tr>
<tr><td>Last Month Growth</td><td>Displays the change of storage for the last month. This typically shows an increase (growth), but if more meeting recordings are deleted than created, then it shows a decrease.
Note: This column is applicable only to AudioCodes hosted storage for GRS.</td></tr>
<tr><td>Available Storage</td><td>Displays the total available storage space (in GB).
Note: This column is applicable only to AudioCodes hosted storage for</td></tr>
</table>

Table Column	Description
	GRS.
Storage Left	Displays the remaining storage space (in GB). **Note:** This column is applicable only to AudioCodes hosted storage for GRS.
Month Left	Displays the estimated number of months remaining before the storage is full. **Note:** This column is applicable only to AudioCodes hosted storage for GRS.

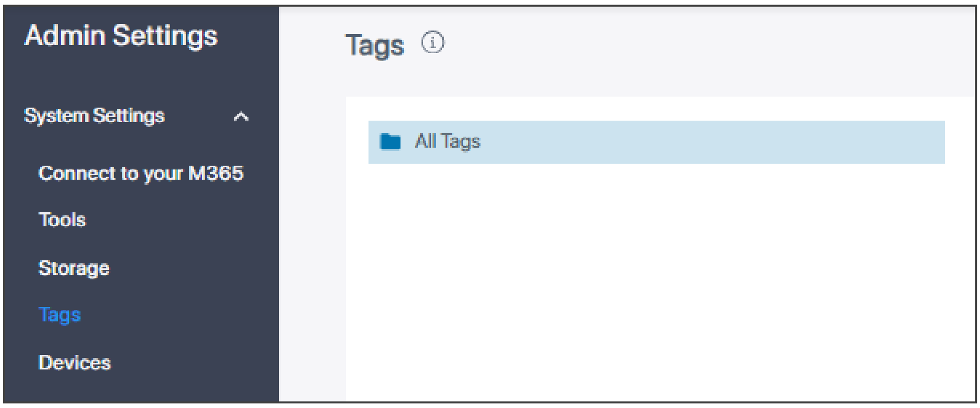
Tags

Tags can be added to meeting recordings to make it easier to search for specific information in them.

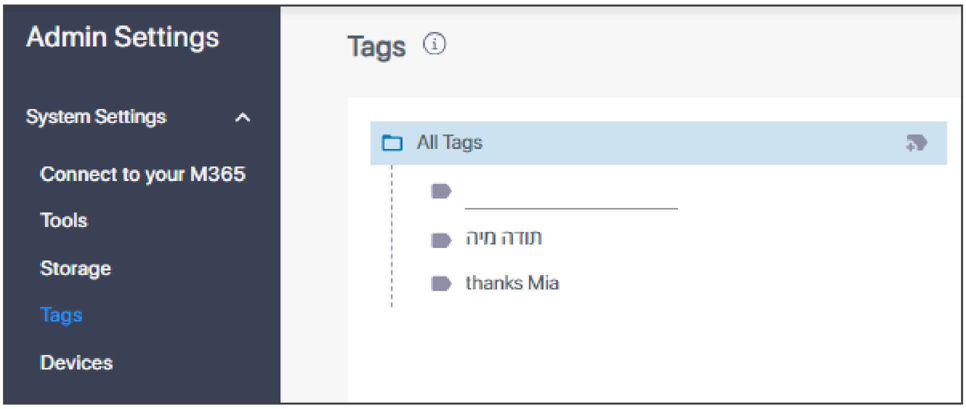


➢ To define a tag:

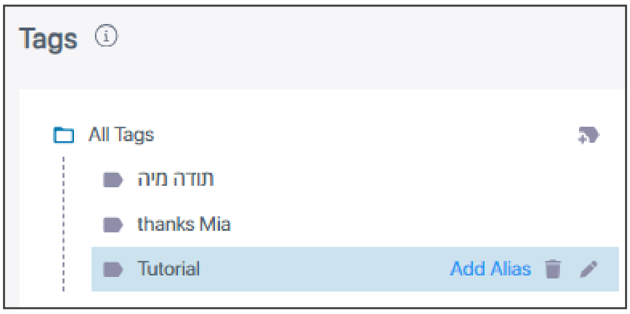
1. Under the 'System Settings' menu, click the **Tags** option.



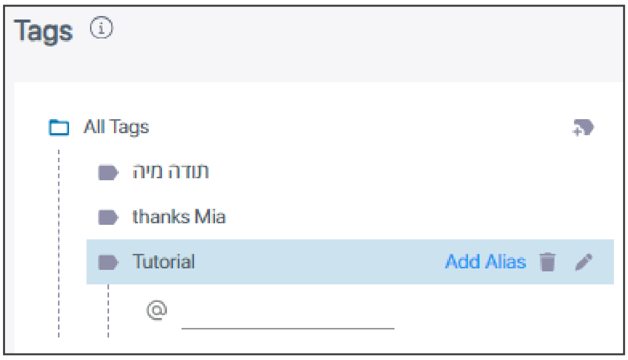
2. Point you mouse over the **All Tags** bar and then click the icon.



3. In the field  , enter a tag name and then enter.



4. Select **Add Alias** from the menu.



Two categorical levels of 'alias' can be added under the tag. These categorical levels facilitate organizing your corporate meetings around subject matter (for example, around products).

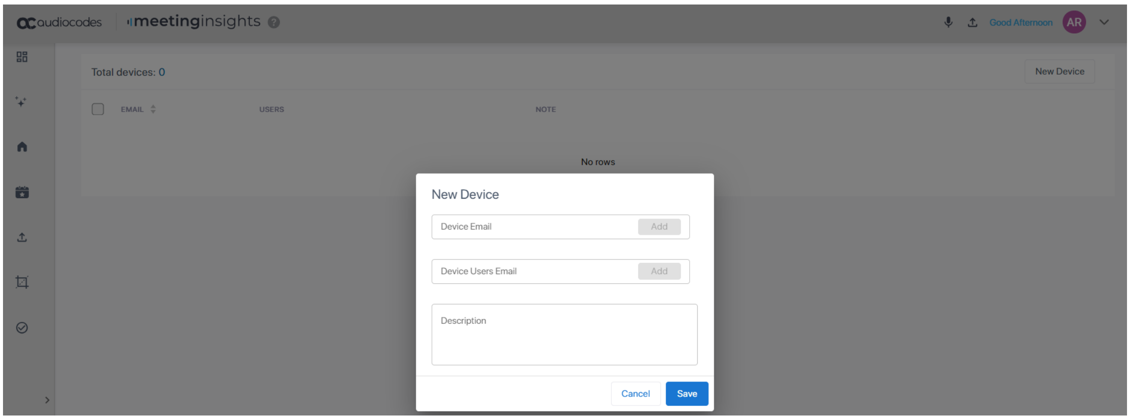
5. Optionally select the delete icon or edit icon to facilitate building meeting junctures.

Devices

Admin must define a device in the enterprise's physical conference room. Meeting Insights identifies speakers participating physically in the room by their voice and doesn't assign a specific user to the device. Defining the room's email address is sufficient to associate the device with the room.

➢ To configure a device:

1. Under the 'System Settings' menu, click the **Devices** option.



2. Enter the device email and click **Add**.
3. Enter the device user's email and click **Add**.

   If a call comes in on a CAP located in a conference room around which a number of attendees are sitting and the device is unassociated with any specific user, recording management with Meeting Insights will not be possible. Defining an email address is sufficient to associate the phone with a specific user to make recording management possible.

   Note that Meeting Insights applies speaker detection on the device by using the email addresses of all attendees in the meeting, i.e., the invited users voiceprint, if available, is used for device speaker detection.

11 Configuring User Settings

Admin can configure the following user settings:

- User Profiles
- Admin Profiles
- Licensed Users
- Unlicensed Users
- Recording Notifications
- User Preferences on page 80

User Profiles

Only users assigned with a license are able to access Meeting Insights or record meetings according to their profile. The remaining users who don't have a license but participated in a meeting will not have access to Meeting Insights. Meeting Insights caches their info to present them in the meeting info. To use Meeting Insights, a user must be connected to at least one user profile. Three user profiles are provided with Meeting Insights. Admin can create more.

See also 'Unlicensed Users' page here in which admin can view the info collected and if necessary remove. Users who had a license but were unassigned from their license will also be displayed in this page.

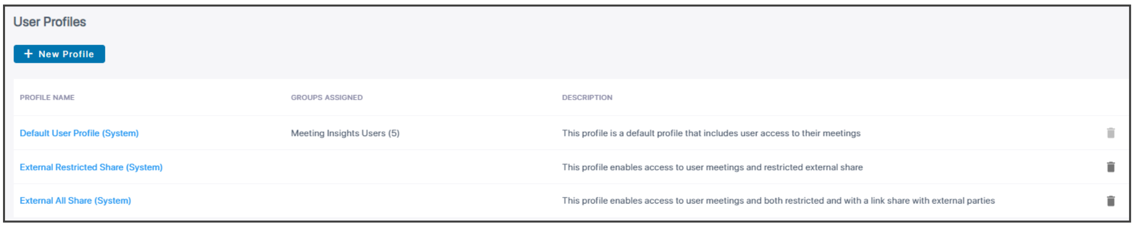
Three profiles are provided:

- **Default User Profile (System)**. This profile is a default profile that includes user access to their meetings.
- **External Restricted Share (System)**. This profile enables access to user meetings and restricted external share.
- **External All Share (System)**. This profile enables access to user meetings and both restricted and with a link share with external parties.

> - You cannot delete a profile while it is assigned to an AAD group. You must assign the group to another profile before you can delete the profile.
> - To assign a User Profile to users, see Assigning a Meeting Insights License to Users on page 22.

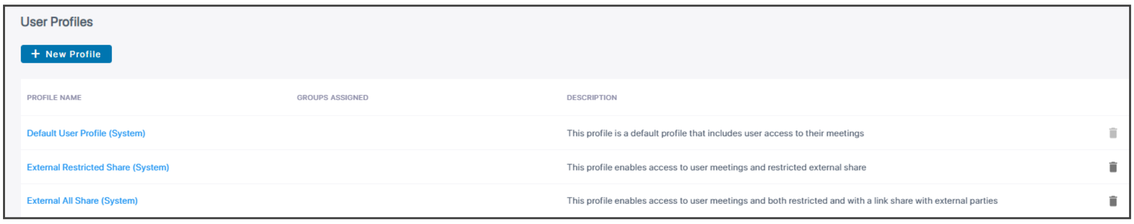
➢ **To configure a user profile:**

1. Under the 'User Settings' menu, click the **User Profiles** option.

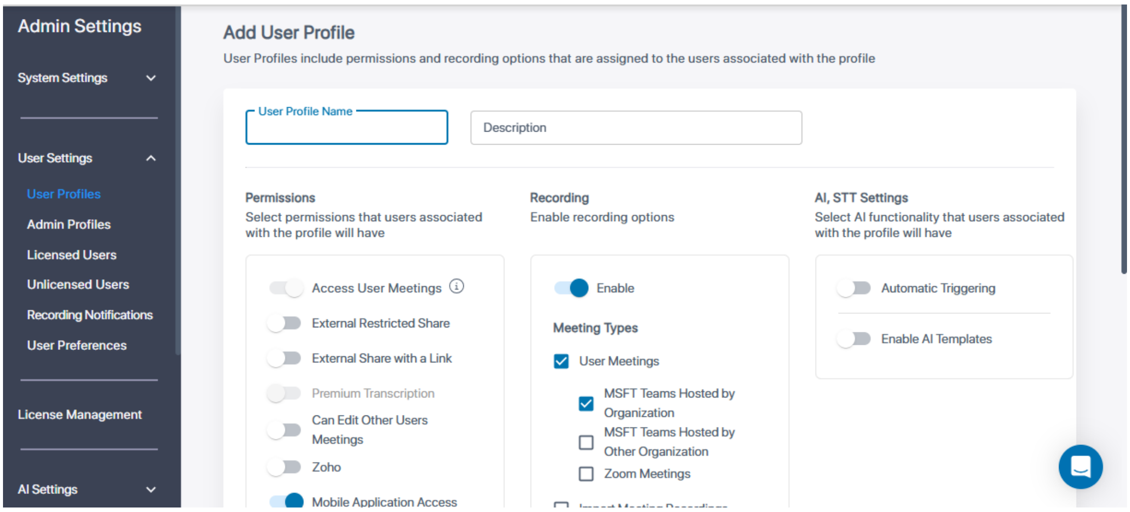


2. View the three default profiles.

- The figure above shows the **Meeting Insights Users (5)** user group assigned with **Default User Profile (System)**, which you did in step 3 when assigning a license shown here.
- The figure below shows no groups assigned. To assign a group to a user profile, see step 3 when assigning a license shown here.



3. Click **New Profile** to add another (customized) user profile to the three that are already available.



4. Configure the fields using the table below as reference.

Field	Description
'User Profile Name'	Enter an intuitive name for effective management later
'Description'	Enter a description of the profile for effective management later
Permissions	

Field	Description
Access User Meetings	Always enabled, this option is used for user access to their meetings. It cannot be disabled. The option is grayed out to indicate that the user always has access to meetings they organized or participated in and to meetings that were shared with them. This option is always enabled and can't disabled.
External Restricted Share	Enable this setting to allow the user to share meeting recordings with external parties who participated in the meetings. To access a meeting recording, external parties will go through their email verification and code access process.
External Share with a Link	Enable this setting to allow sharing the meeting recording with a link; anybody with the link will be able to access the recording.
Premium Transcription	The 'Premium Transcription' option applies only to Hebrew speakers and will mostly be unavailable. It's controllable at the tenant level. Contact your Service Provider if you are interested in this option.
Can Edit Other Users Meetings	People whose 'Auto Can Edit' setting is activated get the 'Can Edit' permission automatically prior to the meeting, i.e., this permission gives them the same level of control of the meeting as the owner, making them a co-owner. They can view, edit, etc. (just like owner of the meeting). It's the same permission that's available when 'Can View' is changed to 'Can Edit' through the meeting side panel or meeting sharing options.
Zoho	Enables Meeting Insights integration with Zoho, allowing users to send their action items to their organization's Zoho platform. **Note:** This option is available only if you have enabled Zoho integration (see Integrating Meeting Insights with Zoho on page 95).
Mobile Applic-ation Access	Enables access and use of Meeting Insights standalone mobile app.
Recording	
Enable	Allows users in the groups assigned to the profile to record the meetings they organize (they must be the meeting organizer).
User Meetings	Enables MIA to record meetings of users assigned to the profile when it's invited to the meeting and the user is the meeting organizer. You can enable this feature on different platforms, by selecting one or more of the following check boxes: ■ **MSFT Teams Hosted by Organization**: (Default) Microsoft Teams

Field	Description
	meetings that are hosted by your organization. ■ **MSFT Teams Hosted by Other Organization**: Microsoft Teams meetings that are hosted by other organizations. For more information, see Enabling Users to Record External Teams Meetings on page 36. ■ **Zoom Meetings**: Zoom meetings that are hosted by your organization or some other organization. For more information, see Enabling Users to Record Zoom Meetings on page 33.
Import Meeting Recordings	Allows the user permission to import meeting recordings created by third-party tools into Meeting Insights.
Recording on Mobile App	Allows users to ad hoc record conversations (by their mobile phone's microphone) when using Meeting Insights standalone mobile app. **Note:** This option is available only if the **Mobile Application Access** toggle button (see above) is turned on.
Select Storage	Meeting Insights stores meeting recording audio, screen sharing content, generated images, transcriptions, and AI insights in separate Azure Blob storage, tailored to regional preferences and hosted in AudioCodes data centers. Customers who need control and ownership of their stored data can add additional Azure Blob Storage accounts for various locations (Bring Your Own Blob Storage or BYOS). Once the BYOS locations are configured, they can be assigned to user profiles, enabling recordings for users assigned to those profiles to be stored in the designated storage. To configure storage accounts, see Storage on page 52.
Meeting Recordings Retention Period	Select how long video meeting recordings are retained (i.e., how many days recordings are kept in storage). If the set limit is exceeded, recordings will be deleted. ■ **Unlimited**- recordings are never deleted and admins must practice caution because the storage location will eventually reach full capacity. ■ **90 Days** ■ **180 Days** ■ **1 Year - Default** ■ **2 Years**(730 days) ■ **3 Years**(1095 days)

Field	Description
	■ **Custom** - enter a specific number of days. **Note:** Once a day, Meeting Insights deletes recordings that exceed the retention period.
Allow Users to Extend Recordings Retention	Allows users to overwrite the retention period (defined above in **Meeting Recordings Retention Period**) by setting the meetings to not be deleted. In this case, the meeting is not deleted as part of the retention period. It can be deleted manually when needed.
AI, STT Settings	
Automatic Triggering	For details on these settings, see Enabling Automatic Triggering of AI below.
Enable AI Templates	For details on these settings, see Enabling Template-based AI-Powered Summaries on page 70.

5. Click **Apply**. You can assign a user group to this user profile as shown here in step 3 (when assigning a license).

Enabling Automatic Triggering of AI

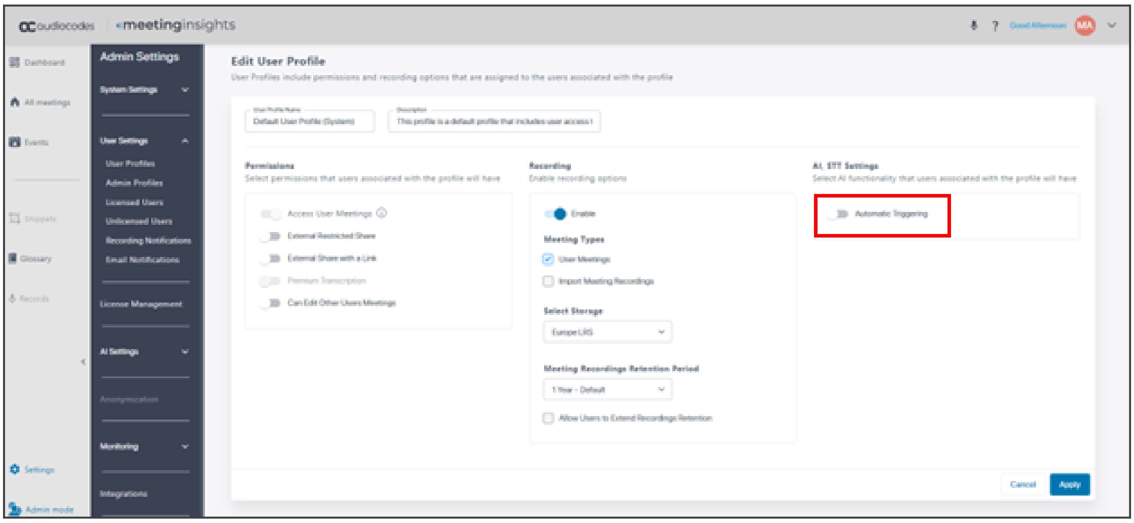
When Automatic AI triggering is enabled, you can control it in the User Profile page.

If your application excludes 'Automatic AI Triggering' and you would like to include the feature, contact your Service Provider.

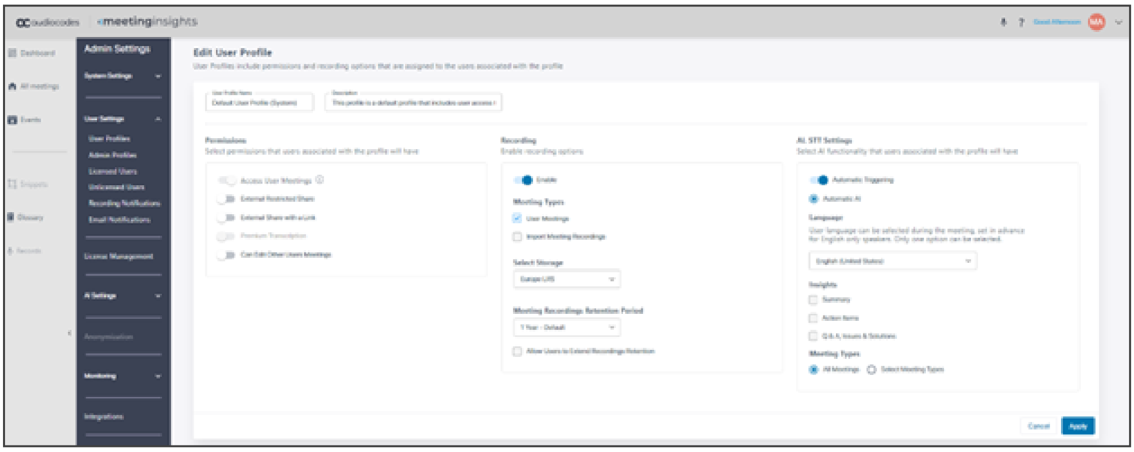
- When automatic triggering is enabled, the user associated with the User Profile automatically gets AI generation of the selected insights.
- AI generation takes place when the meeting ends and may take time (up to half of the meeting's duration).
- For users configured with 'Automatic Publish', Meeting Recap with generated insights is automatically sent out to internal participants of the meeting when generation finishes.

➢ **To enable Automatic AI Triggering:**

1. Open the User Profile page. The figure below shows the Edit User Profile page.



2. [Refer to the previous figure] Enable the 'Automatic Triggering' setting.



> ⚠ When you enable 'Automatic Triggering' in a User Profile, users assigned to the profile will have Automatic AI triggered automatically on their meetings according to the configuration.

3. Optionally select AI Insights to generate automatically. The rest of the available AIs can be generated manually after the meeting ends. Check the insights you want to generate.

4. Configure 'Language'. AI languages can be one of the Speech To Text languages (STT) enabled in your application. The following AI languages are currently supported:

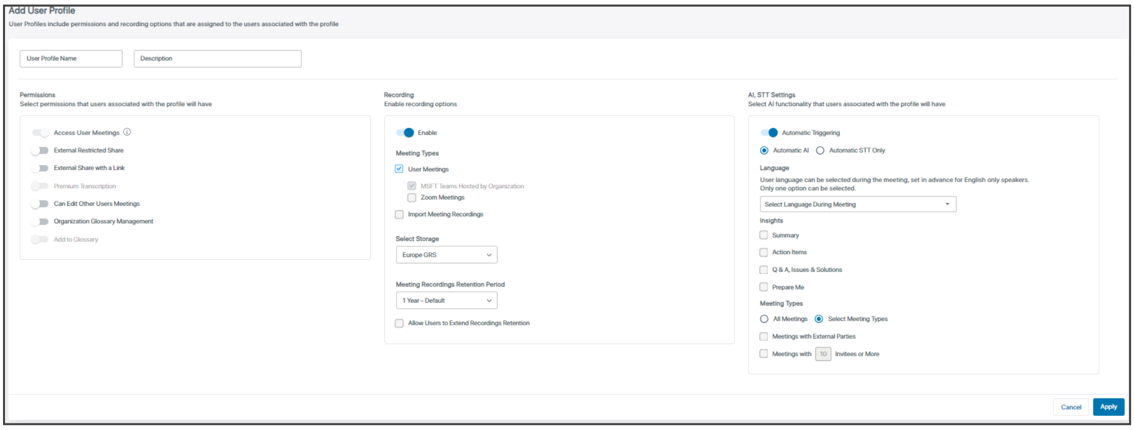
   - English (United States)
   - Hebrew
   - French (France)

5. Select 'Insights':

   - Summary
   - Action Items
   - Q&A Issues & Solutions

6. Select whether to trigger AI on ‘All Meetings’ or ‘Select Meeting Types’. If you select the latter, the following options are available:

   - Meetings with External Parties
   - Meetings with *n* Invitees or More



Enabling Template-based AI-Powered Summaries

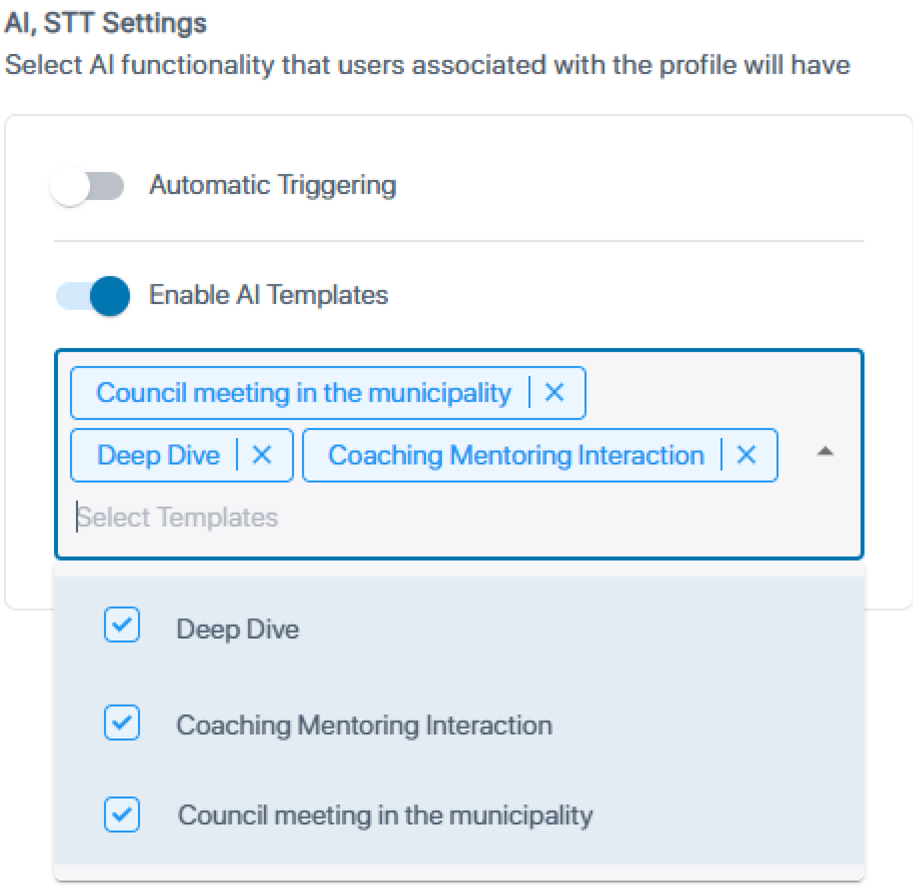
You can enable AI-generated summaries to conform to a custom layout templates. The templates are tailored to the specific needs of your organization, allowing meeting summaries to adhere to a specific format. For example, the organization may want the summary to be categorized using specific terms such as 'Meeting Agenda', 'Main Concerns', and 'Wishful Goal'.

Owners of meeting recordings that are enabled to use templates can run AI-powered summaries based on one or more of the templates. In other words, the Owner can generate multiple summaries of the same meeting recording, where each is based on a different template.

> ⚠ To view a list of available templates, see Viewing and Naming Templates for AI-Powered Summaries on page 86.

➢ To enable template-based AI-powered summaries:

1. In the **Admin Settings** navigation pane, expand **User Settings**, and then click **User Profiles**.
2. Click **New Profile** to add a new User Profile, or select an existing User Profile.
3. Under the **AI, STT Settings** group, do the following:
   a. Click the **Enable AI Templates** toggle button to turn it on.
   b. From the 'Select Templates' drop-down list, select one or more templates:



4. Click **Apply**.

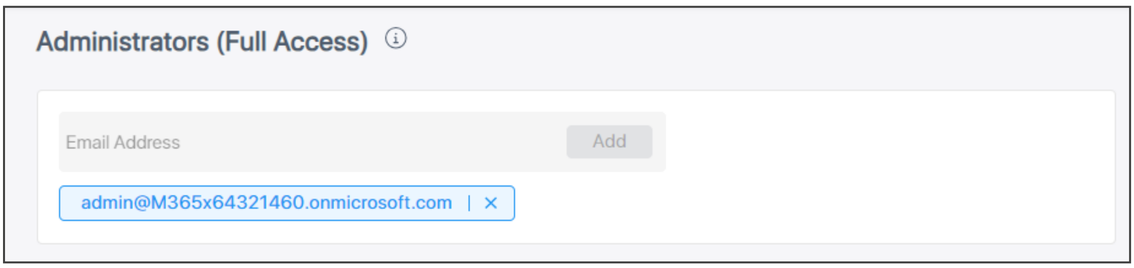
Admin Profiles

You can configure admin profiles.

The number of admins is limited to five by default. If more are needed, you can request your Service Provider.

➢ **To configure an admin profile:**

1. Under the 'User Settings' menu, click the **Admin Profiles** option.



2. Enter the email address of the admin to add and then click **Add**.

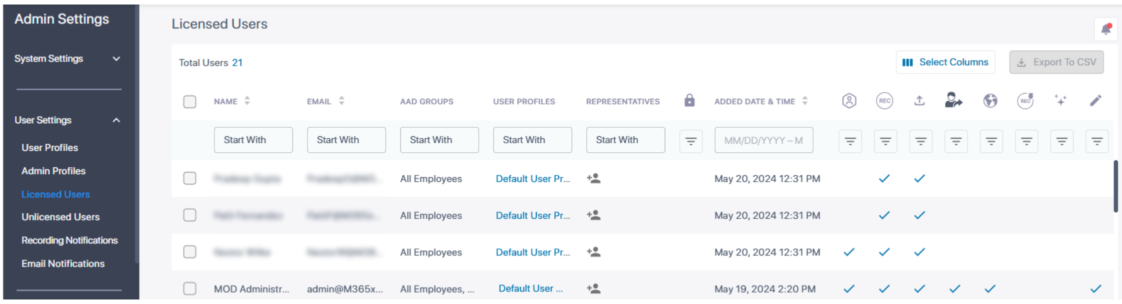
- Added email address(es) are of admins who will be the *default* admins.
- Default admins have full access privileges; they can access all Meeting Insights pages and do and see everything.
- If you lose access or the default admin account is unavailable or deleted, contact the Service Provider to reset the admin account by setting the account you provide.

Licensed Users

The Licensed Users page enables admin to view all licensed users in the system and their permissions. The page also enables admin to assign representatives for users in case a user will need another user to have full access to their recordings. If the employee will leave the company, for example, the assigned representative will have owner access to the departing employee's meeting recordings.

➢ To manage licensed users:

1. Under the ‘User Settings’ menu, click the **Licensed Users** option.

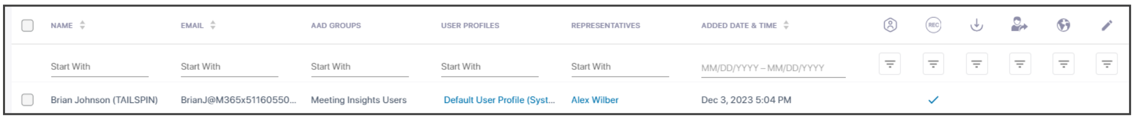


2. Select a single licensed user -OR- select multiple licensed users -OR- check the box next to the NAME column to select *all* licensed users.
3. Point your mouse over a permission icon, e.g., the Admin Permission icon or the Recording Notification icon; a tooltip pops up identifying the icon.
4. Under the permission icon you require, click and from the popup, select **ALL**, **Enabled** or **Disabled**.
5. [Optionally] Add Representatives: Click the icon adjacent to the user to whom to add a representative.

6. Enter in the 'Search' field the name of the user to add as representative.

Only a licensed user can be added as a representative of another user.

7. Check the box and then click **Apply**. The name of the user who you added as representative is displayed in the REPRESENTATIVES column in the Licensed Users page.



8. View the 'lock' icon if it's displayed (not shown in the preceding figures).

- Purpose: The 'lock' icon is a security feature displayed in rare cases involving user account changes within the organization.
- The icon is displayed when a former employee's User Principal Name (UPN) is reused. This can happen if the employee returns to the organization or if the same UPN is assigned to a new employee. When this icon is displayed adjacent to a listed account, if the organization's admin wants to allow that employee (user) access to the meeting recordings of the employee that left, click the icon to unlock them. If you don't want the new employee to have access, open a support ticket with Service Provider's Support to resolve the conflict.
- What the feature does:
  - ✓ When a user with the same UPN is detected, the account is locked.
  - ✓ The lock prevents the new user from accessing old meeting recordings on behalf of the old user.
  - ✓ The lock also stops new recordings and logins for the new account.
- Admin can unlock the user; the user will then have access to the meeting recordings of the old user.

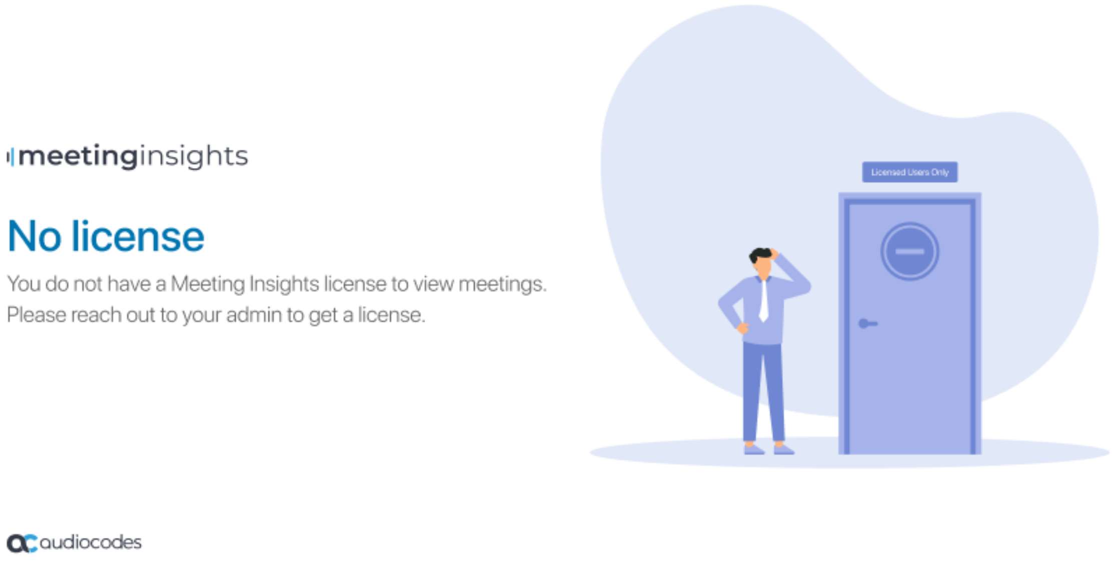
   a. Select the user.

   b. Click the icon.

Unlicensed Users

The Unlicensed Users page enables admin to manage all unlicensed users in the system. Unlicensed users are users who either participated in licensed user meetings and their info such as name and UPN are maintained in the system for presentation as part of the meetings they participated in, or users who had a license before.

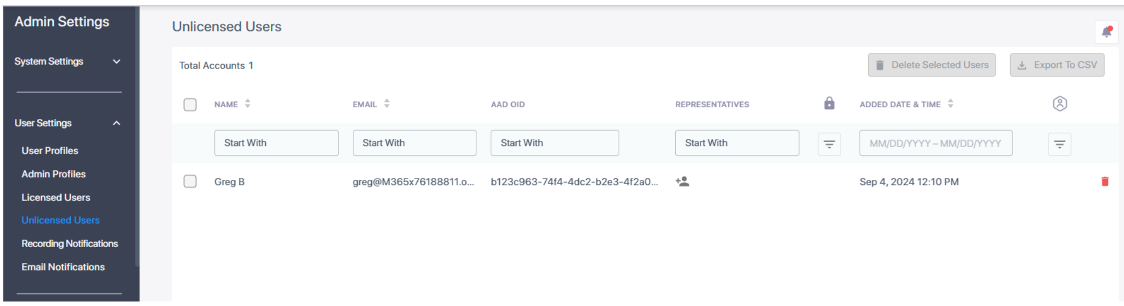
If an unlicensed user receives an email from Meeting Insights about, for example, the recap, when the user clicks the button for accessing the meeting recording, the following message is displayed:



- Admin can delete these users if their info needs to be deleted.
- The user and their info will be added again if they participate in a meeting after it is deleted.
- Deletion of a user from the page doesn't delete their display name from meetings.

➢ To manage unlicensed users:

1. Under the 'User Settings' menu, click the **Unlicensed Users** option.



2. (Optionally) Select all unlicensed users listed in the page by checking the box next to 'Name'; to deselect all, click the same box again.
3. Select a single unlicensed user or select multiple unlicensed users by checking the box next to each entry; the number of unlicensed users you selected is displayed out of the total number of unlicensed users.
4. (Optionally) Filter the page by
   - 'Name': In the **Start With** field under the 'Name' column, enter letters in the name.
   - 'Email': In the **Start With** field under the 'Email' column, enter an email address.
   - 'AAD OID': In the **Start With** field under the 'AAD OID' column, enter the OID of the AAD user.

- 'Representatives': In the **Start With** field under the 'Representatives' column, enter the name of a representative.
- : Filters by **ALL**, **Unlocked** or **Locked** users.
- 'Added Date & Time': Click **MM/DD/YY - MM/DD/YY** and in the calendar that pops up, select the start and end day of a period.

- The lock icon is a security feature displayed in rare cases involving user account changes within the organization.
- The icon is displayed when a former employee's User Principal Name (UPN) is reused. This can happen if the employee returns to the organization or if the same UPN is assigned to a new employee. When this icon is displayed adjacent to a listed account, if the organization's admin wants to allow that employee (user) access to the meeting recordings of the employee that left, click the icon to unlock them. If you don't want the new employee to have access, open a support ticket with Service Provider's Support to resolve the conflict.
- What the feature does:
  - ✓ When a user with the same UPN is detected, the account is locked.
  - ✓ The lock prevents the new user from accessing old meeting recordings on behalf of the old user.
  - ✓ The lock also stops new recordings and logins for the new account.
- Admin can unlock the user; the user will then have access to the meeting recordings of the old user.

Recording Notifications

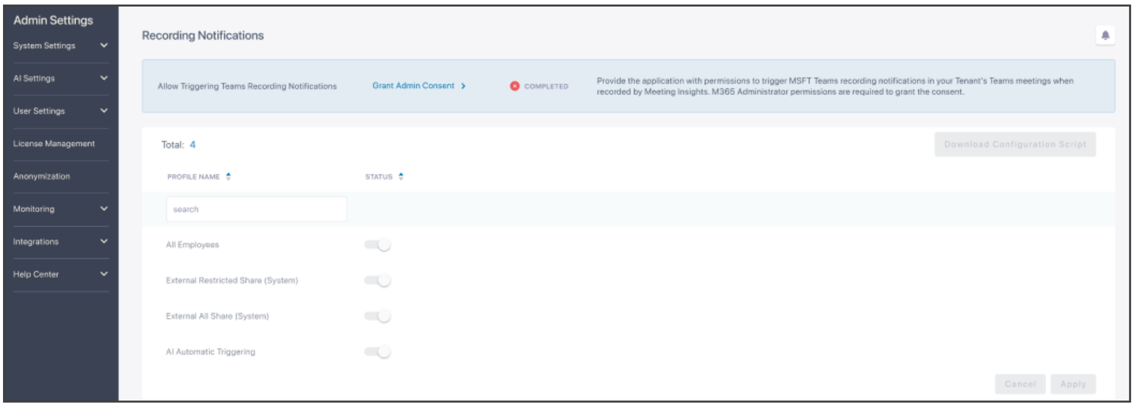
Meeting Insights can trigger Microsoft recording notifications. Admin can configure the feature in the Recording Notifications page.

When a meeting is recorded, Meeting Insights triggers Microsoft to provide audio and visual notifications to meeting participants. Users can't overwrite the configuration. Meeting recording starts only when the owner-organizer joins the meeting. If they leave the meeting, recording is paused; if they rejoin, recording resumes. If the feature is disabled, recording continues regardless of whether they joined, left, or didn't join or leave.

The procedure described in this section for enabling recording notifications involves running a Microsoft script that requires Teams Administrator permissions.

➢ **To trigger recording notifications during meetings when recorded by Meeting Insights:**

1. Under the 'User Settings' menu, click the **Recording Notifications** option.



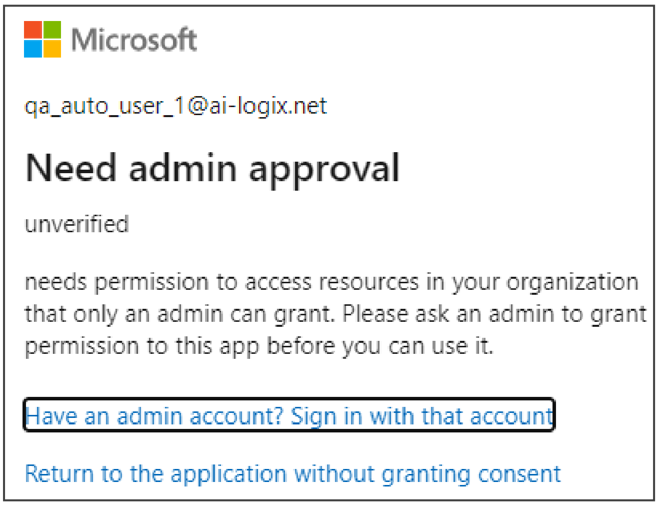
2. Make sure admin has been granted consent to allow Teams recording notifications to be triggered during meetings recorded by Meeting Insights.

   indicates consent has been granted

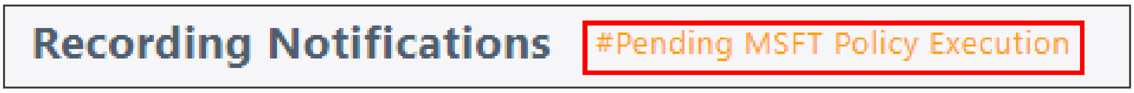
   indicates consent has not been granted yet and must be granted

- If consent has not been granted, the page will be uneditable.
- Recording notifications require the 'Allow Meeting Insights to Be Added to Ongoing Meetings' script to be successfully executed from the 'Connect to M365' page. The script enables the notification bot to access meeting information.

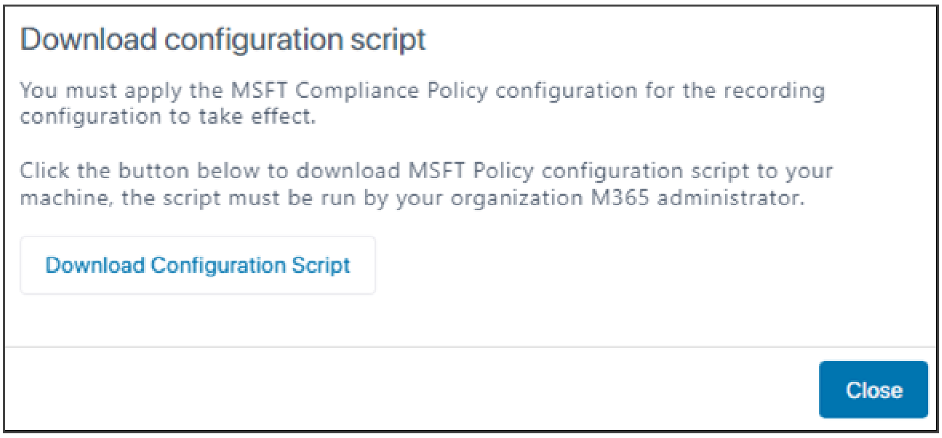
3. Click **Grant Admin Consent >** if consent has not been granted yet.



4. Sign in with your M365 admin account.
5. Enable the User Profile.
   - For example, enable the default user profile **Default User Profile (System)**.
   - All users with this profile will receive recording notifications during meetings they organize.
   - See here for information about how to configure a User Profile.
6. After changing a User Profile, the Recording Notifications page displays this message:

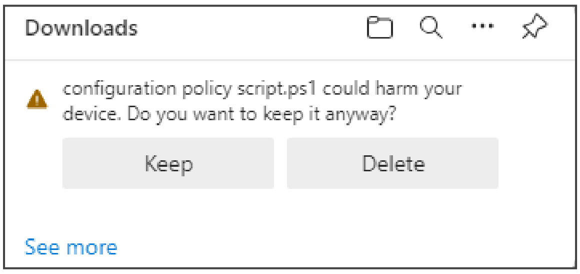


7. Click the **Download Configuration Script** button. The script must be executed by the M365 admin.



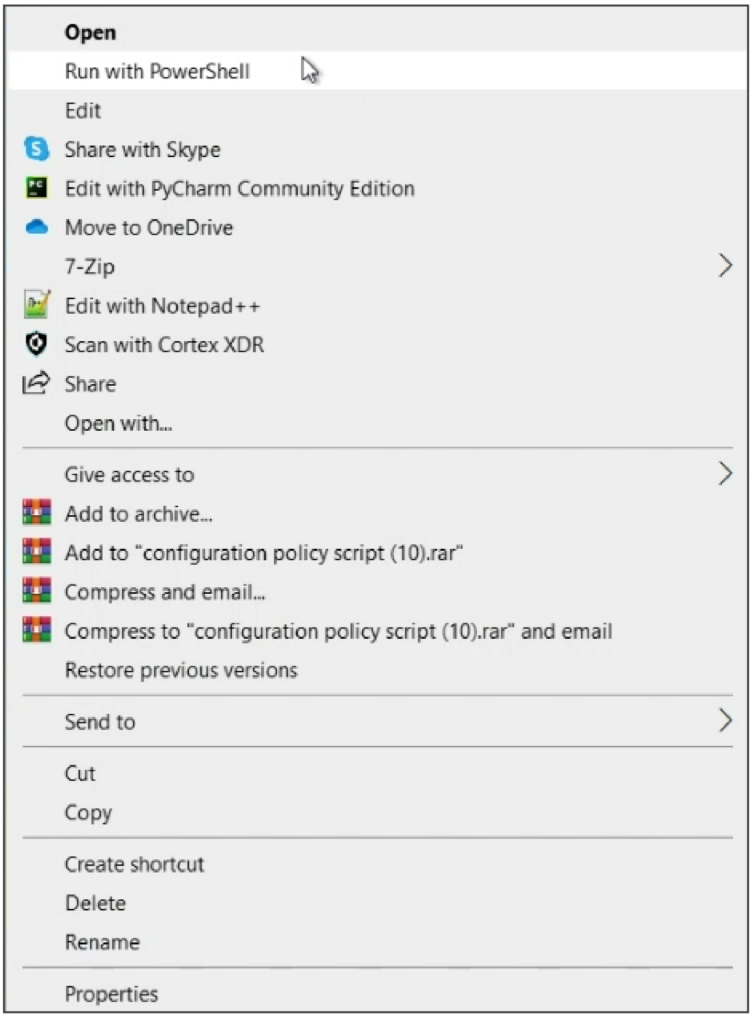
The script must be run to enable recording notifications in Microsoft. It may take time for the Microsoft configuration to take effect. Meetings of the users enabled for recording notifications will not be recorded until the configuration takes effect on the Microsoft side.

8. Click **Download Configuration Script**; the following prompt is displayed:

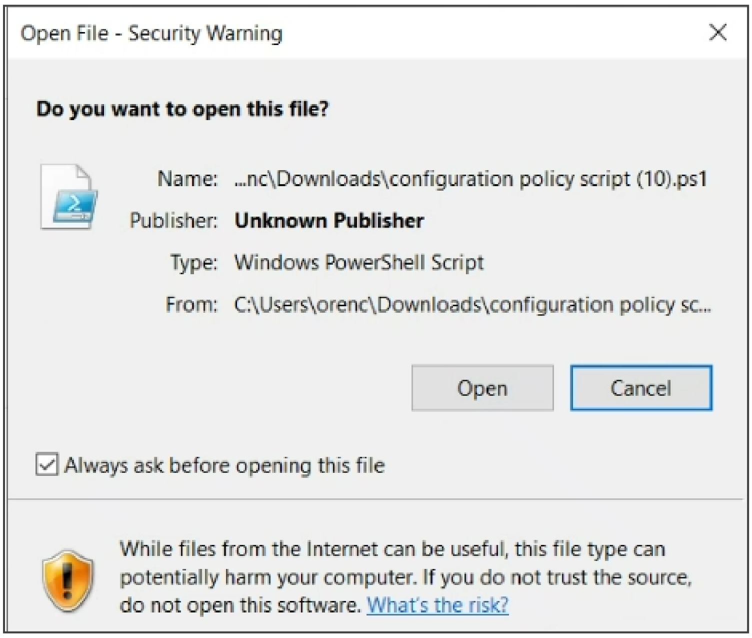


- Only Microsoft Edge displays the 'Keep' prompt.
- Chrome immediately presents the download option.

9. (In Edge) Click **Keep**.
10. (In Chrome) Click the download icon.
11. Right-click the downloaded **policy script.ps1** file.



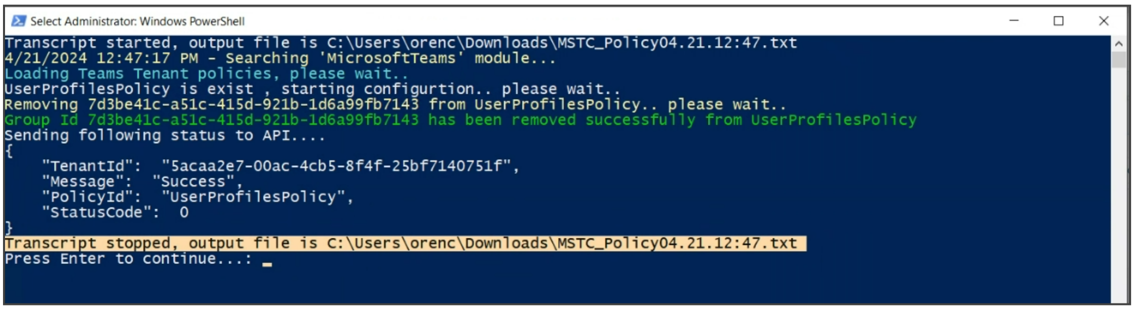
12. Select the option **Run with PowerShell**.



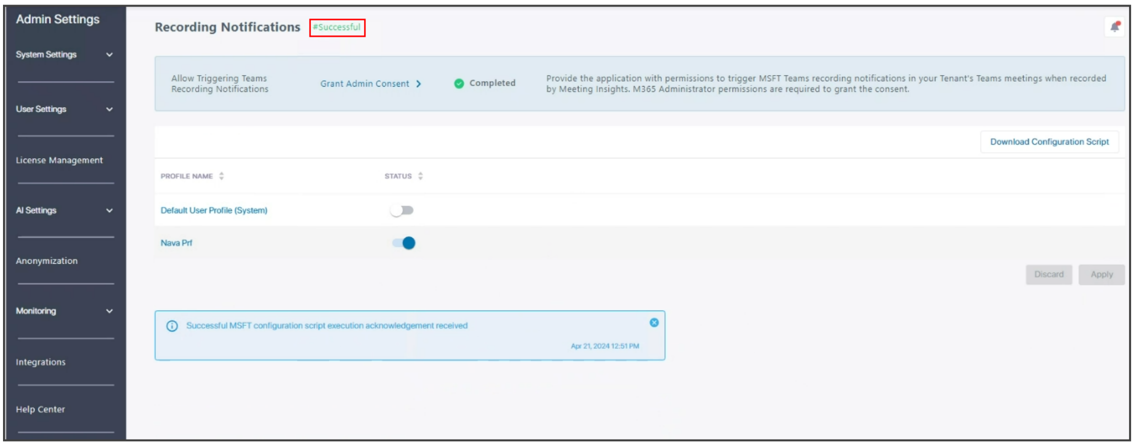
13. Click **Open**.

14. Click **Yes**.

15. In PowerShell, type 'A' and then enter.



16. After the script is run, you'll view the 'Transcript stopped' indication shown in the figure above, and the 'Successful' message shown in the Recording Notifications page in the figure below.



- Enabling users for recording notifications may slow down users' call establishment.
- Removing an AAD group or adding an AAD group to User Profiles that are enabled for recording notification requires downloading and executing the script for the change to take effect.

User Preferences

You can configure the following preferences for users:

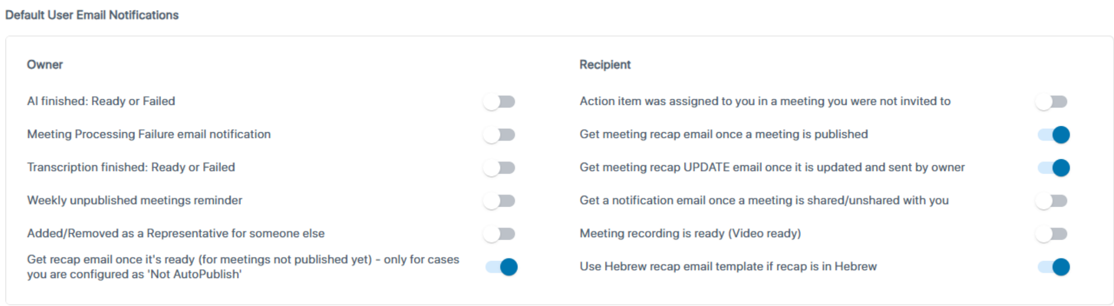
- Email notification preferences - see Email Notifications below
- Publishing time preferences for meeting recordings - see Publishing Time Preferences on page 82

Email Notifications

You can configure Meeting Insights with permissions to enable Microsoft recording notifications for your users during meetings in your Teams' tenant.

➢ **To manage email notifications:**

1. Under the 'User Settings' menu, click the **User Preferences** option. The email notification options are displayed under the **Default User Email Notifications** group:



2. Under **Owner**, configure email notifications for Owners of meeting recordings:

Email Notification	Description
Owner	
AI finished: Ready or Failed	Switch on | off for an email notification be sent | not sent to users, indicating that AI Summarization is finished and that its status is Ready | Failed.
Meeting Processing Failure email notification	Switch on | off for an email notification to be sent | not sent to users indicating that meeting processing failed.

Email Notification	Description
Transcription finished: Ready or Failed	Switch on | off for a notification to be sent | not sent to users indicating that the transcription is finished and that its status is Ready | Failed.
Weekly unpublished meetings reminder	Switch on | off for an email notification to be sent | not sent to users every week, reminding them about their unpublished meetings.
Added/Removed as a Representative for someone else	Switch on | off for a notification to be sent | not sent to users indicating that they've been added | removed as a representative for someone else.
Get recap email once it's ready (for meetings not published yet) - only for cases you are configured as 'Not AutoPublish'	Switch on | off for an email to be sent | not sent to users indicating that a recap is ready (for unpublished meetings). Applies only if users are configured as 'Not AutoPublish'.

3. Under **Recipient**, configure email notifications for participants of meeting recordings:

   a. Click the toggle button corresponding to each email notification type to switch it on or off:

Email Notification	Description
Recipient	
Action item was assigned to you in a meeting you were not invited to	Switch on | off for a notification to be sent | not sent to users after an action item is assigned to them in a meeting to which they were not invited.
Get meeting recap email once a meeting is published	Switch on | off for a notification to be sent | not sent to users indicating the meeting recording has been published.
Get meeting recap UPDATE email once it is updated and sent by owner	Switch on | off for a notification email to be sent | not sent to users indicating that a meeting recap has been updated by the owner.
Get a notification email once a meeting is shared/unshared with you	Switch on | off for a notification email to be sent | not sent to users, indicating a meeting recording has been shared | unshared with them.
Meeting recording is ready (Video ready)	Switch on | off for a notification to be sent | not sent to users indicating that the meeting recording is ready (video ready).
Use Hebrew recap email	Switch on | off for a Hebrew recap email template to be

Email Notification	Description
template if recap is in Hebrew	used if the recap is in Hebrew.

Publishing Time Preferences

Meeting Insights supports the following publishing time options:

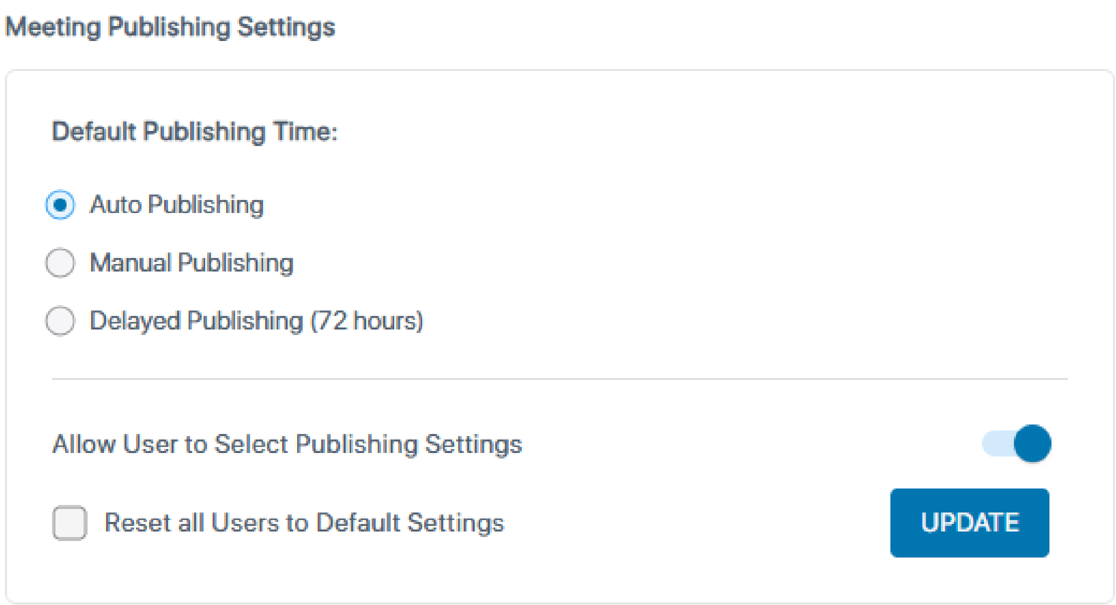
- **Auto Publishing:** (Default) Meeting Insights automatically publishes the meeting recording immediately after it ends.
- **Manual Publishing:** The user needs to manually publish the a meeting recording (by clicking the meeting recording's **Publish** button).
- **Delayed Publishing:** Meeting Insights automatically publishes the meeting recording three days (72 hours) after it has ended.

You can configure preferences for your organization's users regarding publishing of meeting recordings, including the following:

- Selecting one the above publishing options as the default.
- Allowing users to select any of the above publishing options; otherwise, only the default publishing option is available.
- Resetting the currently selected publishing option of each user to the default option.

➢ **To configure publishing preferences:**

1. Under the ‘User Settings’ menu, click the **User Preferences** option; the User Preferences page appears.
2. Scroll down to the **Meeting Publishing Settings** group:



3. Under 'Default Publishing Time', select the default publishing option for your users (**Auto Publishing**, **Manual Publishing**, or **Delayed Publishing (72 hours)**. You can find an explanation of each option in the beginning of this section.
4. To allow users to select any of the publishing options, click the **Allow User To Select Publishing Settings** toggle button to on. If you don't want publishing options available (displayed) to users, but instead want them to use only the default publishing option, then click the toggle button off.
5. If you've allowed users to select a preferred publishing option (see Step 4 - toggle button on), you can force (overwrite) all the users' currently selected publishing option to change to the default publishing option (see Step 3). To enable this, select the 'Reset all Users to Default Settings' check box.
6. Click **Update** to apply your settings.

- If you change the default publishing option and all options are available to users (i.e., **Allow User To Select Publishing Settings** toggle button is on), but the 'Reset all Users to Default Settings' check box is cleared:
  - ✓ For users whose currently selected option was not the previous default option, their selected option is retained (i.e., not changed to default).
  - ✓ For users whose currently selected option was the previous default option, their option is changed to the new default option.
- If you change the default publishing option and all options are available to users (i.e., **Allow User To Select Publishing Settings** toggle button is on), and you've selected the 'Reset all Users to Default Settings' check box, **all** users are forcibly changed to the new default option.
- If you disable users from selecting publishing options (i.e., **Allow User To Select Publishing Settings** toggle button is off), publishing options are not displayed to users and all users have the same publishing option, which is the default.

12 AI Settings

Meeting Insights supports various Artificial Intelligence (AI) features:

- Configuring AI-Powered Transcription below
- Configuring AI-Powered Insights on the next page
- Viewing and Resetting Voiceprints on the next page
- Viewing and Naming Templates for AI-Powered Summaries on page 86

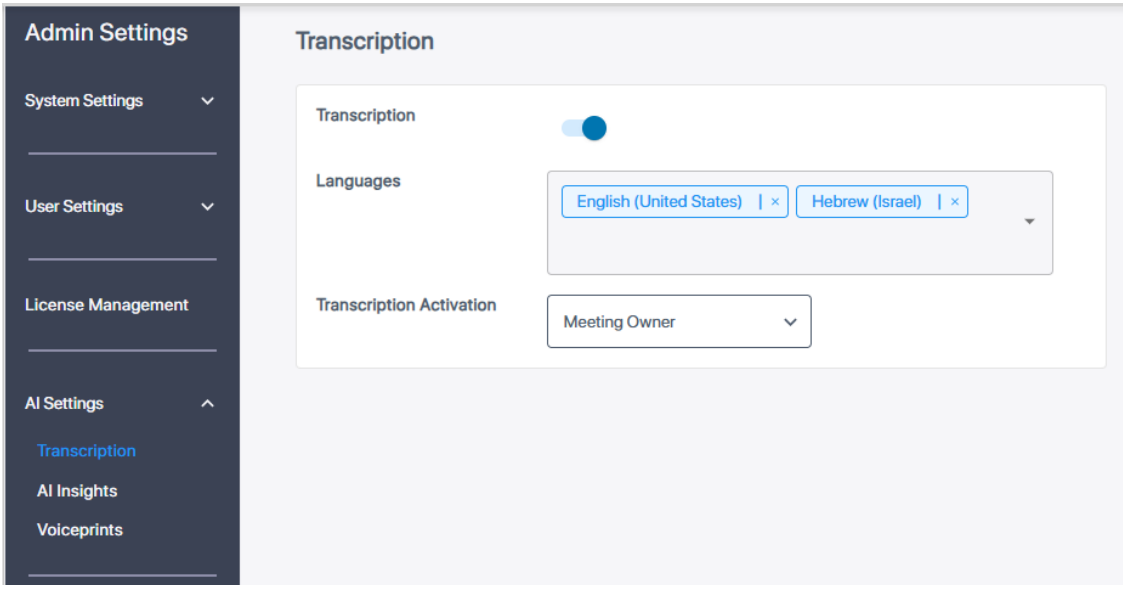
Configuring AI-Powered Transcription

Meeting Insights supports Artificial Intelligence (AI) to convert audio recordings of meetings to textual documentation.

The AI-powered transcription feature is enabled by default.

➢ To configure AI-powered transcription:

1. Under the 'AI Settings' menu, click the **Transcription** option.



2. Click the **Transcription** toggle button to turn on the AI-powered transcription feature.
3. From the 'Transcription Activation' drop-down list, select who can trigger AI-generated transcriptions of meeting recordings:
   - **Meeting Owner** - only the owner or a user with edit permissions.
   - **Anyone** - anyone with access to the meeting recording.

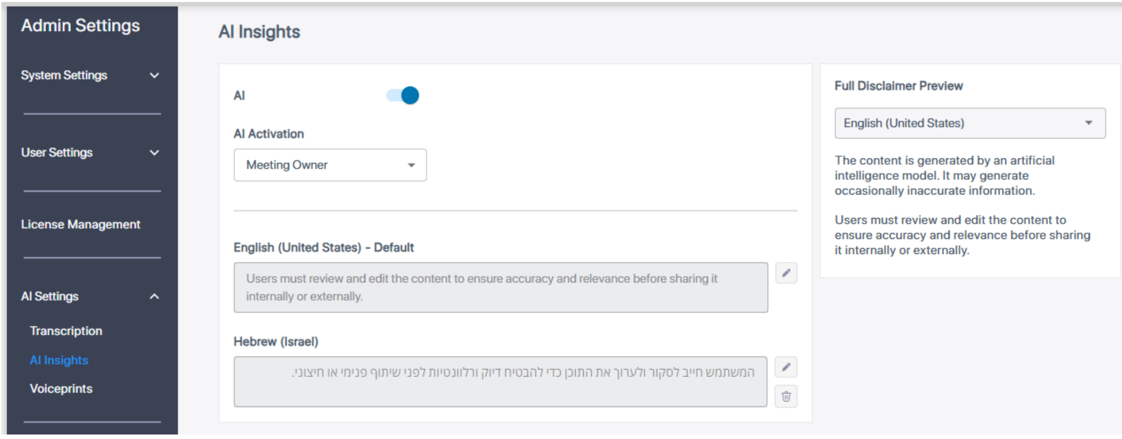
Configuring AI-Powered Insights

Meeting Insights supports AI-powered Insights.

- The AI Insights feature is enabled by default.
- If you disable the AI Insights feature, admin will view the AIs of old meetings but will not be able to trigger new ones.

➢ To configure AI-powered Insights:

1. Under the ‘AI Settings’ menu, select **AI Insights**.



2. Click the **AI** toggle button to turn on the AI-powered Insights feature.
3. From the ‘AI Activation’ drop-down, select who can trigger AI-generated insights of meeting recordings:
   - **Anyone** - anyone with access to the meeting recording (default).
   - **Meeting Owner** - only the owner or a user with edit permissions.
4. To customize the disclaimer:
   a. Click the pencil icon corresponding to the disclaimer language.
   b. Type the disclaimer text, and then click the tick icon.
   c. To view a preview of your disclaimer, from the 'Full Disclaimer Preview' drop-down list, select your disclaimer.

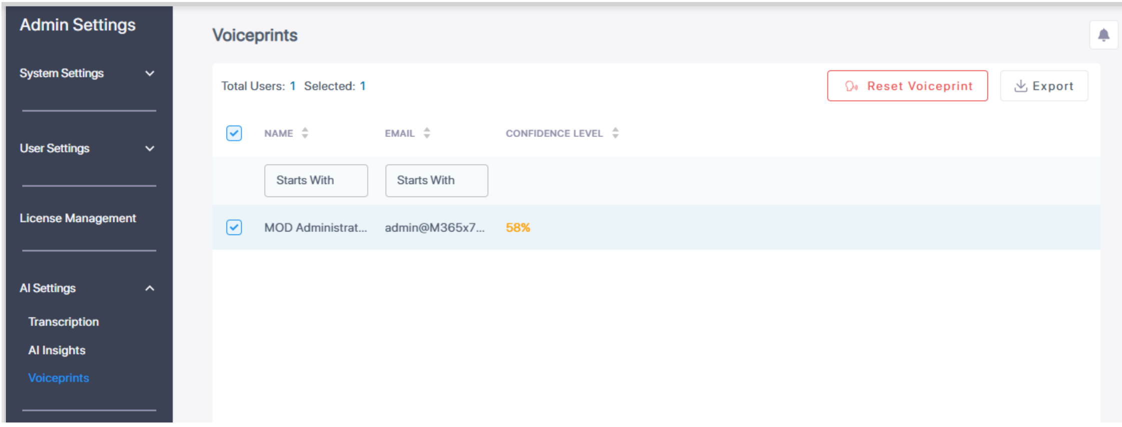
Viewing and Resetting Voiceprints

Admin can view users' voiceprints and their confidence level. Admin can also reset voiceprints.

Voiceprint examiners interpret spectograms using aural and instrumental comparisons of a known voice with an unknown voice. They examine time, frequency and intensity of the sounds captured on the spectograph. Pitch, dialect, resonance, breath patterns and other speech characteristics are registered.

➢ To view users' voiceprints and their confidence level:

1. Open the Voiceprints page (**Admin Settings** > **AI Settings** > **Voiceprints**).



2. View each voiceprint and its (color-coded) confidence level:
   - Red = no voiceprint
   - Yellow = insufficient
   - Green = good

➢ To reset a voiceprint:

1. On the Voiceprints page, select the voiceprint(s) to reset.
2. Click the **Reset Voiceprint** button; a confirmation message appears.
3. Click **RESET** to confirm.

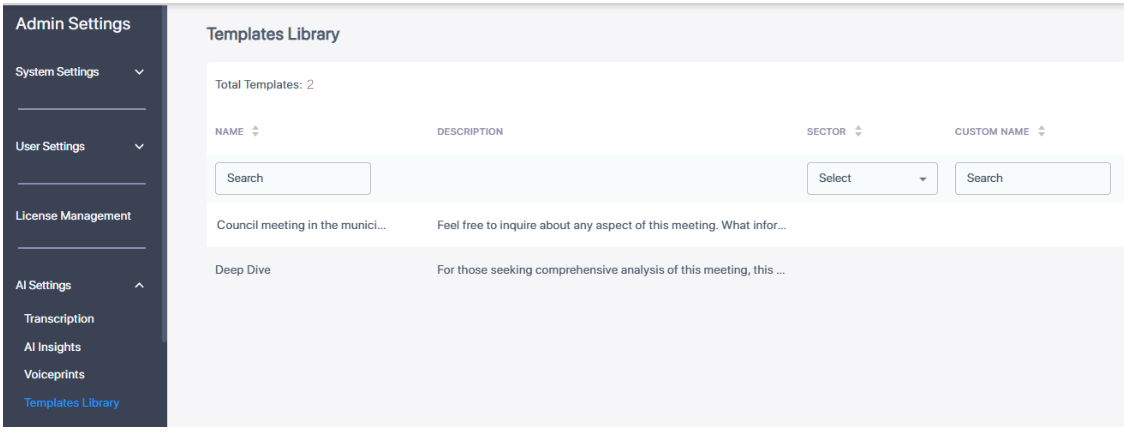
Viewing and Naming Templates for AI-Powered Summaries

You can view a list of all uploaded templates. Additionally, you can configure a 'Custom Name' for each template, which is displayed to end users in Meeting Insights. This name should be clear and user-friendly, making it easy for users to recognize and identify the template.

- The template 'Name' is only for the administrator, but is displayed to end users if you don't configure a 'Custom Name'.
- The template 'Custom Name' must be unique.
- To enable template-based AI-powered summaries per User Profile, see Enabling Template-based AI-Powered Summaries on page 70.

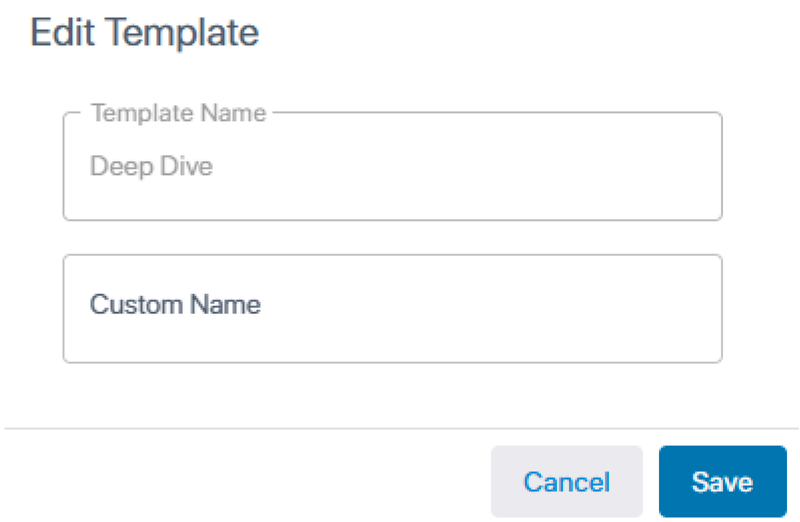
➢ To view templates or change custom name:

1. In the **Admin Settings** navigation pane, expand **AI Settings**, and then click **Templates Library**; a list of the installed templates are displayed:



2. To configure a name for the template:

   a. Click the icon corresponding to the required template; the following dialog box appears:



   b. In the 'Custom Name' field, type a name for the template.

   c. Click **Save**.

13 Monitoring

Two menu options are available:

- Audit Trail
- System Activity Log

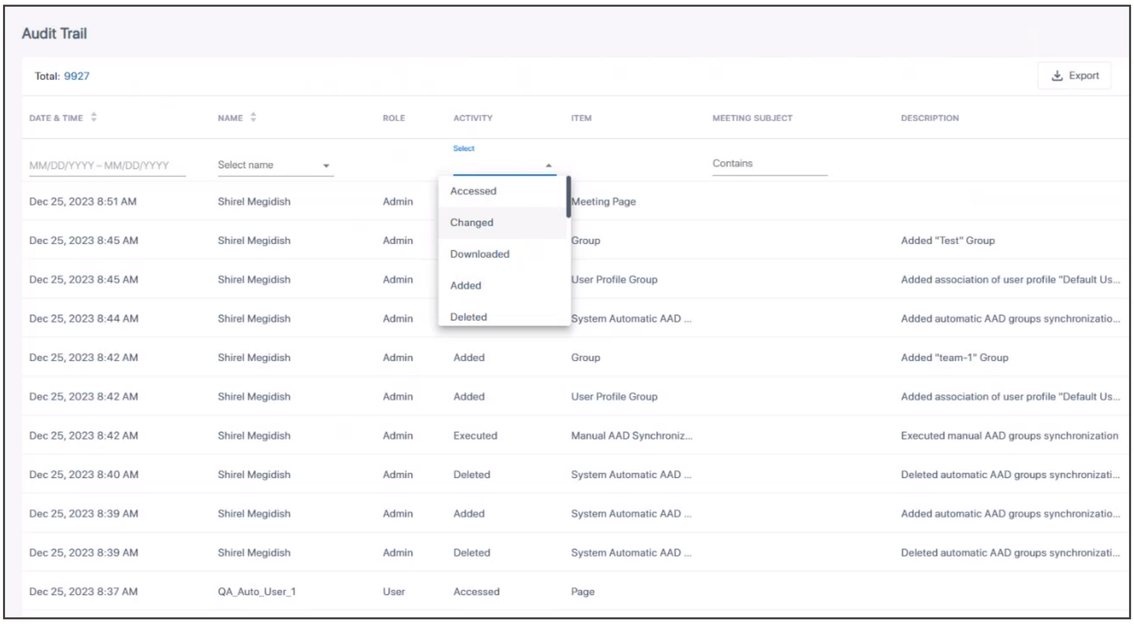
Audit Trail

Meeting Insights features an 'Audit Trail' which logs for future reference admin and user activities performed in Meeting Insights.

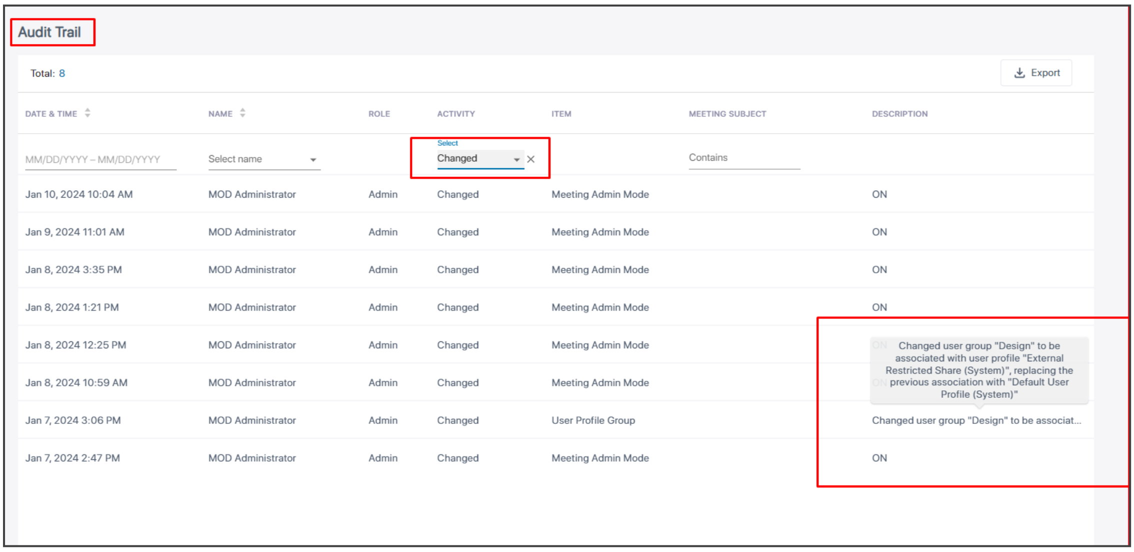
> Meeting Insights retains audit logs (audit trail) for a period of 1 year.

➢ To monitor audit trail:

1. Under the 'Monitoring' menu, click the **Audit Trail** option.



2. [Optionally] Select an Activity filter in order to filter the page by an action users perform in the system (Accessed, Changed, Downloaded, Added, Deleted, etc.). Other filters can also be selected to exclude more unwanted information from the page for more effective management. After the user profile of a user group is changed, for example, the Audit Trail page's **Activity** filter enables you to determine details such as at what time the change was made, who made it, which user group's user profile was changed, and from what profile to what profile.



- All logins / logouts of all users are recorded.
- The activity **Deleted** is also associated with the item of **Meeting deletion**, so if you select this activity, this item will also be displayed.
- The activity **Downloaded** is associated with items such as **Meeting Downloaded** or **Recap downloaded**.
- There are no items associated with the activity **Accessed**; the activity implies generic access to content, or else the item indicates Meeting and the subject of the meeting.
- Items associated with the activity **Added** | **Deleted** | **Changed** are (for example) Participant | ActionItem | Highlight | EditPermissions | External share, etc.; these items will be displayed if you select this activity.

3. [Optionally] Select a Date filter. Click the calendar icon and from the popup calendar select a month | day | year; only activities that took place on this date will be displayed in the page (activities that did not take place on this date will be excluded).
4. [Optionally] Select a Meeting Subject filter. Enter the subject of the meeting; only activities associated with meetings whose subject line matches the text you entered will be displayed (activities associated with meetings whose subject line does not match the text will be excluded).
5. [Optionally] Select a Name filter. Click the drop-down arrow and in the 'Search' field displayed, specify the name of a user; only entries related to that user will be displayed.

More than one filter can be applied: Activity, Date, Meeting Subject and/or Name.

6. Click the **Export to CSV** option to export the Audit Trail in CSV format that you can easily share with others.

System Activity Log

The System Activity Log page enables admin to view system activities that occur either following admin operations (license added due to admin mapping of groups or adding users), or automatically, such as when:

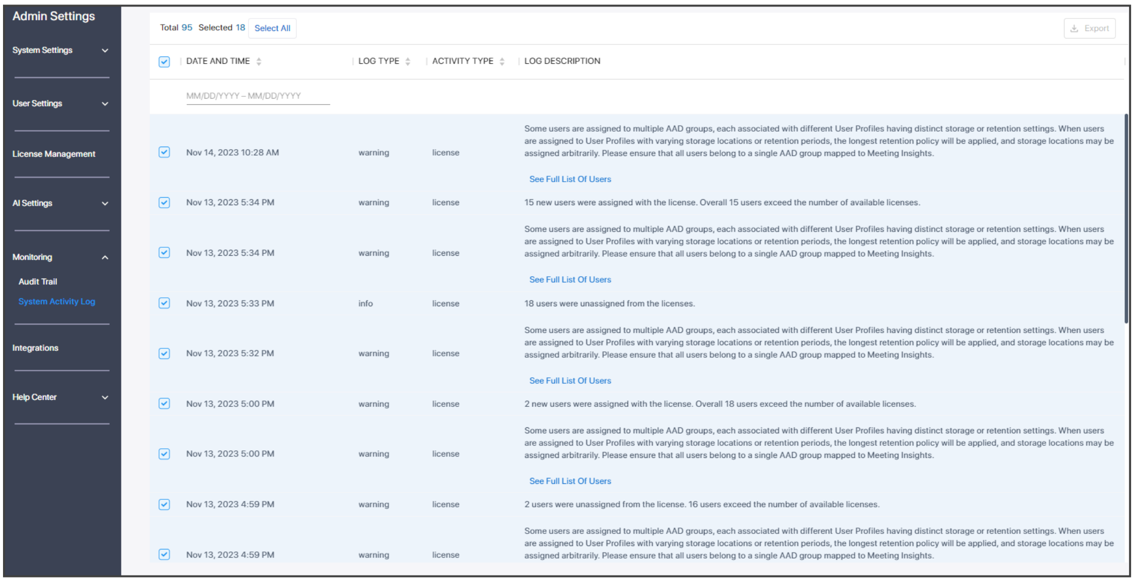
- A new user is added via automatic synchronization from AAD to a user group
- A new user group is added via automatic synchronization from AAD to Meeting Insights.

Logged activities can be filtered by date and time so that system activities which occurred outside that date | time are excluded from display.

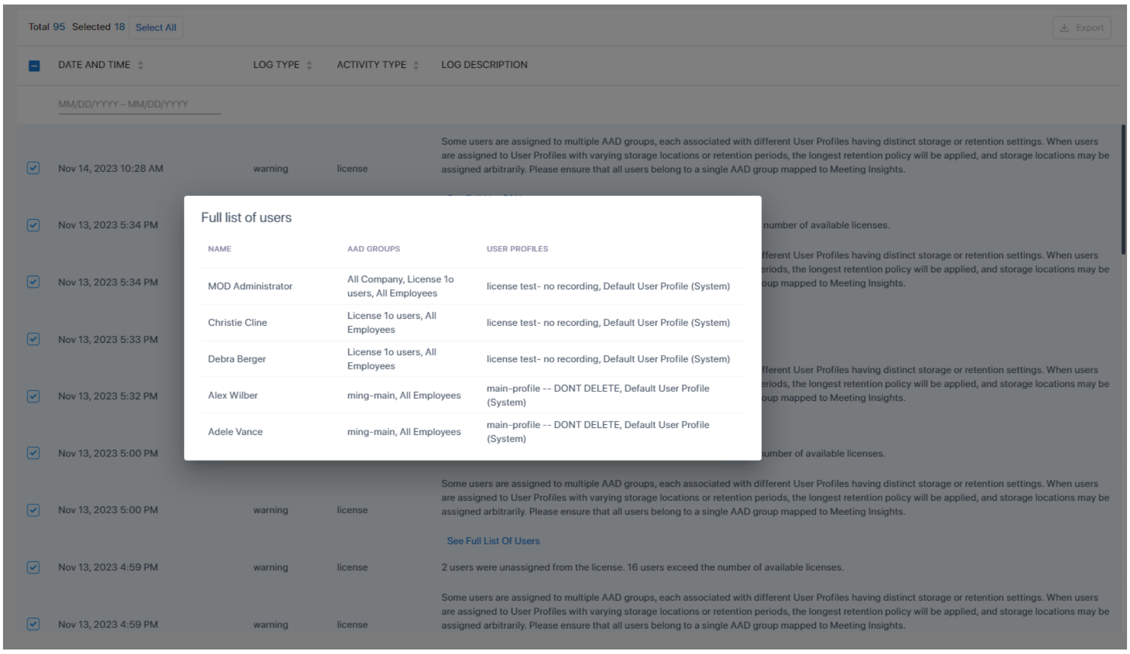
Meeting Insights retains system activity logs for a period of 6 months.

➢ To filter System Activity Log:

1. Under the 'Monitoring' menu, click the **System Activity Log** option.



2. (Optionally) Select all logs by checking the box next to 'Date and Time'; to deselect all, click the same box again.
3. Select a single log or select multiple logs by checking the box next to each log entry; the number of logs you selected is displayed out of the total number of logs available.
4. (Optionally) Filter the page by 'Date and Time', 'Log Type' or 'Activity Type' column; click the column header.
5. (Optionally) Filter the page by period: Click **MM/DD/YY - MM/DD/YY** and in the calendar that pops up, select the start day and the end day.
6. Under the 'Log Description' column, click the **See Full List Of Users** link in the row of a log.



7. In a log, view for example how many times users were added or removed from a license (the count).

8. (Optionally) Click the **Export** button in the uppermost right corner of the page and in the format prompt, click the **Export to Excel** button.

14 Integrations

You can integrate the following third-party applications with Meeting Insights:

- Microsoft Planner - see Integrating Meeting Insights with Microsoft Planner below
- Salesforce customer relationship management (CRM) platform - see Integrating Meeting Insights with Salesforce on page 97

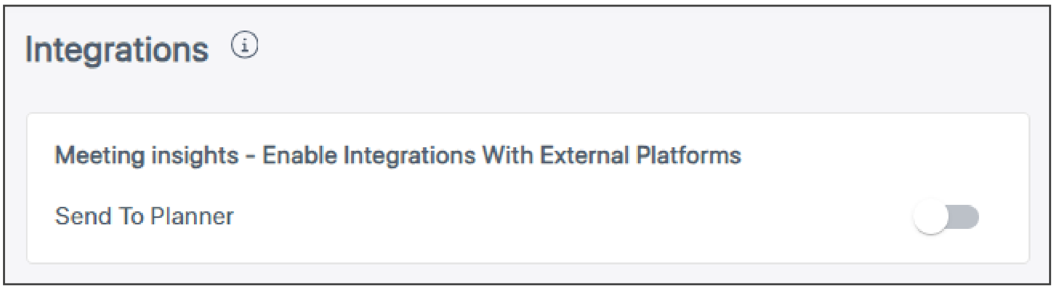
Integrating Meeting Insights with Microsoft Planner

The instructions here show how to integrate Microsoft Planner with Meeting Insights.

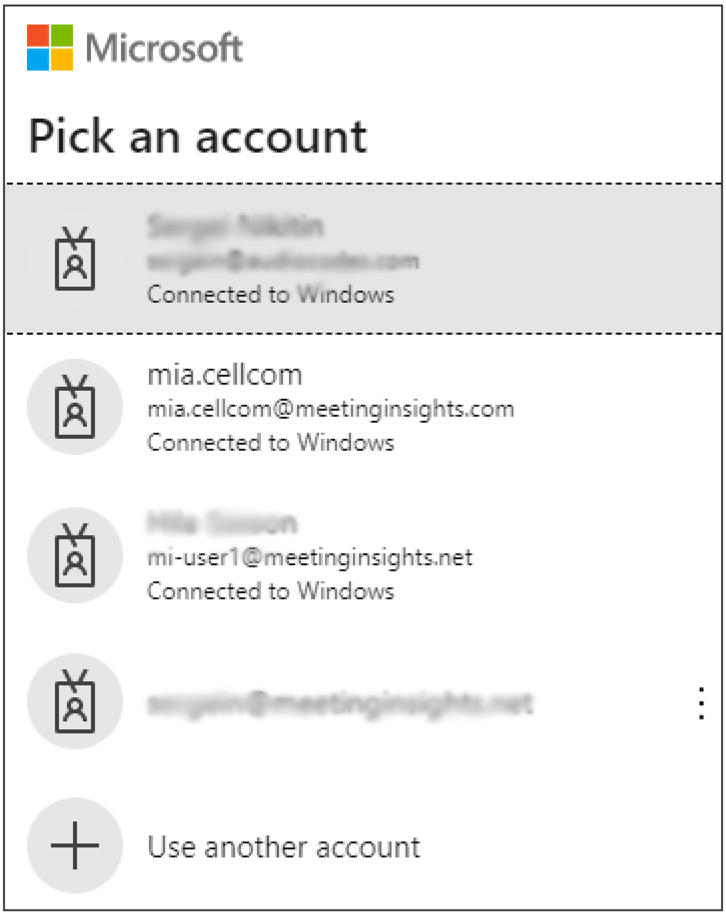
> Before integrating Microsoft Planner, the logged-in user must have Meeting Insights 'admin' privileges and Azure 'tenant admin' privileges.

➢ To integrate Microsoft Planner:

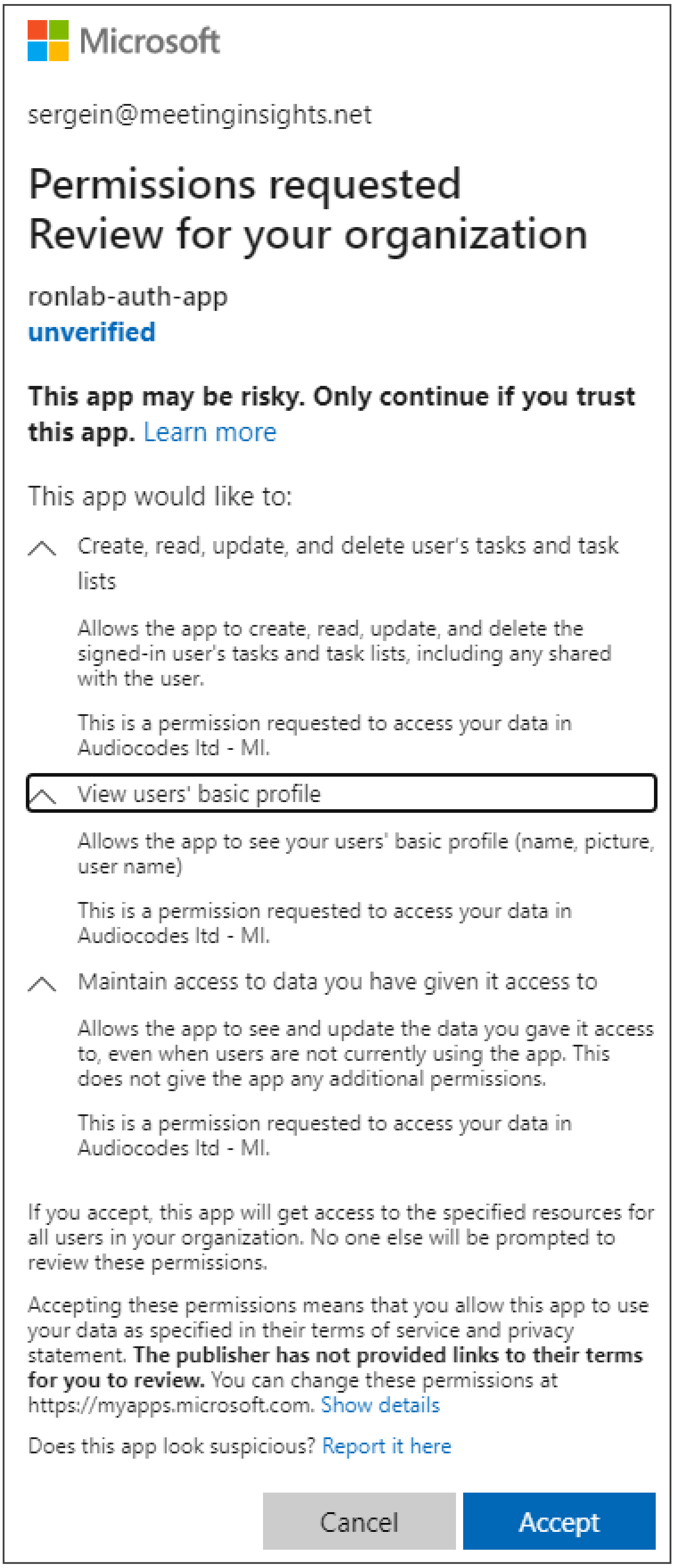
1. Under the ‘Settings’ menu, click the **Integrations** option.



2. Enable the **Send to Planner** setting; you will be redirected to the following Microsoft admin login prompt:



3. Pick an account.

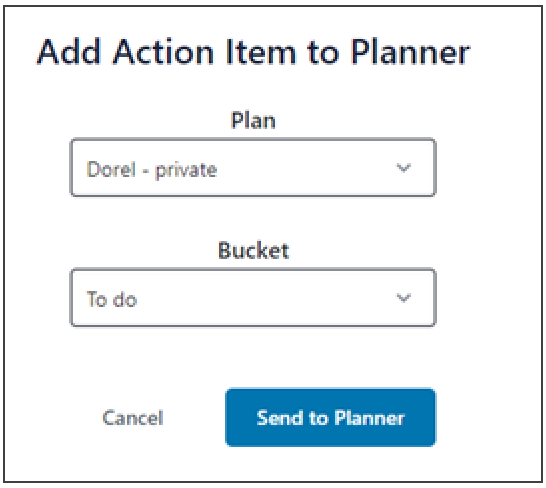

Microsoft
sergein@meetinginsights.net
Permissions requested
Review for your organization
ronlab-auth-app
unverified
This app may be risky. Only continue if you trust this app. Learn more
This app would like to:
Create, read, update, and delete user's tasks and task lists
Allows the app to create, read, update, and delete the signed-in user's tasks and task lists, including any shared with the user.
This is a permission requested to access your data in Audiocodes ltd - MI.
View users' basic profile
Allows the app to see your users' basic profile (name, picture, user name)
This is a permission requested to access your data in Audiocodes ltd - MI.
Maintain access to data you have given it access to
Allows the app to see and update the data you gave it access to, even when users are not currently using the app. This does not give the app any additional permissions.
This is a permission requested to access your data in Audiocodes ltd - MI.
If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.
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
Cancel
Accept

4. Click **Accept**; you're giving the app permission to create, read, update, and delete the signed-in user's tasks and task lists, as indicated in the prompt; you'll be redirected back to the 'Settings' page; click the **Integrations** tab to make sure it's enabled.

5. Use the following example of the user sending an action item to Microsoft Planner (during a live meeting) as a reference:

6. Click the **Action Items** menu.

7. Choose a plan and a bucket, and then click **Send to Planner**.



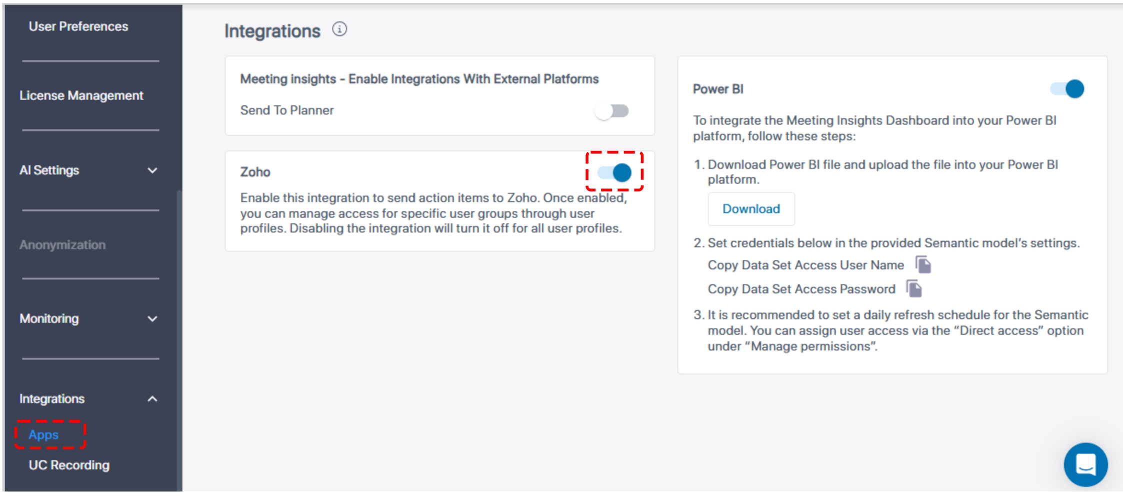
Integrating Meeting Insights with Zoho

To integrate Meeting Insights with Zoho so that users (per User Profile) can send their action items to their Zoho account's Task List within a Project, you first need to enable the integration.

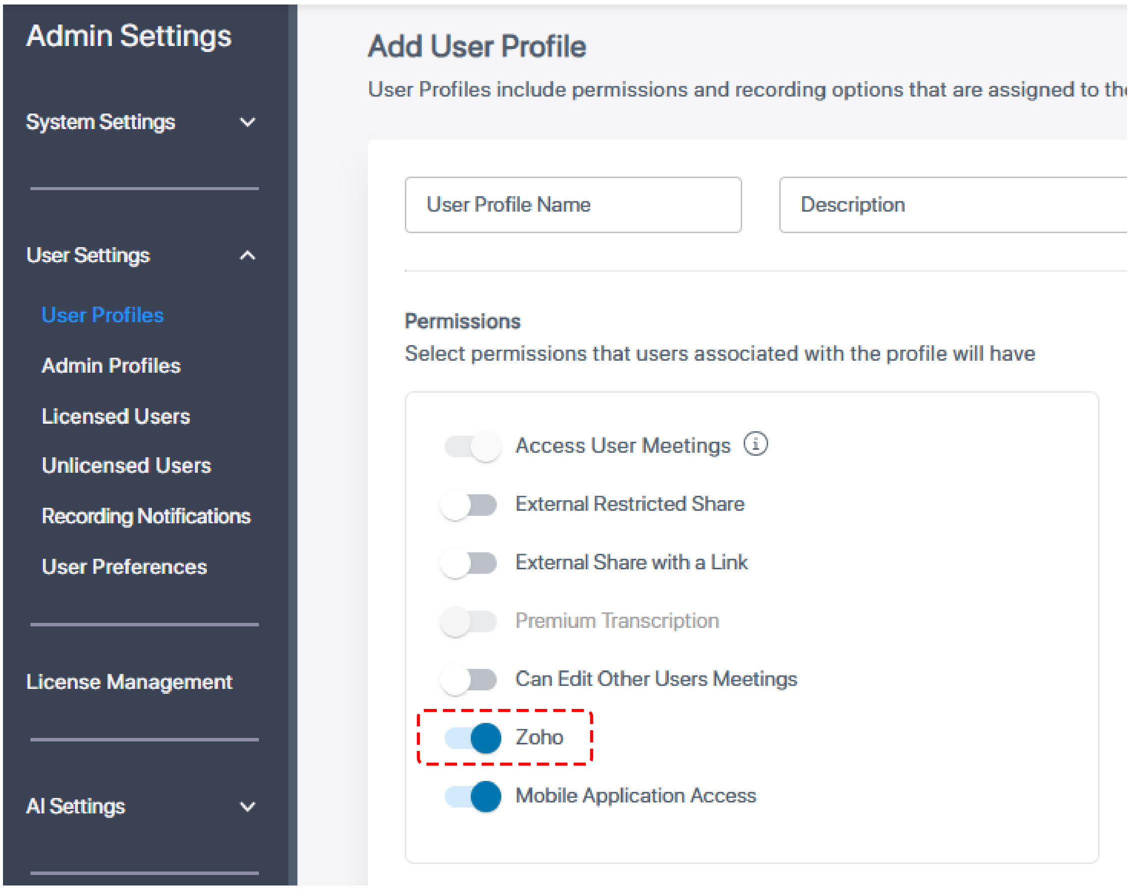
➢ **To enable Zoho integration:**

1. In the Admin Settings navigation pane, expand **Integrations**, and then click **Apps**.

2. Click the **Zoho** toggle switch to turn on integration:



3. Enable Zoho for specific User Profiles (see User Profiles on page 64):
    a. In the Admin Settings navigation pane, expand **User Settings**, and then click **User Profiles**.
    b. Add a new User Profile or edit an existing one.
    c. Under the Permissions group, click the **Zoho** toggle button to turn it on:



4. Click **Apply**.

Integrating Meeting Insights with Salesforce

You can leverage the power of AI-generated meeting summaries by integrating Meeting Insights with your organization's Salesforce platform. This integration allows users to send summaries to specific Salesforce objects, such as the Account object, populating designated fields like 'ACompany'. This ensures key discussion points from sales meetings are readily accessible within Salesforce, opportunities are kept up-to-date, and sales efficiency is improved.

- Only AI-powered bullet-summaries are sent to Salesforce.
- Only the following Salesforce objects are supported:
  - ✓ Account
  - ✓ Opportunity
- When Meeting Insights updates a Salesforce object field with the AI-powered summary, it adds the new content to any existing content.
- Disabling Salesforce integration deletes all associated data and settings of the tenant.

Integration includes the following main steps:

- Setting up Salesforce and obtaining required information for Meeting Insights (see Setting Up Salesforce and Obtaining Required Information below).
- Configuring Meeting Insights for integrating with your Salesforce platform (see Configuring Meeting Insights for Salesforce Integration on page 102).

Setting Up Salesforce and Obtaining Required Information

Before you can configure Meeting Insights to integrate with your organization's Salesforce platform, you need to do the following in Salesforce:

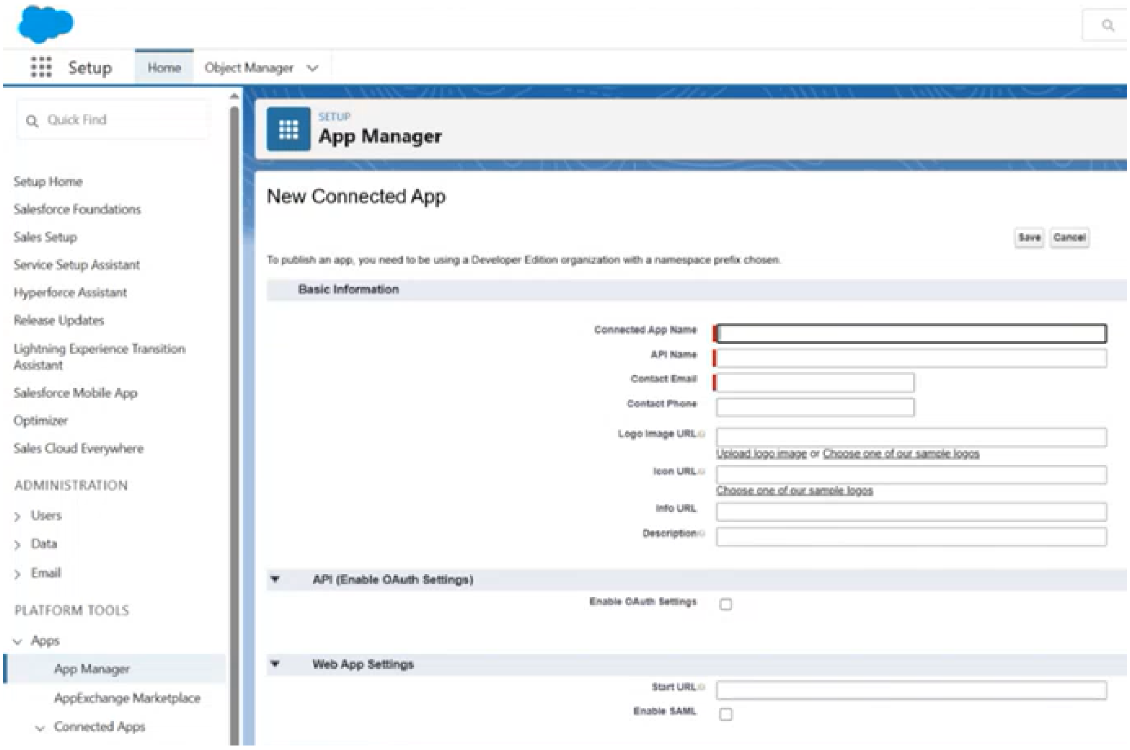
1. Create a Connected App for integration with Meeting Insights - see Creating a Connected App in Salesforce below.
2. Obtain the following information for Meeting Insights:
   - Salesforce domain URL - Obtaining the Salesforce Domain URL on page 99.
   - Connected App client ID and client secret key - Obtaining Client ID and Secret of Salesforce Connected App on page 100.
   - Field (API) names of the Account and Opportunity Salesforce objects where Meeting Insights can send AI-powered meeting summaries - Obtaining Salesforce Object Field (API) Names on page 101.

Creating a Connected App in Salesforce

A connected app is a framework that enables an external application (i.e., Meeting Insights) to integrate with Salesforce using APIs and standard protocols.

➢ To create a connected app:

1. Sign in to your Salesforce account.
2. Click the gear ⚙ icon in the top-right corner, and then choose **Setup**.
3. In the left navigation menu, expand **Apps**, and then choose **App Manager**.
4. Click the **New Connected App** button; a dialog box appears.
5. Select **Create a Connected App**, and then click **Continue**; the New Connected App page appears:



6. Under the **Basic Information** group, configure the following:
   - In the 'Connected App Name' field, type a name for the connected app.
   - In the 'Contact Email' field, type the email of the contact person for this integration.
7. Under the **API (Enable OAuth Settings)** group, configure the following:
   a. Select the 'Enable OAuth Settings' check box.
   b. In the 'Callback URL' field, enter all these URLs or the URL according to your region:
      - **EMEA:** https://emea.meetinginsights.com/mi/redirect/salesforce
      - **Australia:** https://au.meetinginsights.com/mi/redirect/salesforce
      - **Americas:** https://americas.meetinginsights.com/mi/redirect/salesforce
   c. For **Selected OAuth Scopes**, select the following scopes from the **Available OAuth Scopes** list:
      - **Full access (full)**

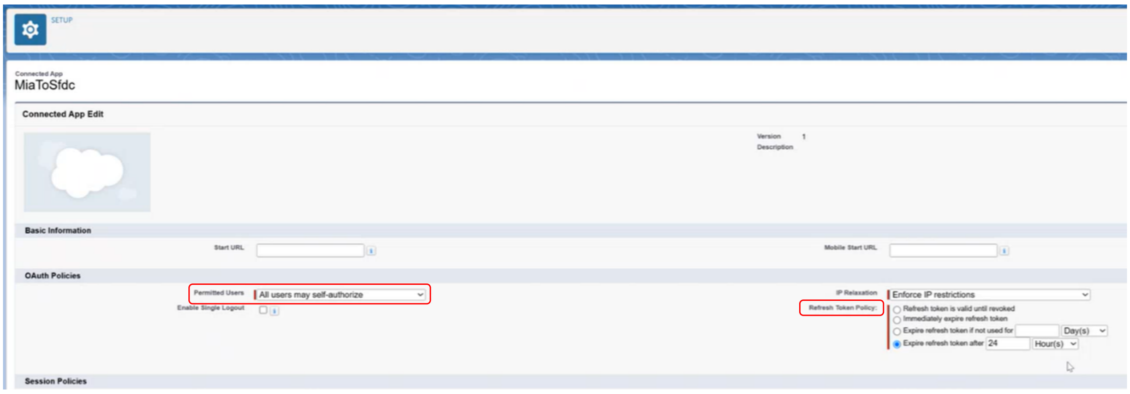
- **Manage user data via APIs (api)**
- **Perform requests at any time (refresh_token, offline_access)**

d. Select the 'Enable Client Credentials Flow' check box.

8. Click **Save**; the connected app is created and is now listed in the App Manager list.
9. In the App Manager list, click the down-pointing arrow corresponding to the new connected app, and then from the drop-down menu, choose **Manage**.
10. Click the **Edit Policies** button, and then configure the following:

a. From the 'Permitted Users' drop-down list, select **All users may self-authorize**.

b. For 'Refresh Token Policy' it's recommended to select **Expire refresh token after 24 Hour(s)**. This means that once the user logs into Salesforce from Meeting Insights, the user only needs to log in again after 24 hours.



11. Click **Save**.

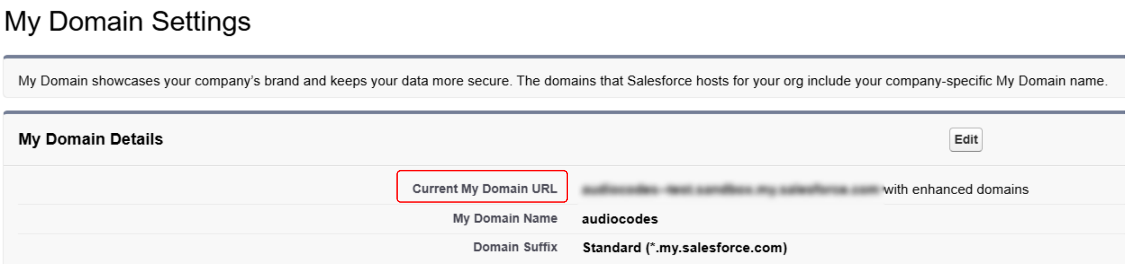
Obtaining the Salesforce Domain URL

The following procedure describes how to obtain your organization's Salesforce domain URL, which you need for configuring Meeting Insights.

➢ To obtain client ID and secret:

1. Sign in to your Salesforce account.
2. Click the gear ⚙ icon in the top-right corner, and then choose **Setup**.
3. In the left navigation menu, expand **Company Settings**, and then choose **My Domain**.

The domain URL is displayed in the 'Current My Domain URL' field:

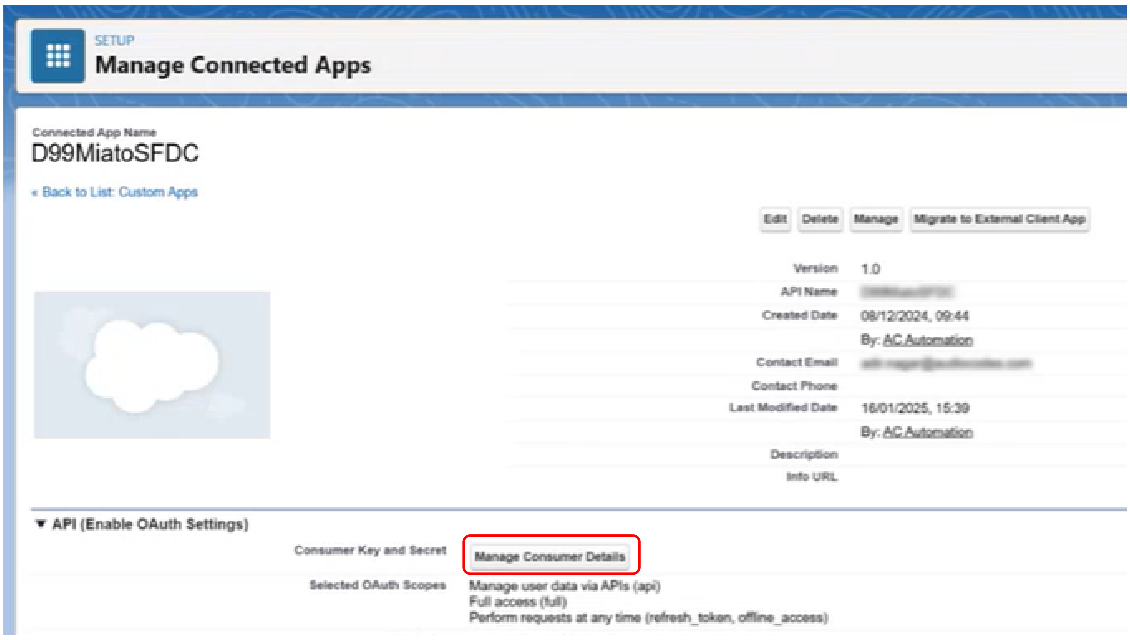


Obtaining Client ID and Secret of Salesforce Connected App

Once you've created the connected app for Meeting Insights integration, you can obtain its client ID and client secret, which you need for configuring Meeting Insights.

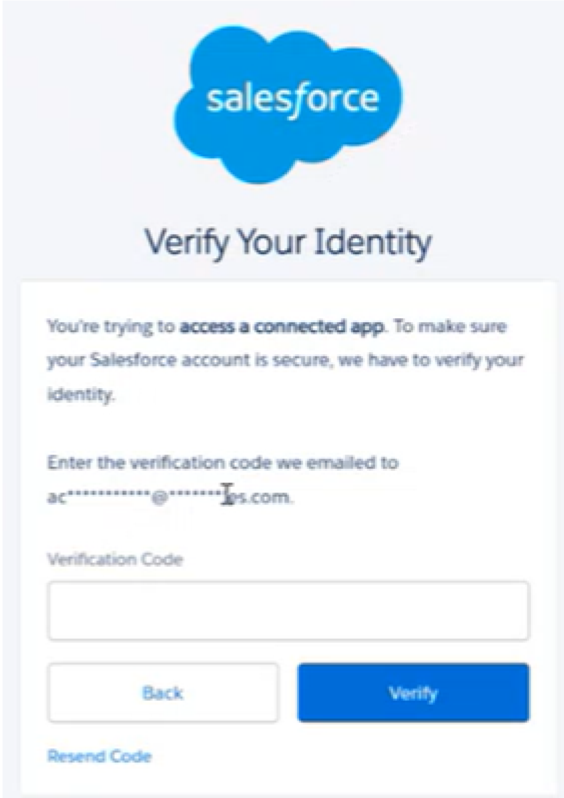
➢ To obtain client ID and secret:

1. Sign in to your Salesforce account.
2. Click the gear ⚙ icon in the top-right corner, and then choose **Setup**.
3. In the left navigation menu, expand **Apps**, and then choose **App Manager**.
4. In the App Manager list, click the down-pointing arrow corresponding to the new connected app, and then from the drop-down menu, choose **View**.
5. Click the **Manage Consumer Details** button:



   A verification code is sent to your email.

6. Enter the code in the 'Verification Code' field in the displayed dialog box:



7. Click **Verify**; the client ID is displayed in the 'Consumer Key' field and the client secret is displayed in the 'Consumer Secret' field:

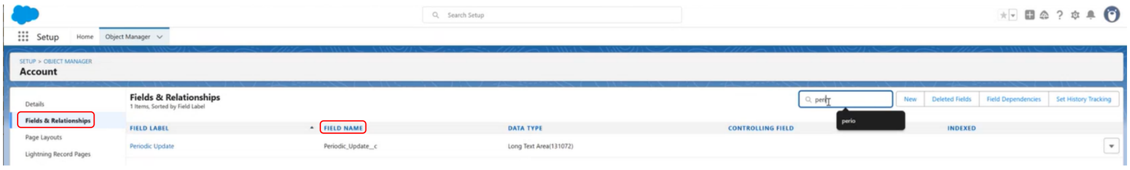
Obtaining Salesforce Object Field (API) Names

The following procedure describes how to obtain the field names for the Account and Opportunity objects. These must be the API field names, which you need for configuring Meeting Insights.

➢ **To obtain object field names:**

1. Sign in to your Salesforce account.

2. Click the gear ⚙ icon in the top-right corner, and then choose **Setup**.
3. In the left navigation menu, choose **Object Manager**, and then select the object (e.g., Account).
4. Click **Fields & Relationships**, and then search for the required field. The API field name is displayed in the 'Field Name' column, as shown in the following example:

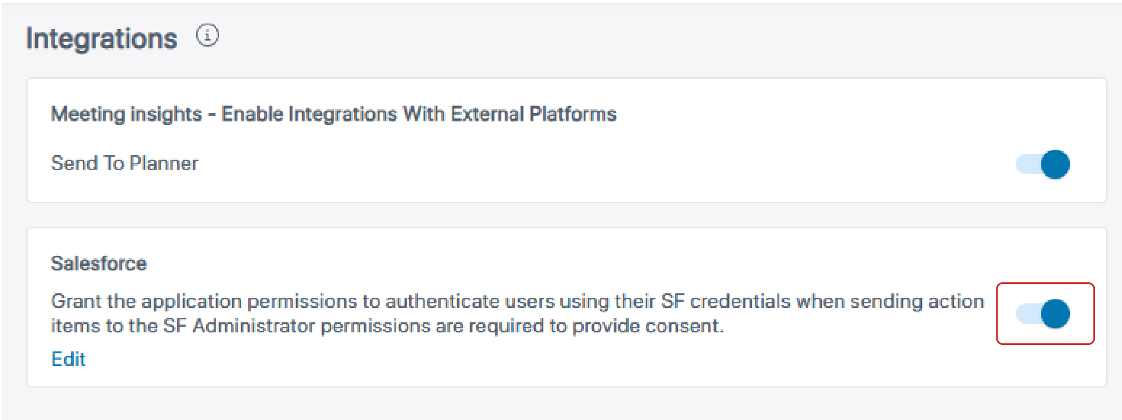


Configuring Meeting Insights for Salesforce Integration

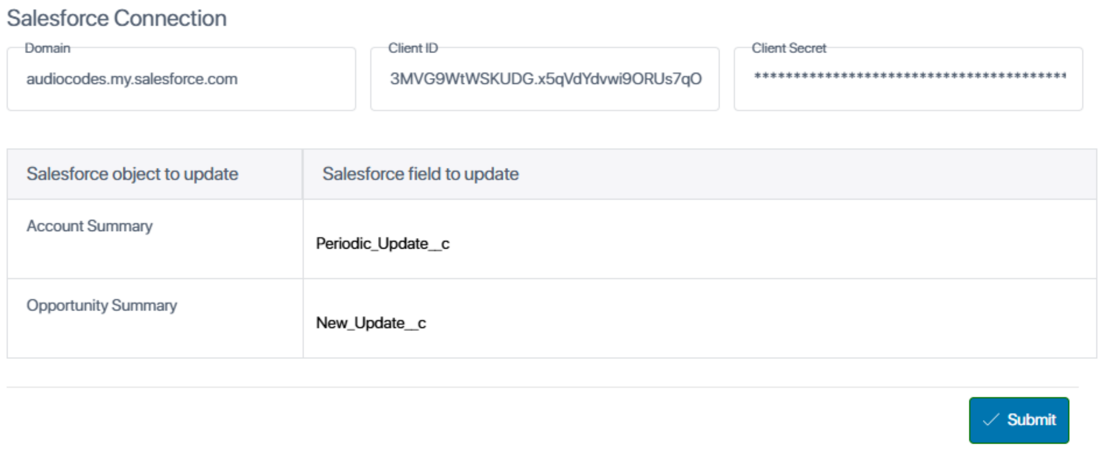
Once you have obtained the required information from your Salesforce account (see Setting Up Salesforce and Obtaining Required Information on page 97), you can configure Meeting Insights for integration with Salesforce.

➢ To configure Meeting Insights for Salesforce integration:

1. Under the ‘Settings’ menu, expand **Integrations**, and then click **Apps**; the Integrations page appears.
2. Under the **Salesforce** group, click the toggle button to enable Salesforce integration:



The following dialog box appears:



3. Configure Salesforce connectivity:

   a. In the 'Domain' field, enter the domain URL of your organization's Salesforce platform. For obtaining the domain URL, see Obtaining the Salesforce Domain URL on page 99.

   b. In the 'Client ID' field, enter the client ID of the Salesforce connected app. For obtaining the client ID, see Obtaining Client ID and Secret of Salesforce Connected App on page 100.

   c. In the 'Client Secret' field, enter the client secret key of the Salesforce connected app. For obtaining the client secret, see Obtaining Client ID and Secret of Salesforce Connected App on page 100.

4. For each Salesforce object listed under 'Salesforce object to update' (Account or Opportunity), enter the Salesforce field name in the corresponding 'Salesforce field to update' column. These are the fields where Meeting Insights sends the meeting summary (if selected by the user).

- The field names must be the **API** field names. To obtain the API field names, see Obtaining Salesforce Object Field (API) Names on page 101.
- Make sure that the field names are exactly as they appear in Salesforce.
- Meeting Insights supports only the Account and Opportunity Salesforce objects.
- When Meeting Insights updates a Salesforce object field with the AI-powered summary, it adds the new content to any existing content.

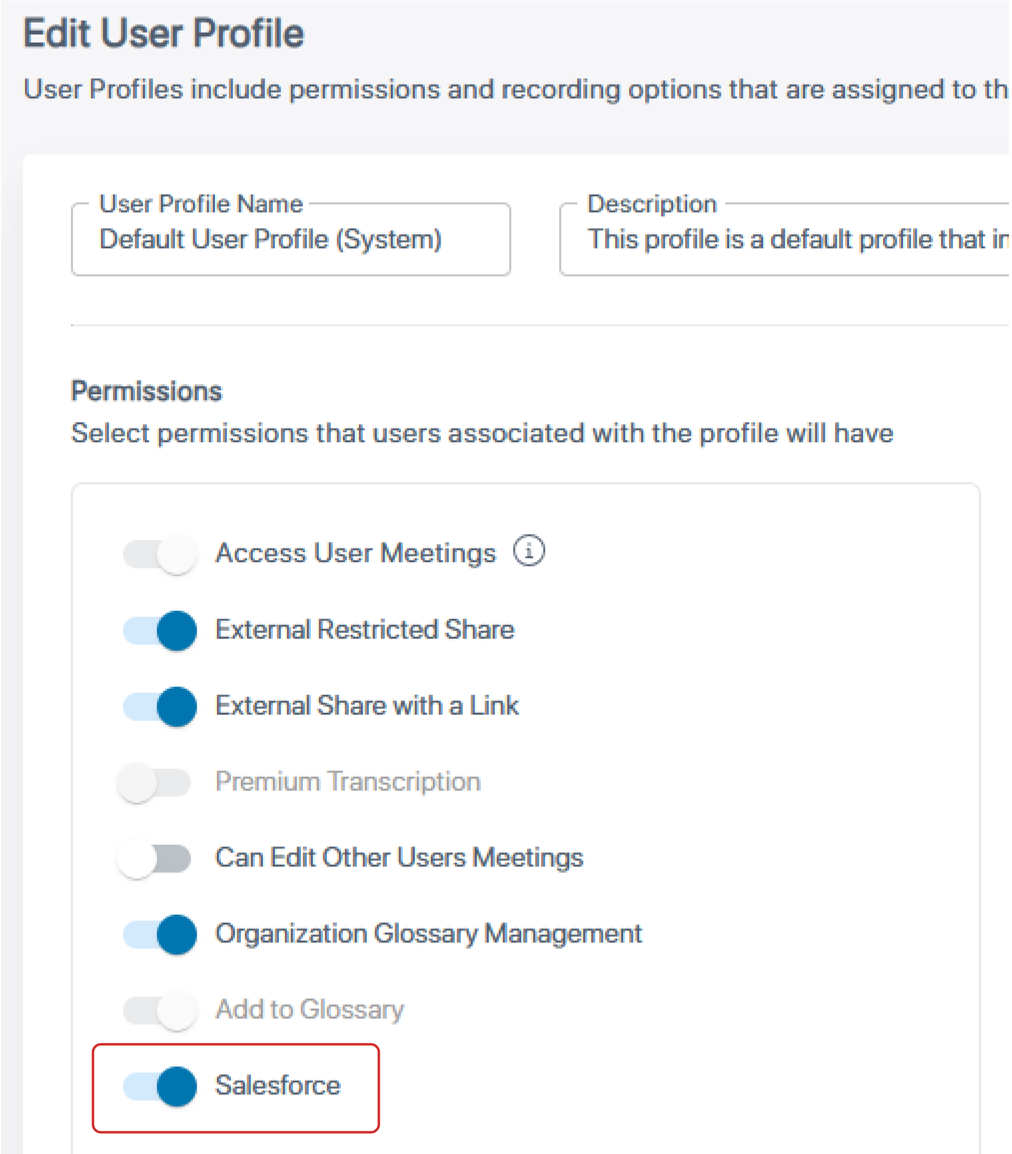
5. Click **Submit**.

6. Enable Salesforce for User Profiles:

   a. Expand the **User Settings** menu, and then click **User Profiles**.

   b. Add a new User Profile or edit an existing one.

   c. Under the Permissions group, click the **Salesforce** toggle button to turn it on:



7. Click **Apply**.

Customizing Bot Names for Recording Zoom and External Teams Meetings

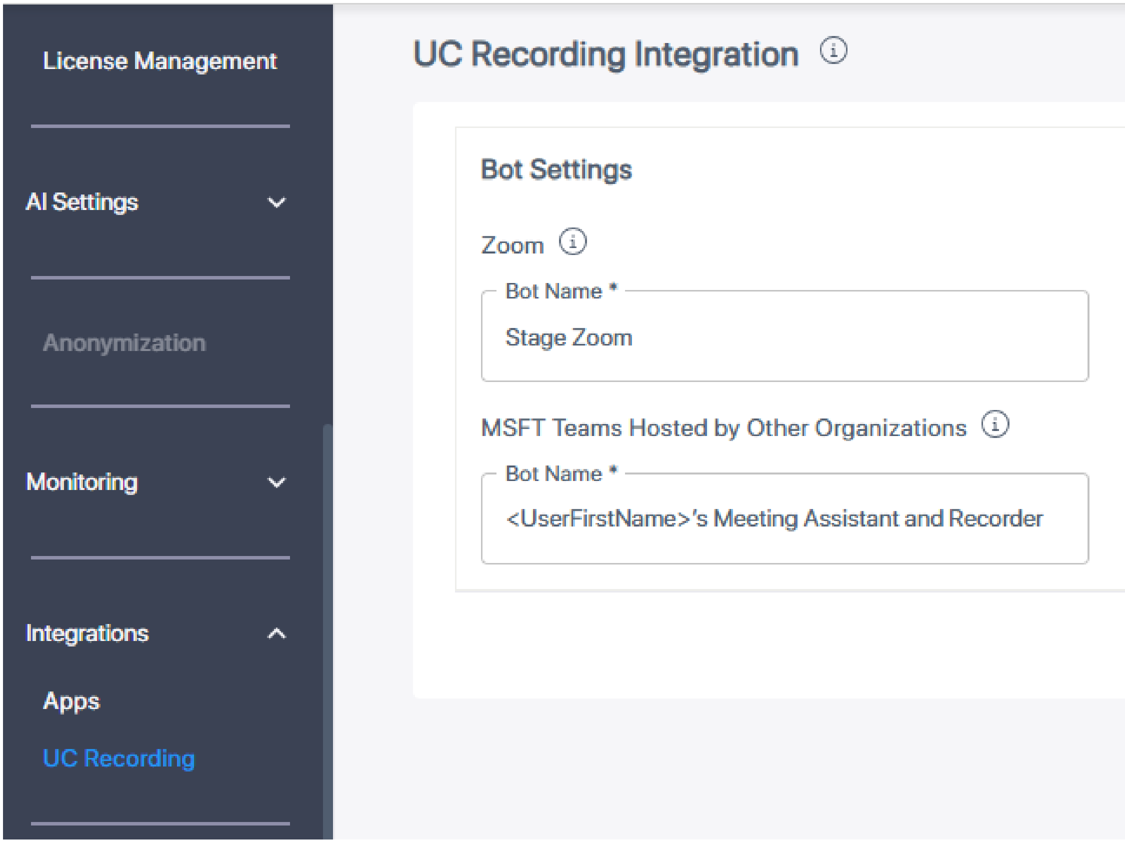
If you've enabled the recording for a User Profile of Zoom meetings, or Microsoft Teams meetings organized by an external organization, you can customize the name of the Meeting Insights bot that joins these meetings to record them.

You can use placeholders (variables or templates) when defining the bot name, which Meeting Insights replaces with real values. For example, if the user's name is John, then the bot name defined as '<UserFirstName>'s Meeting Assistant' is displayed as 'John's Meeting Assistant'.

The default bot names is '<UserFirstName>'s Meeting Assistant and Recorder'.

➢ **To customize bot names:**

1. In the Admin Settings navigation pane, expand **Integrations**, and then click **UC Recording**.



2. **For Zoom meetings:**

   Under **Zoom**, in the 'Bot Name' field, configure a bot name. To view the supported placeholders that you can use, click the **i** icon.

3. **For Microsoft Teams meetings:**

   Under **MSFT Teams Hosted by Other Organizations**, in the 'Bot Name' field, configure a bot name. To view the supported placeholders that you can use, click the **i** icon.

4. Click **Apply**.

15 Configuring Automatic Invitation of MIA to Scheduled Meetings

Admins can configure automatically inviting Meeting Insights Assistant (MIA) to scheduled Teams and Zoom meetings, whether organized by a specific user or by a group of users. When the user then schedules a meeting, MIA is automatically added to the invitees list and the following disclaimer (for example) is added to the body of every invitation:

Disclaimer: The meeting is recorded

> The disclaimer is not displayed to the meeting's organizer when the organizer opens the meeting invitation. It is displayed (at the top of the body of the invitation) to all other recipients of the meeting invitation.

Take the following three steps to configure an automatic invitation of MIA to scheduled meetings:

1. Add a mail-enabled security group in Microsoft 360 admin center. See here how.

> Only a *mail-enabled security group* can be part of the mail rule.

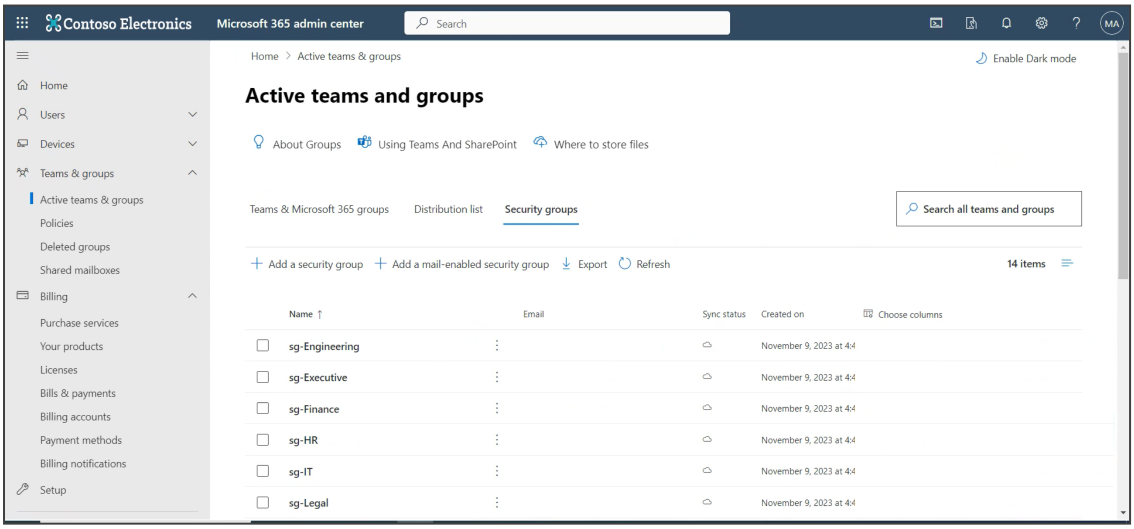
2. Define an auto-invite rule in Exchange admin center. See here how.
3. Test the rule. See here how.

Add a Mail-Enabled Security Group

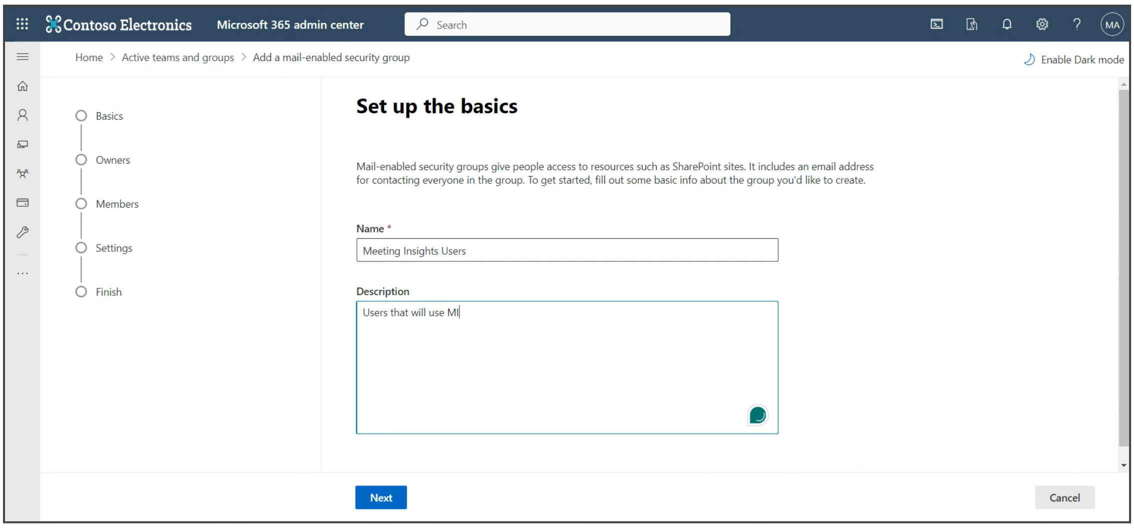
The instructions below focus on how to create a mail-enabled security group through Microsoft 365 admin center.

➢ **To add a mail-enabled security group:**

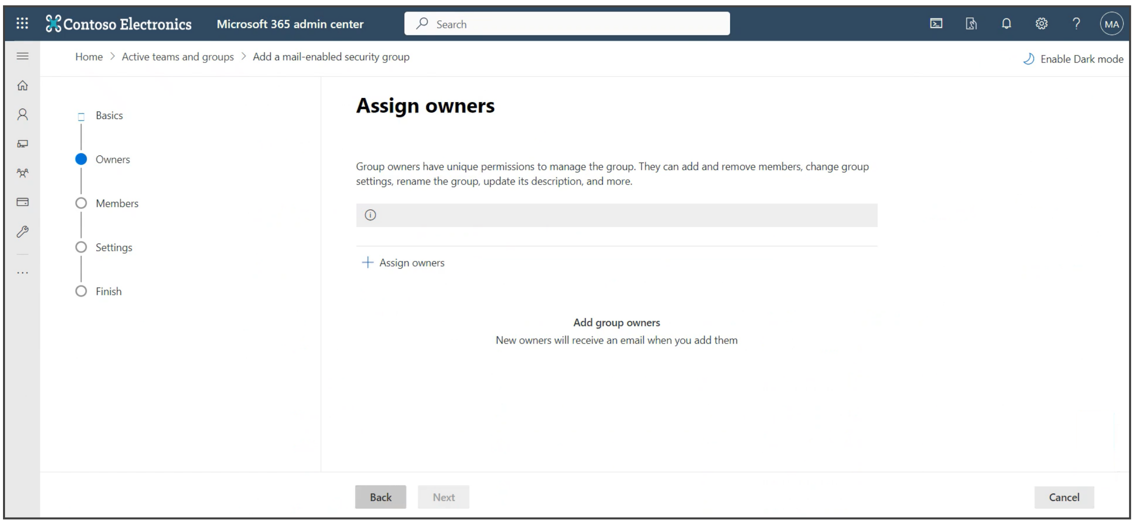
1. In Microsoft 365 admin center, go to **Teams & groups** > **Active teams & groups** > **Security Groups** tab.



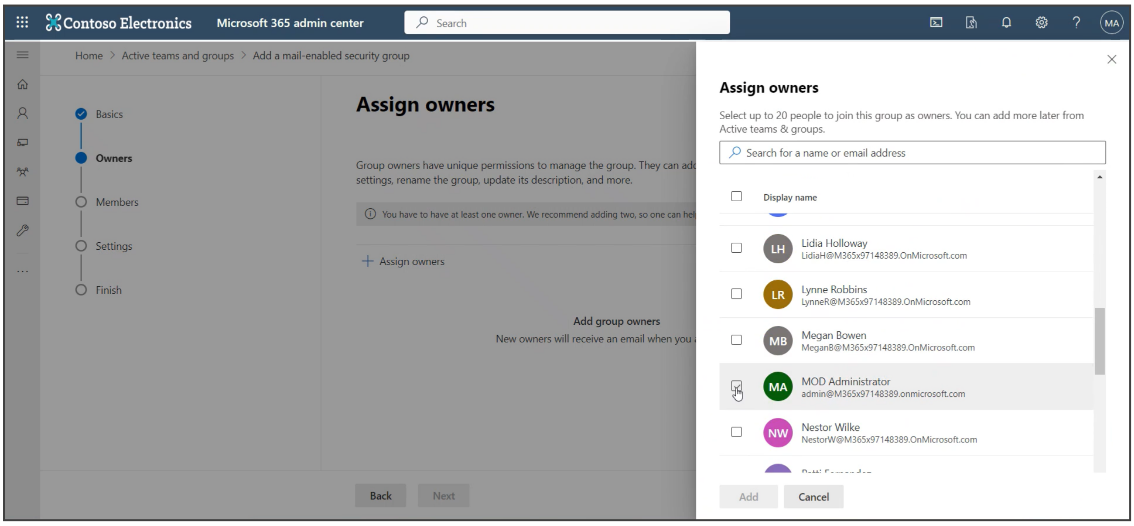
2. In the 'Active teams & groups' page shown above, click **+ Add a mail-enabled security group**.



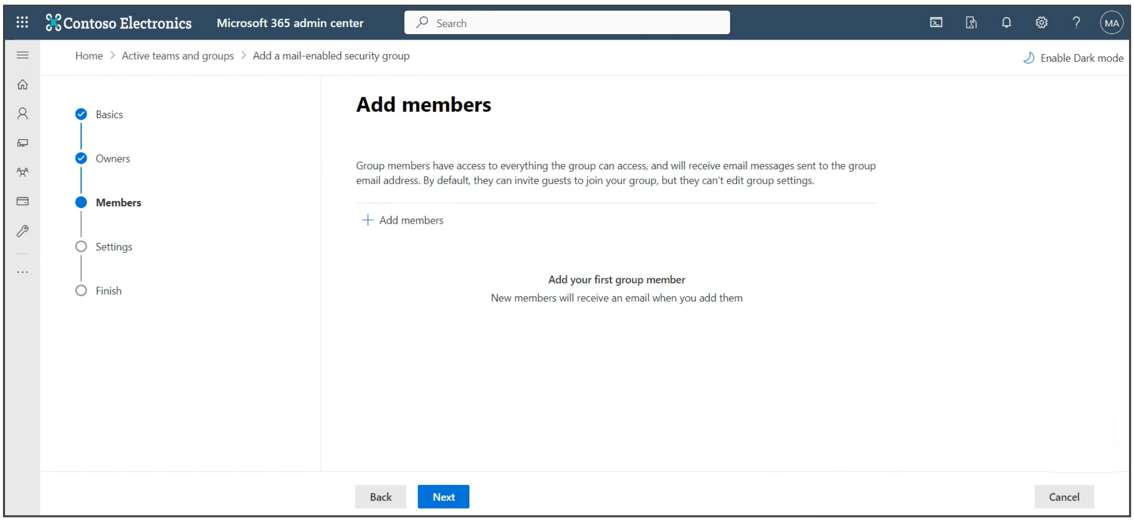
3. In the 'Set up the basics' page shown above, enter **Meeting Insights Users** in the 'Name' field, enter a 'Description' to facilitate effective management later, and then click **Next**.



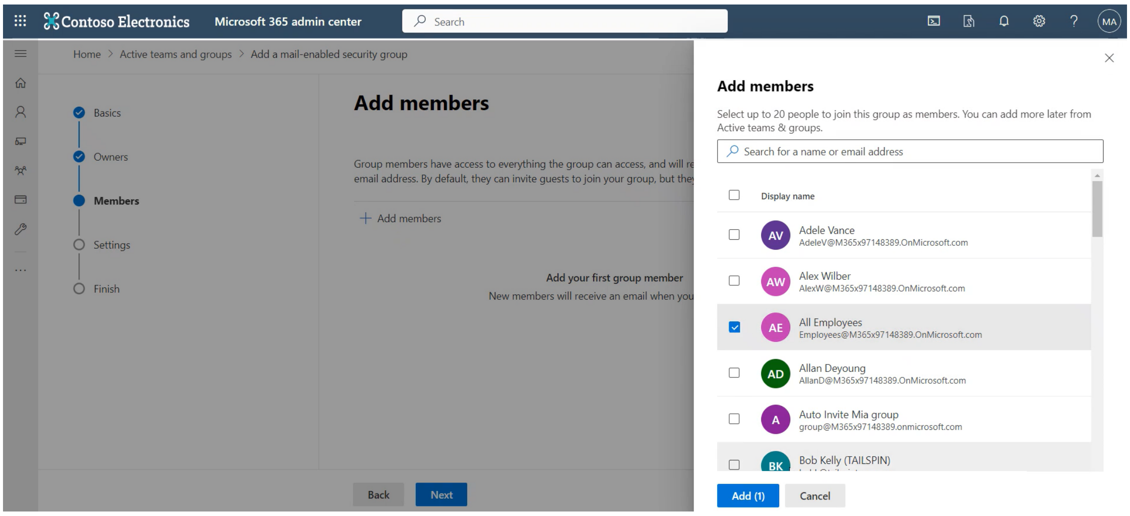
4. In the 'Assign owners' page that opens, click **+ Assign owners.**



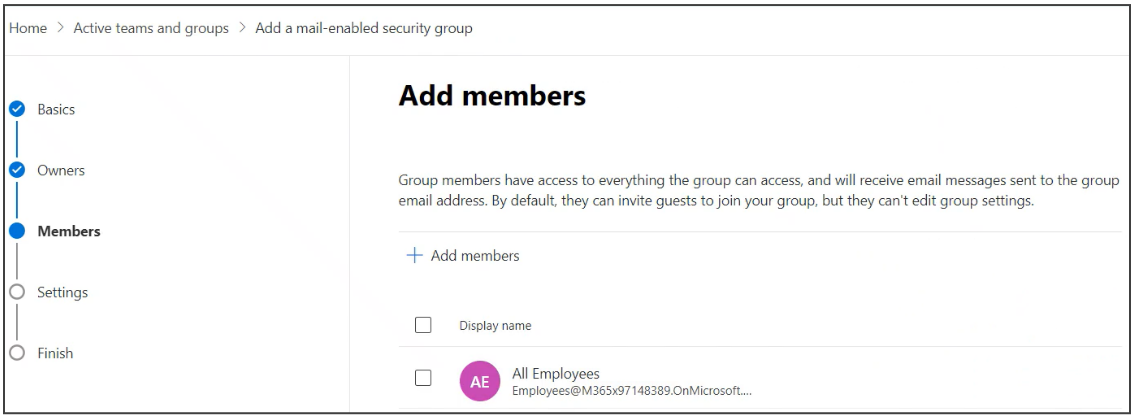
5. From the list that pops up on the right side, select an owner(s) and click **Add**.



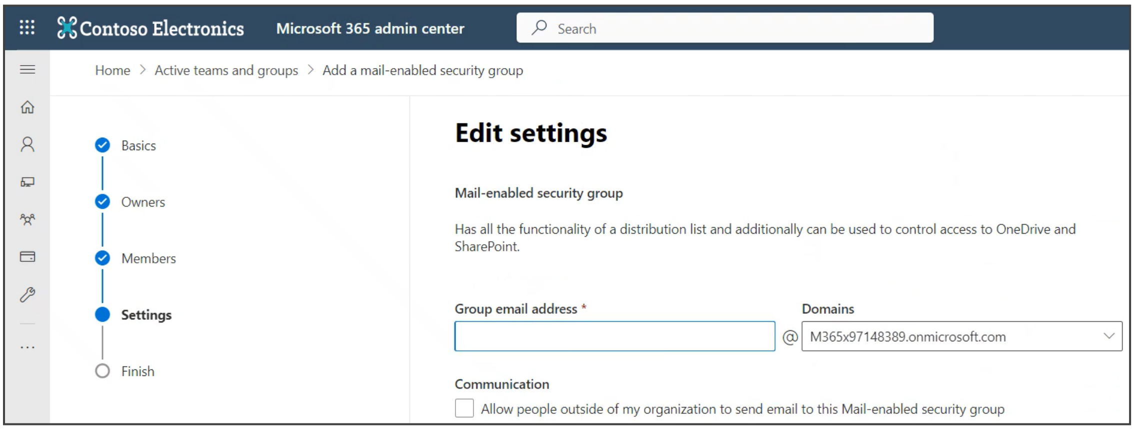
6. In the 'Add members' page shown above, click **+ Add members**.



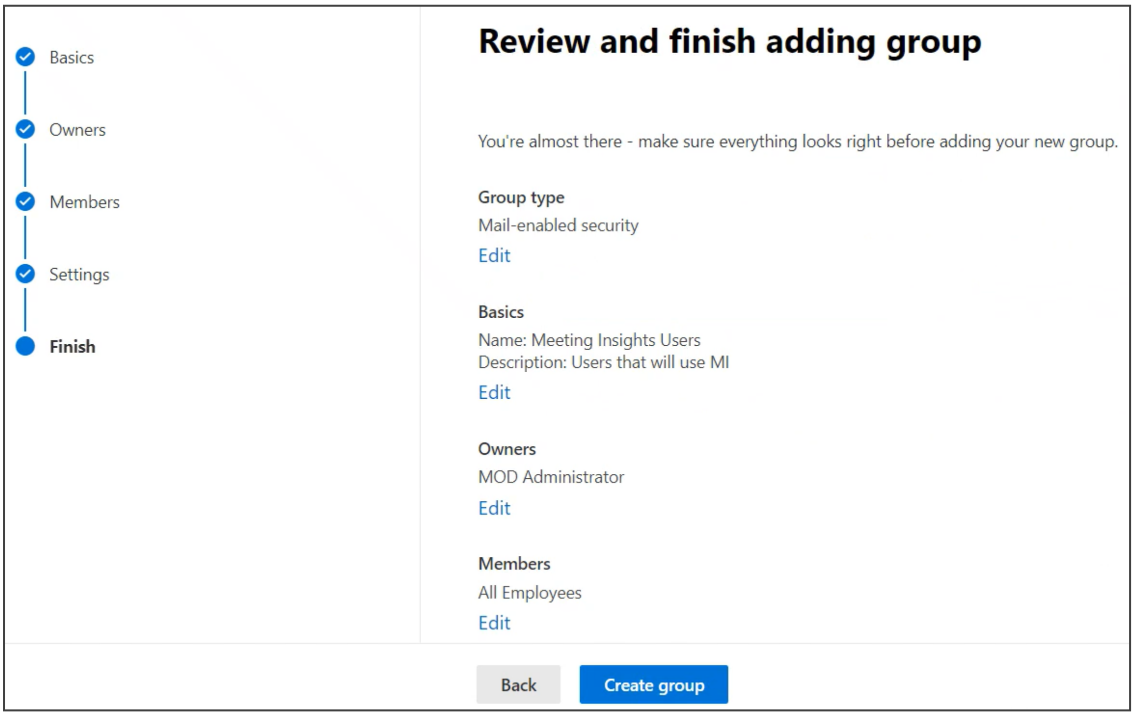
7. Select individual members to add to the group or groups, and then click **Add**.



8. Make sure the members you selected were added, and then click **Next**.

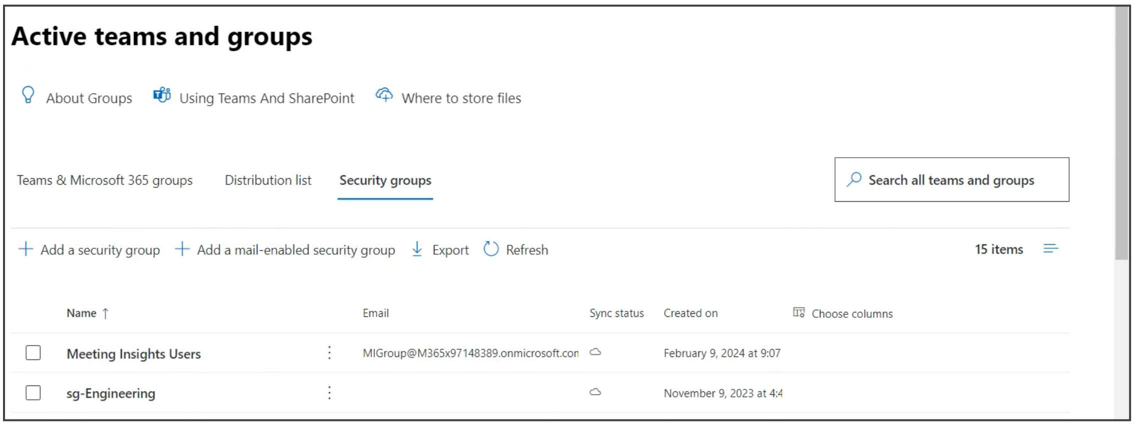


9. In the 'Group email address' field, enter a group name (e.g., MIGroup).



10. Click **Create group**.

11. Click **Close**. View the newly created mail-enabled security group listed in the 'Active teams and groups' page:



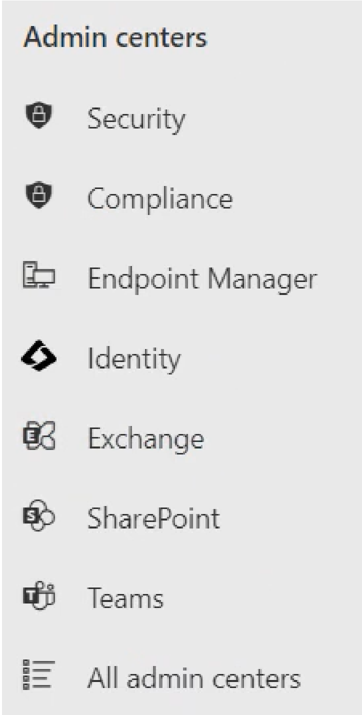
Next: Configure the 'Auto-Invite' rule as shown here.

Configure an Auto-Invite Rule

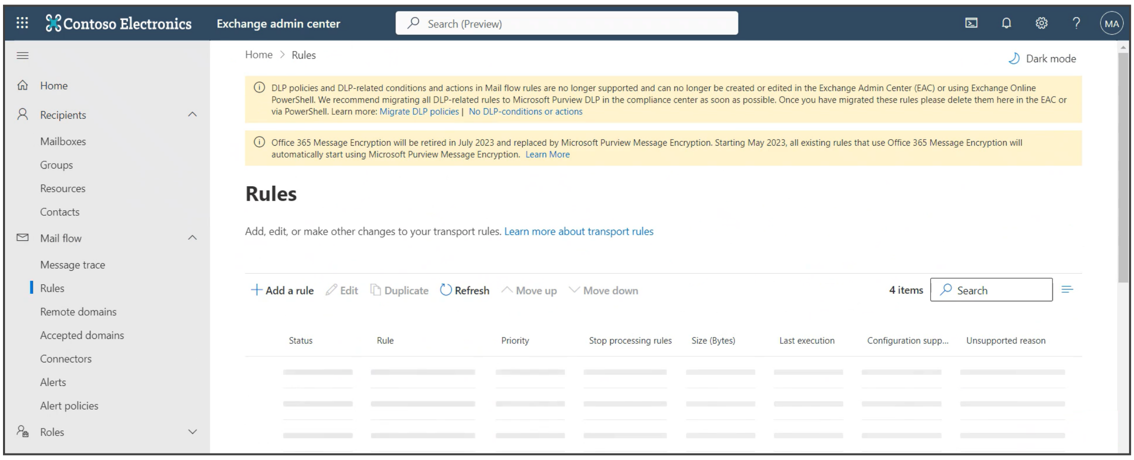
After adding a mail-enabled security group as shown previously, admins can configure an 'Auto Invite' rule from Microsoft's Exchange admin center. Configuring an Exchange rule from Microsoft 360 admin center involves defining specific conditions, including the message being a calendar event and containing the text 'Microsoft Teams meeting' for Teams meetings or 'Zoom meeting' for Zoom meetings.

➢ **To configure the 'Auto Invite' rule:**

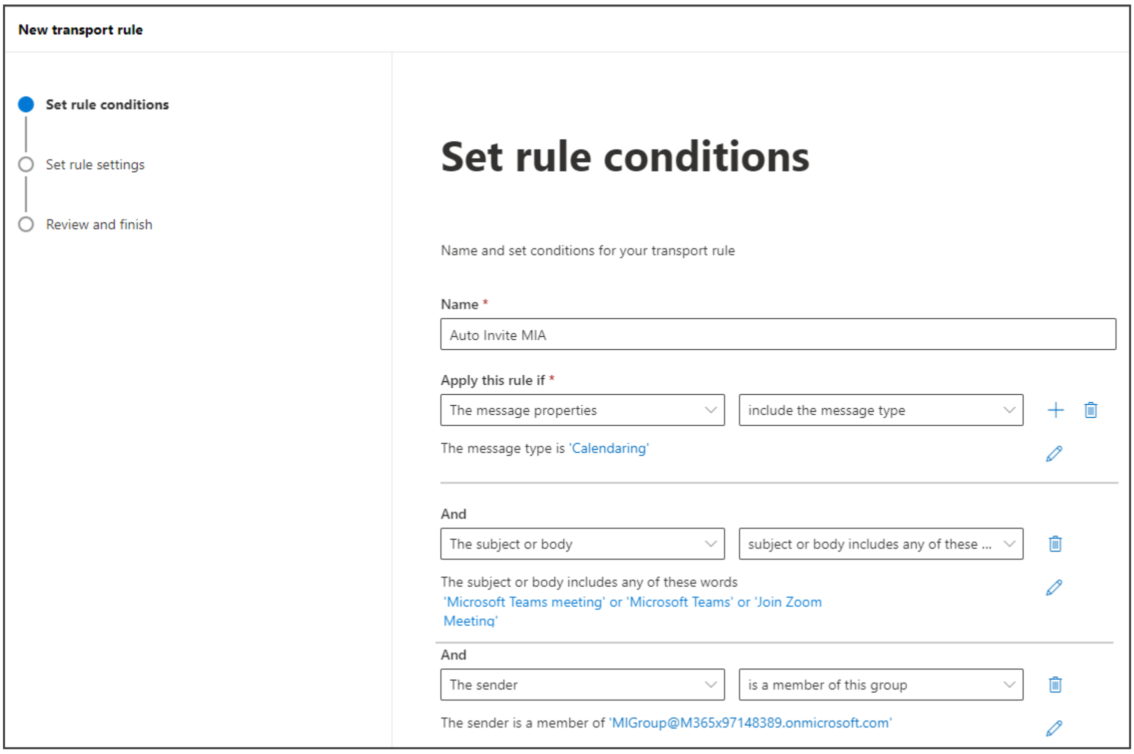
1. From the list of admin centers displayed in Microsoft 365 admin center (in which you added a mail-enabled security group), click **Exchange**.



2. In Exchange admin center, navigate to **Mail flow** > **Rules**.

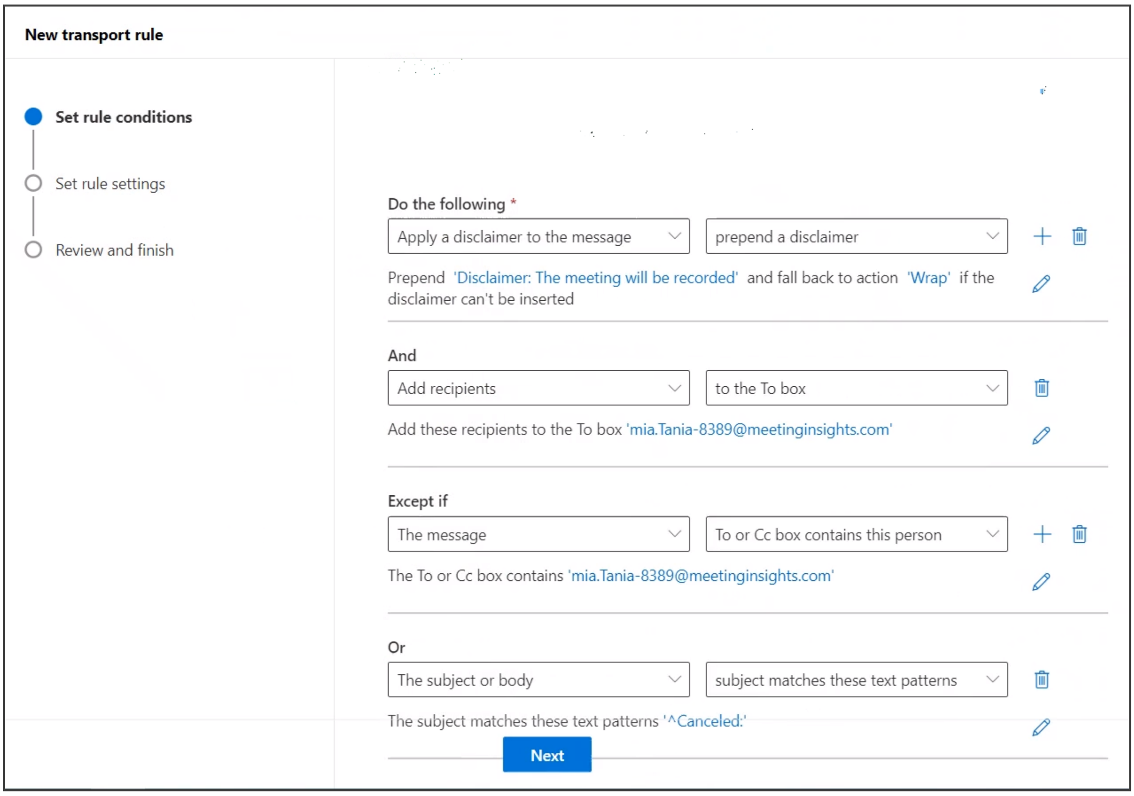


3. In the Rules page, click **+ Add a rule**.

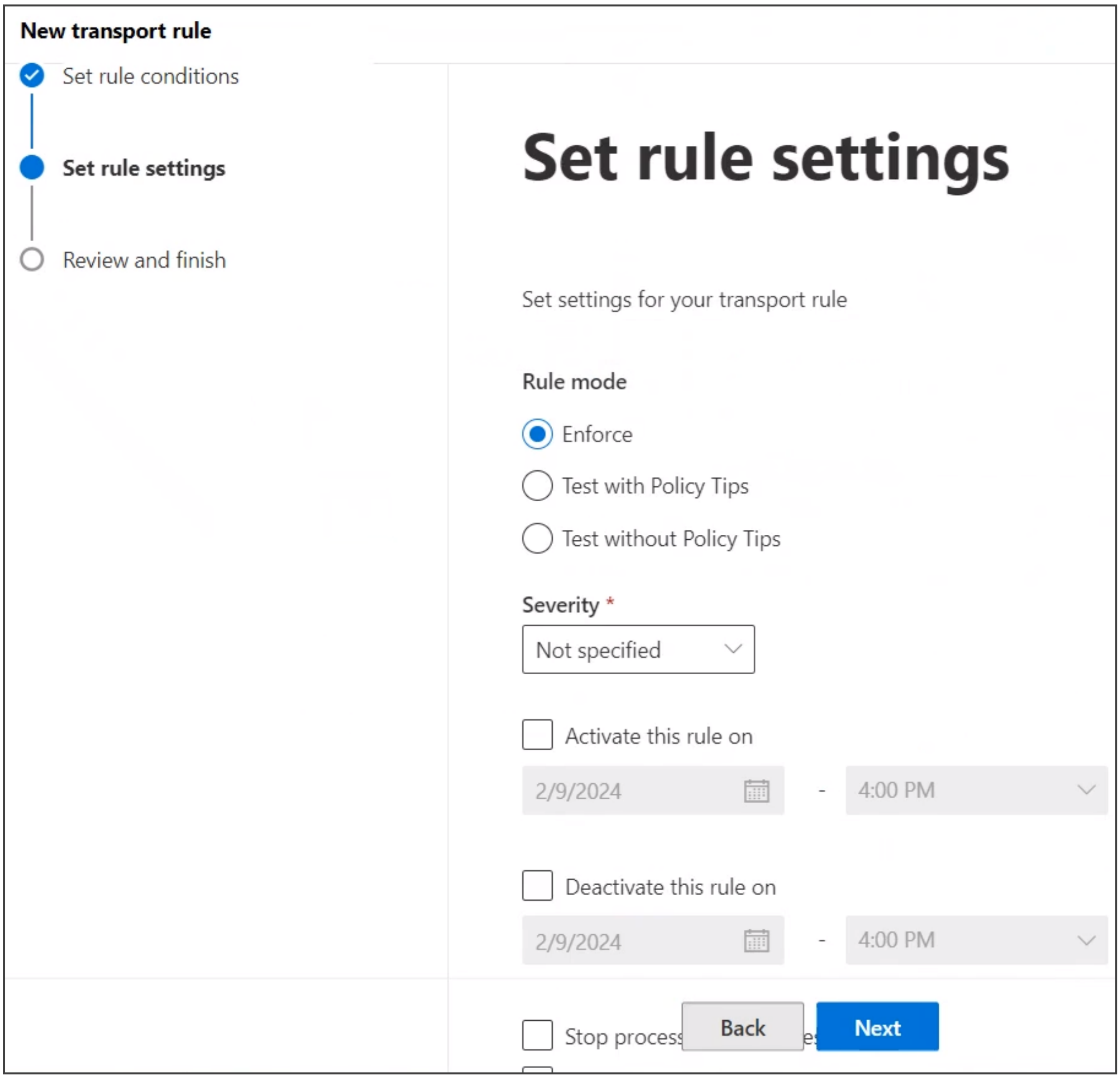


4. Set the following rule conditions using the figure above as reference:
   a. Set a name for the rule, for example, Auto Invite Mia.
   b. From the two **Apply this rule if** drop-downs, select **The message properties** and **include the message type**respectively. Select **Calendaring** as the message type.
   c. Click **+**. From the two **And** drop-downs, select **The subject or body** and **subject or body includes any of these words** respectively. Enter **Microsoft Teams meeting** , **Microsoft Teams**, or **Join Zoom Meeting** as the words.
   d. Click **+**. From the two **And** drop-downs, select **The sender** and **is a member of this group**respectively. Select the group you created in the previous procedure. In the figure above, it is MIGroup@M365x97148389.onmicrosoft.com
5. Scroll down and continue setting the rule conditions using the figure below as reference:
   a. From the two **Do the following** drop-downs, select **Apply a disclaimer to the message** and **prepend a disclaimer** respectively.
      i. For the disclaimer, define any disclaimer your organization requires, for example: 'Disclaimer: The meeting will be recorded'.
      ii. Select 'Wrap' as the action to fall back to if the disclaimer can't be inserted.
   b. Click +. From the two **And** drop-downs, select **Add recipients** and **to the To box** respectively. Define the **To box** email.
   c. From the two **Except if** drop-downs, select **The message** and **To or Cc box contains this person** respectively. Define the person's email address.

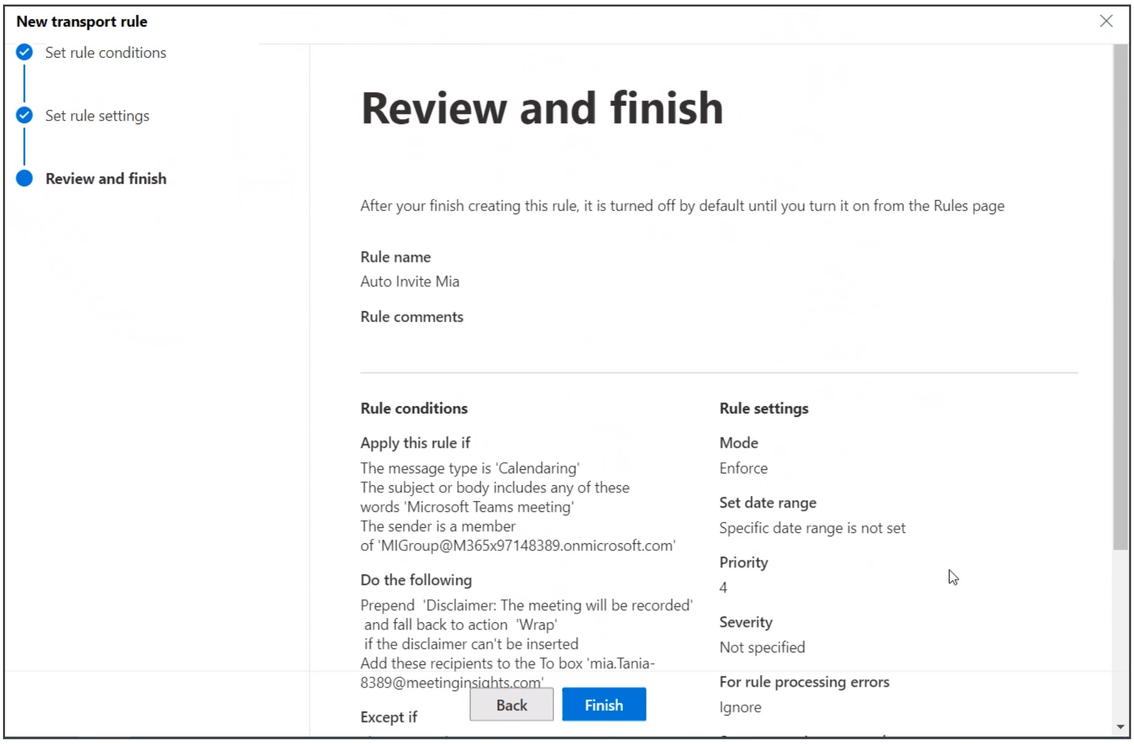
d. From the two **Or** drop-downs, select **The subject or body** and **subject matches these text patterns**respectively. Define the text pattern **^Canceled:**



6. Click **Next**.

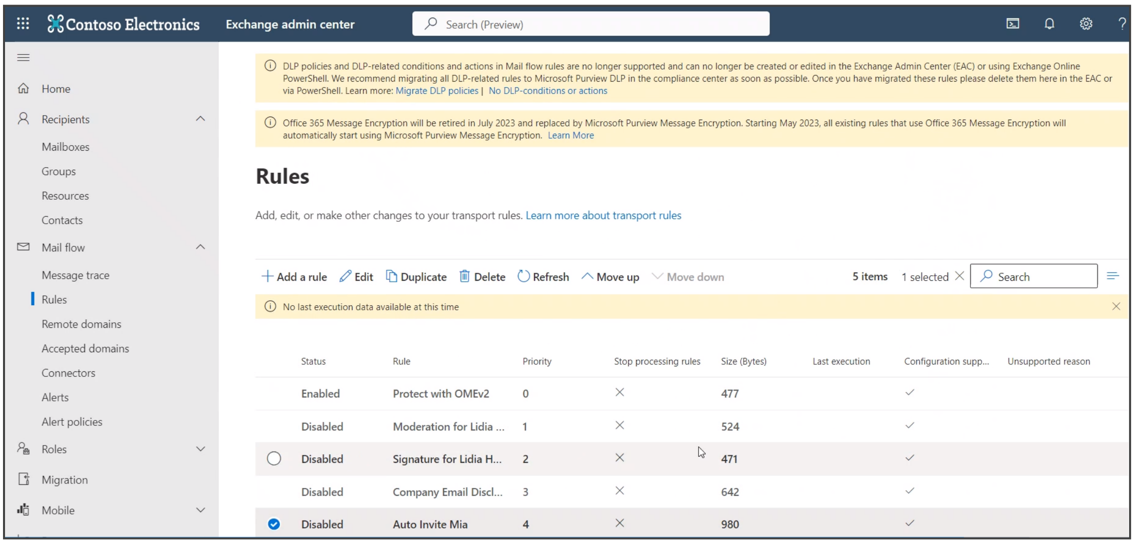


7. Set the rule settings as follows:
   a. Leave 'Rule mode' at its default **Enforce**.
   b. For the 'Severity' level drop-down, optionally leave this filter at **Not specified** or set it according to your organizational requirements (to make the reports easier to use).
   c. Select 'Activate this rule on' and set it to take effect immediately.
   d. From the 'Match sender address in message' drop-down, select **Header**.
8. Click **Next**.

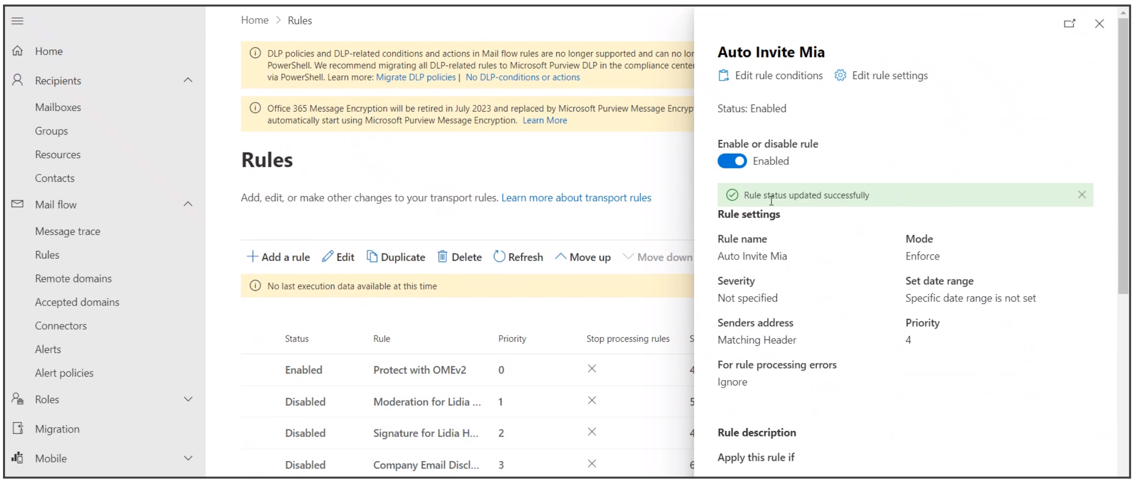


9. Make sure all settings are configured as described until now, and then click **Finish**.

10. Make sure the newly configured rule ('Auto Invite Mia' in the example below) is listed in Exchange admin center.



11. Enable the rule.



It's recommended to enable MIA automatic invite for all users by default. Users who don't want to record a meeting can either pause the recording or remove MIA participants from the meeting.

Next: Test the rule as shown here.

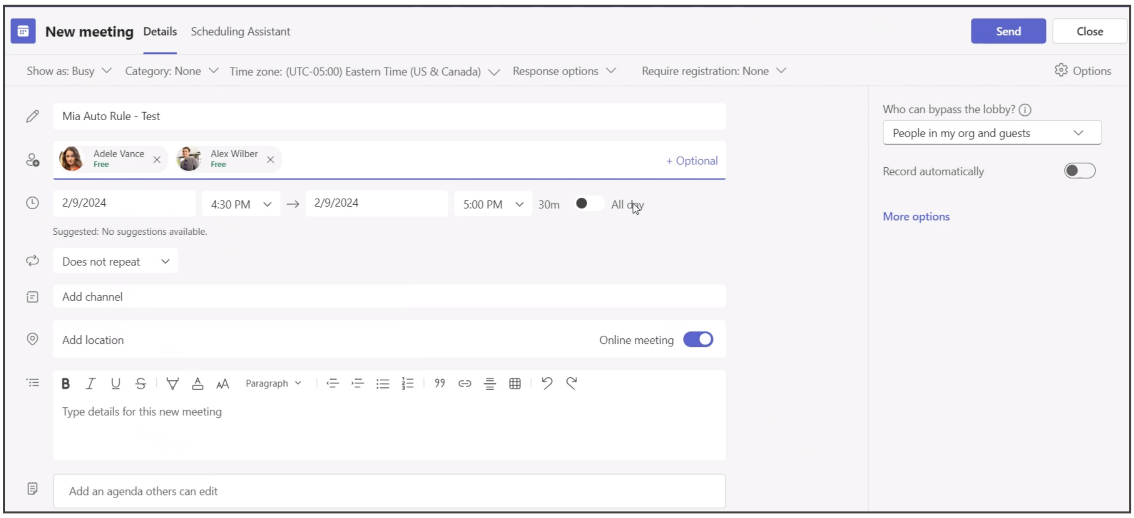
Test the Rule

It takes up to 30 minutes for the MIA 'Auto-Invite' rule to take effect.

Admins can test the MIA 'Auto-Invite' rule to make sure it functions according to expectations.

➢ Test the MIA 'Auto-Invite' rule:

1. Log in to the admin's Teams app, open the Calendar and then click **+ New meeting**.
2. Enter a title for the meeting, for example, 'MIA Auto Rule - Test', and then add required attendees.



3. Click the **Send** button; the rule kicks in.

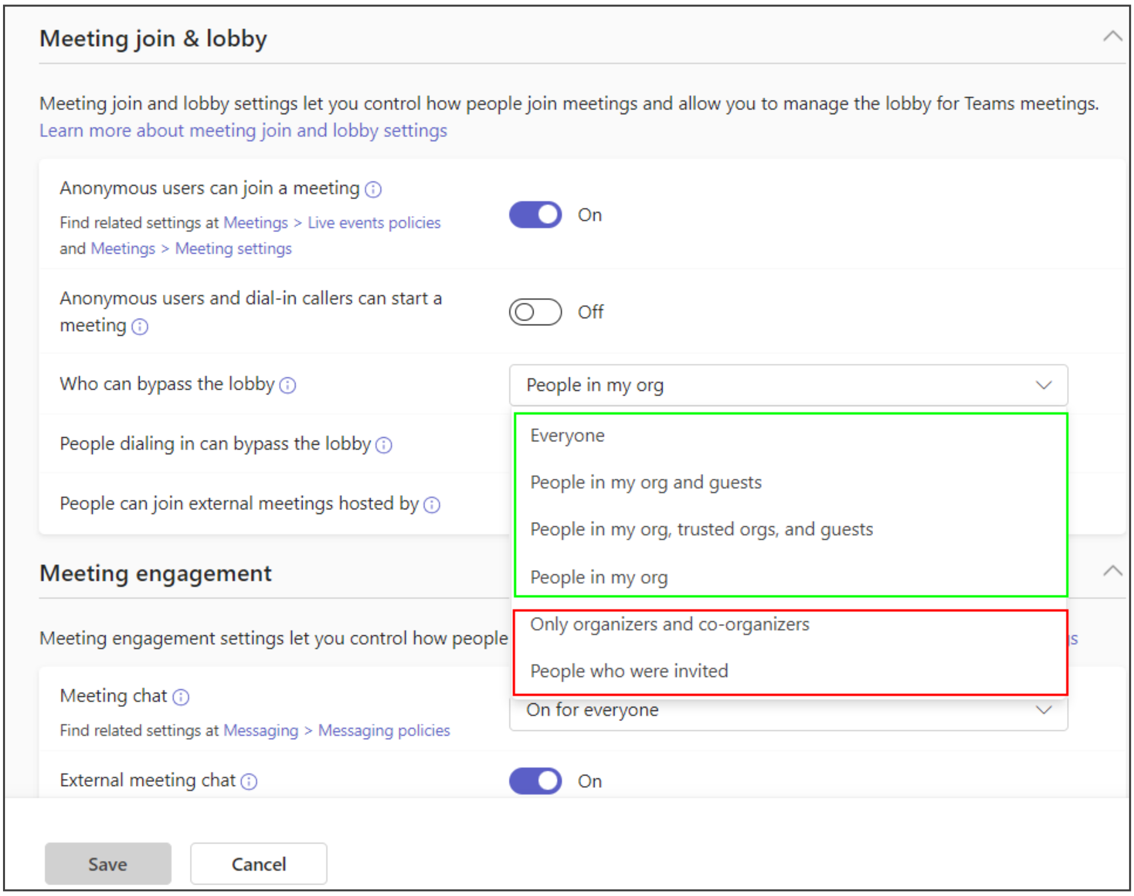
4. In Outlook, make sure the invitation arrived and that MIA was invited.

Managing the Lobby for Teams Meetings

Admin can use the 'Meeting join and lobby' settings in Microsoft Teams admin center (TAC) to manage people joining meetings and to manage the lobby for Teams meetings. Configuration of 'Meeting join and lobby' is part of the meeting policy which takes effect on the meetings of users who are assigned to the policy.

[Refer to the figure below]

- When the meeting policy settings indicated in green (below) are configured, MIA will *bypass* the meeting lobby of users assigned to this policy.
- When the meeting policy settings indicated in red (below) are configured, MIA will be *routed* to the meeting lobby of the users assigned to this policy.



16 Producing Power BI Analytics Usage Reports

Admin can integrate Meeting Insights Analytics Dashboard into their Microsoft Power Business Intelligence (BI).

The following links show how to

1. Enable Power BI integration in Meeting Insights (see here)
2. Install | configure Power BI (see here)
3. Determine usage statistics from reports (see here)
4. Disable Power BI integration (see here)

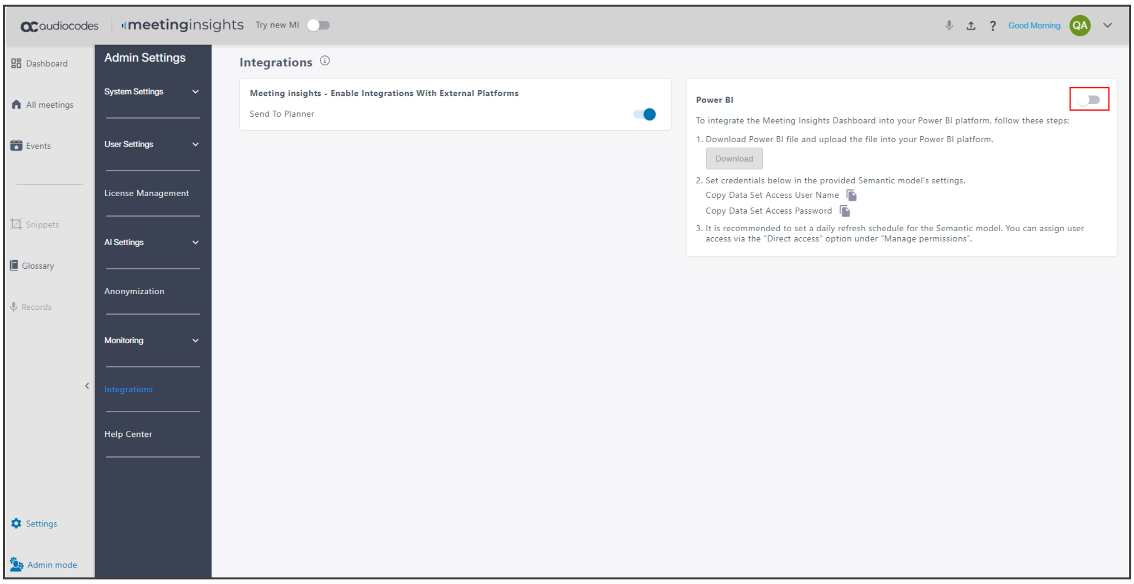
Enabling Power BI Integration in Meeting Insights

The instructions below show admin how to enable Power BI integration in Meeting Insights.

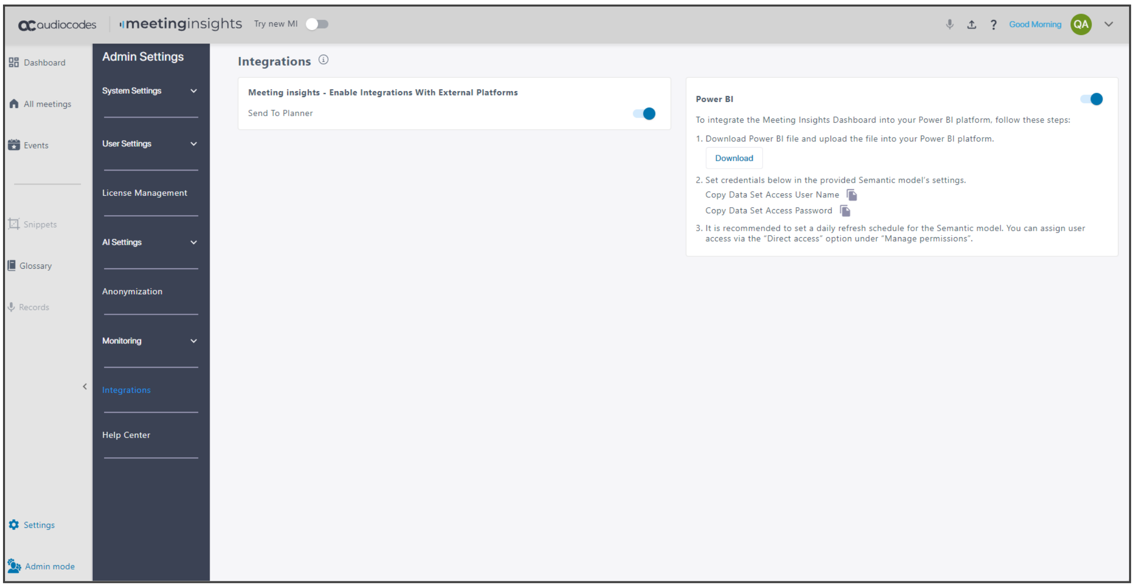
- Admin will view the integration only if it is enabled for their application.
- If you don't have it and you want to have it, contact the Service Provider.

➢ To enable Power BI integration in Meeting Insights:

1. In Meeting Insights, open the Integrations page.



2. Slide the switch indicated in the preceding figure to ON.



3. Click the **Download** button shown in the preceding figure to download the Power BI report file (.pbix) and upload it to your Power BI platform.
4. Copy the credentials and then see step 5 here for further instructions.

Installing | Configuring Power BI Analytics

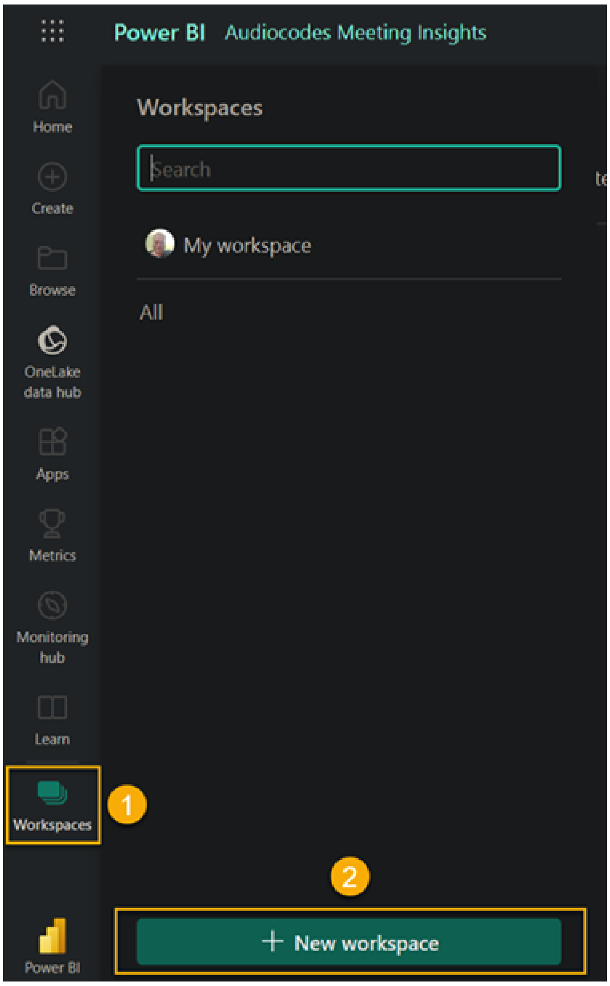
The procedure described here shows how to install | configure Meeting Insights Power BI Analytics.

Prerequisites

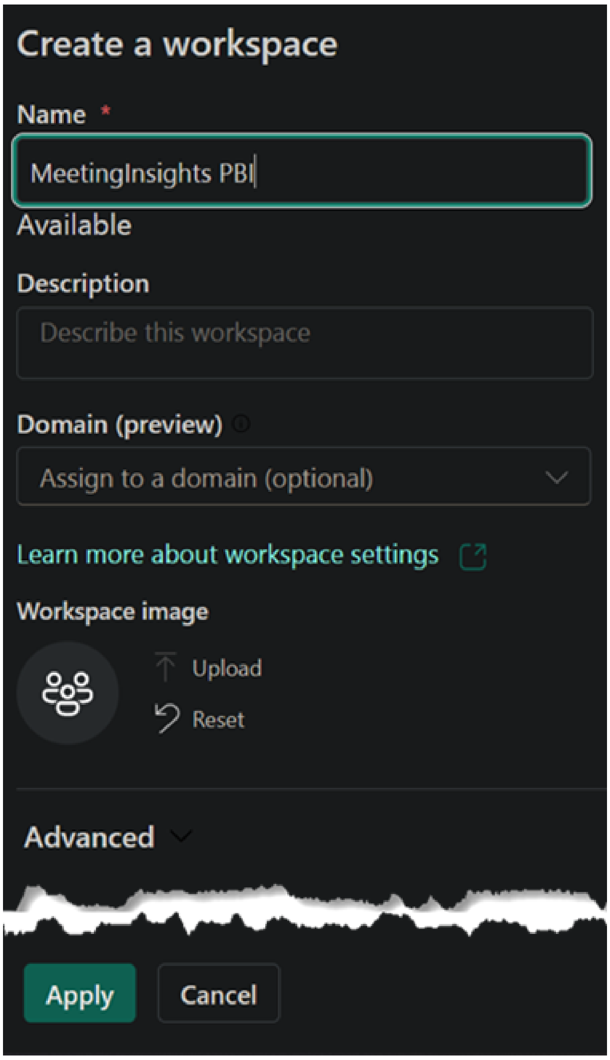
- Office 365 E5 customer account or any Office 365 licensed account with an individual Power BI Pro license attached.
- One Power BI Pro license is included with Microsoft E5 license.

➢ **To install | configure Power BI:**

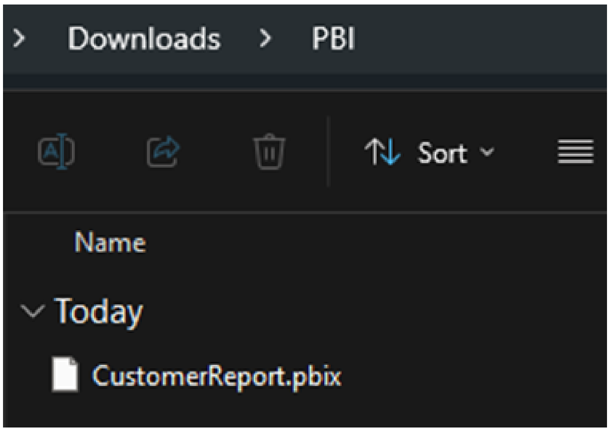
1. Sign in to the Microsoft Power BI portal at https://app.powerbi.com/



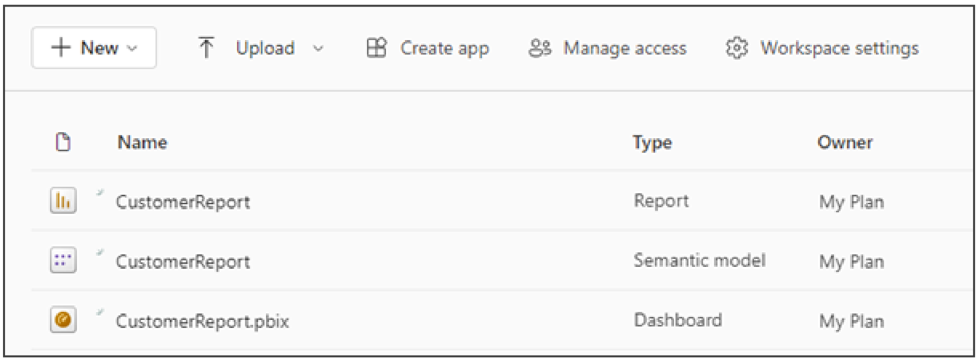
2. Click **+ New workspace**.

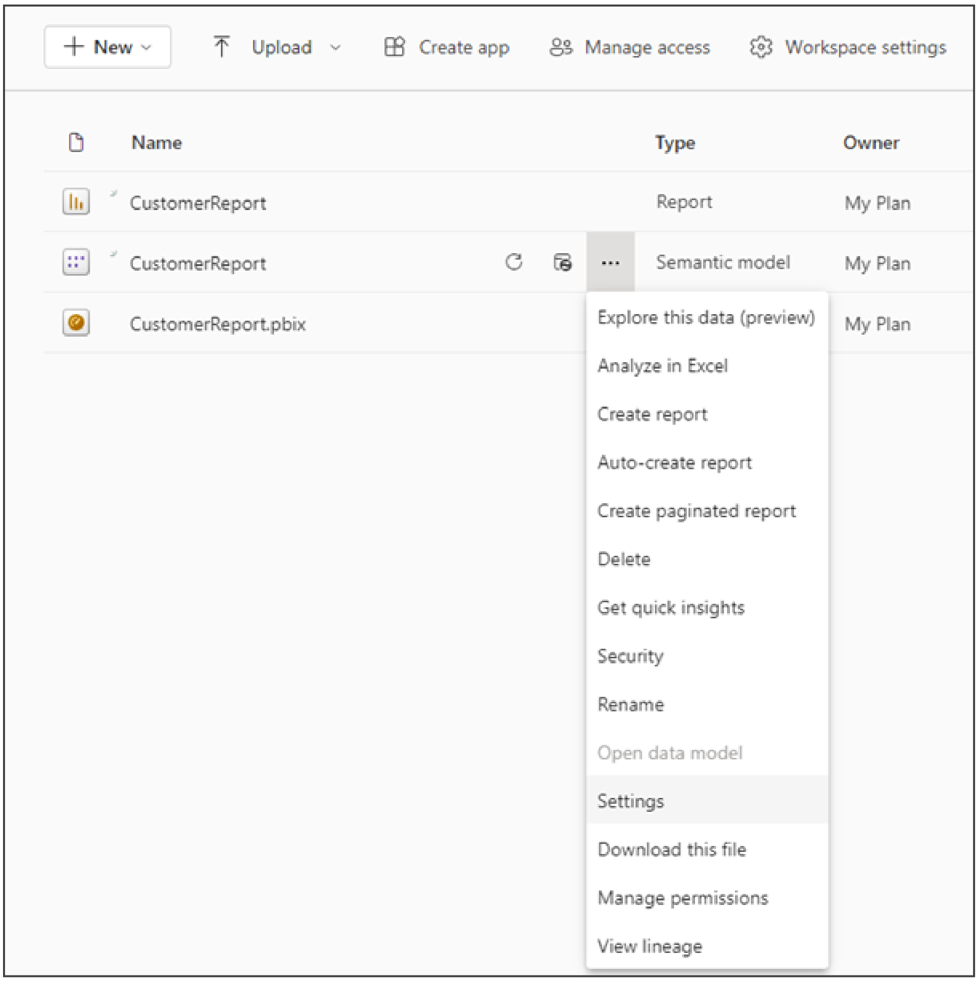


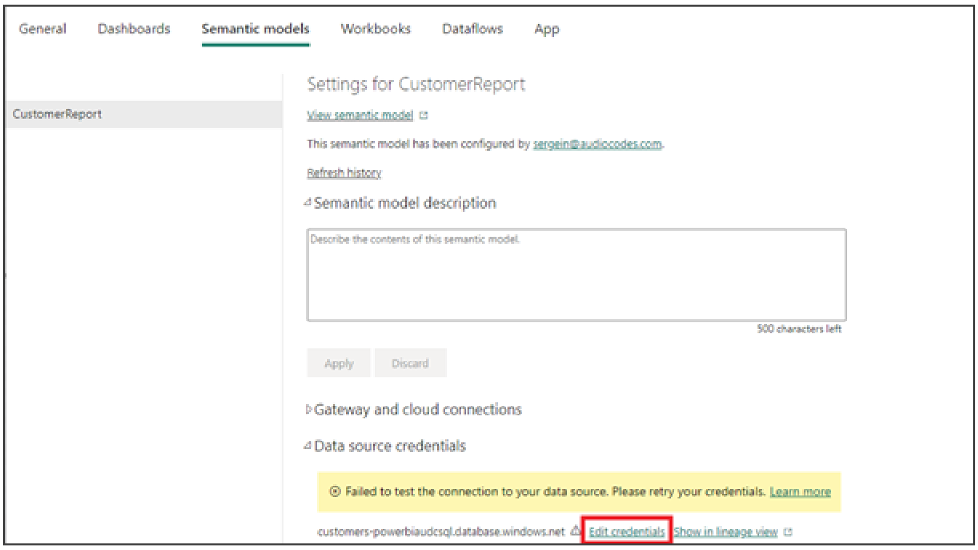
3. Enter a name for the new workspace and click **Apply**.
4. Install the Power BI report file (.pbix) that you downloaded using the Integrations page in Meeting Insights as shown in step 3 here.

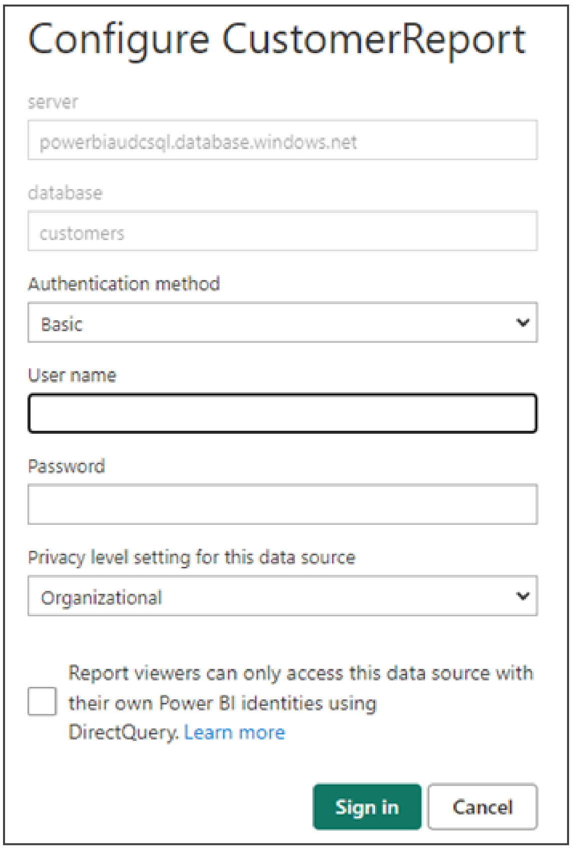


5. Use the following figures as reference to set credentials for the report. Copy the credentials using the Integrations page shown here.

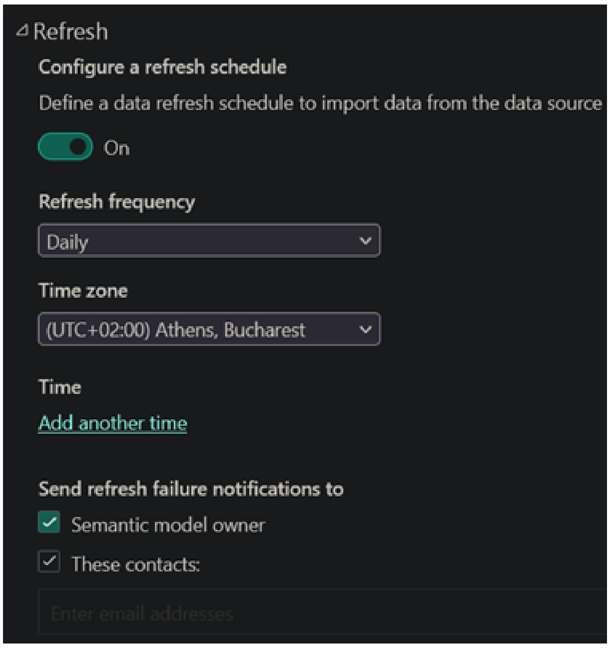



New
Upload
Create app
Manage access
Workspace settings
Name
Type
Owner
CustomerReport
Report
My Plan
CustomerReport
Semantic model
My Plan
CustomerReport.pbix
My Plan
Explore this data (preview)
Analyze in Excel
Create report
Auto-create report
Create paginated report
Delete
Get quick insights
Security
Rename
Open data model
Settings
Download this file
Manage permissions
View lineage


General
Dashboards
Semantic models
Workbooks
Dataflows
App
CustomerReport
Settings for CustomerReport
View semantic model
This semantic model has been configured by sergein@audiocodes.com.
Refresh history
Semantic model description
Describe the contents of this semantic model.
500 characters left
Apply
Discard
Gateway and cloud connections
Data source credentials
Failed to test the connection to your data source. Please retry your credentials. Learn more
customers-powerbiaudcsql.database.windows.net
Edit credentials
Show in lineage view



6. [Recommended] Set a daily refresh schedule for the Semantic model. You can assign user access via the **Direct access** option under 'Manage permissions'.

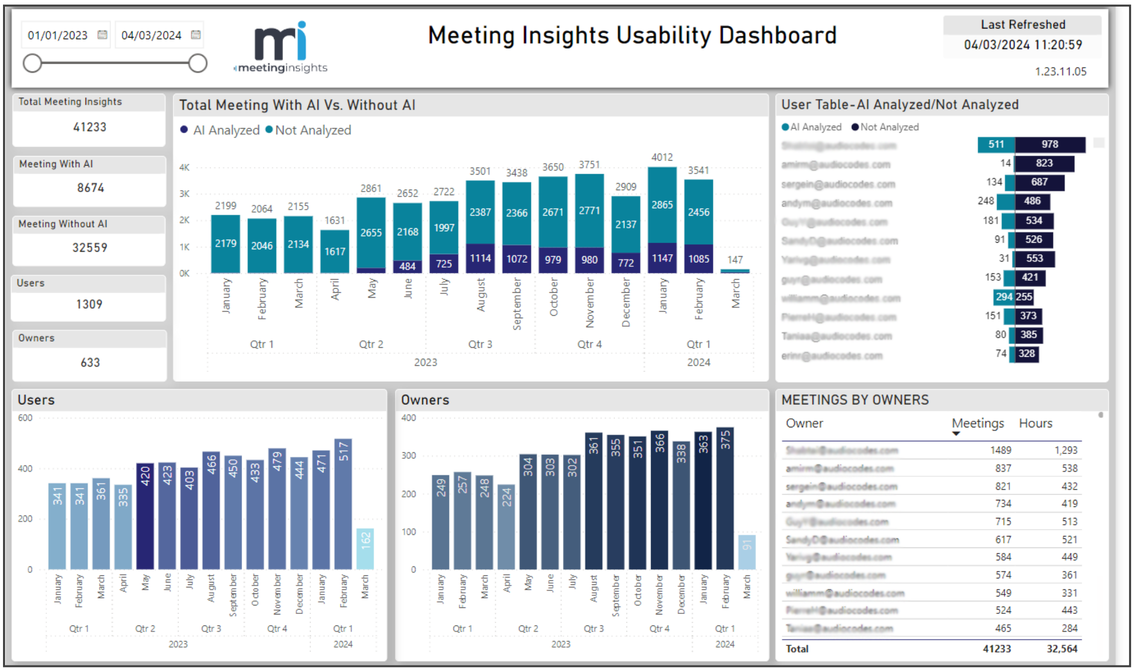


7. Go back to the Workspaces page and click **Refresh now** in the 'Semantic model' item.

Using Reports to Determine Product Usage Statistics

After Meeting Insights is integrated with Microsoft's Power Business Intelligence (BI), administrators and/or management can create business analytics reports showing how and to what extent users in the enterprise are engaging with Meeting Insights and its features.

The figure below shows a **Usability Dashboard** report.



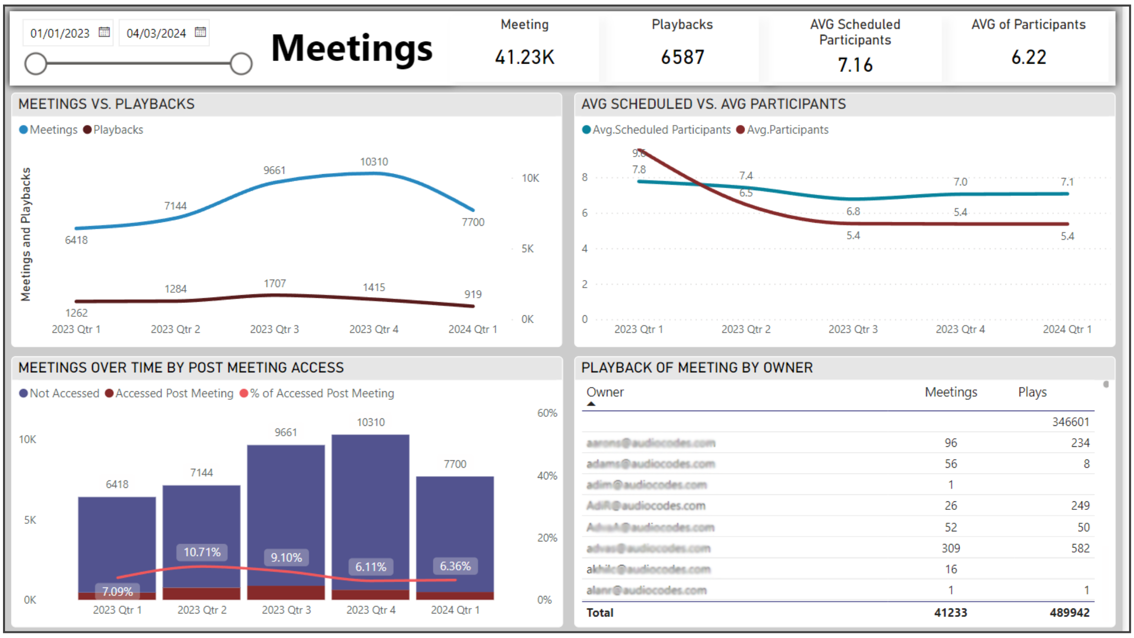
- The **Usability Dashboard** report can give administrators and/or management an indication of the value proposition of Meeting Insights and its key feature, AI.
- The report's statistics and graphs show admin the *extent* to which and the *depth* at which users are using the application and its key feature, AI.
- The report is generated in an admin-friendly Microsoft Power BI template.

[Refer to the preceding figure] Admin can assess at a glance how many meetings with Meeting Insights *in total* were held in the enterprise over a period of time defined in the uppermost left corner of the page. Admin can moreover assess how many of those meetings were analyzed using AI, versus how many were not. Admin can quickly see furthermore how many analyses were run by *users* after meetings, versus how many analyses were run by *owners*.

Admin can view these statistics *per user* in the **User Table-AI Analyzed/Not Analyzed** pane on the right side of the page. The pane presents an ordered list of users, the # of meetings each user had in the defined period, and the # of hours each user spent in meetings.

The **Meetings by Owners** pane below it presents how many meetings *each owner* held and how many hours *each owner* spent in meetings. The pane also shows the *total #* of meetings held by all owners and the *total #* of hours that were spent in meetings by all owners.

The figure below shows a **Meetings** report.



[Refer to the preceding figure] Admin can quickly gauge the *depth* at which users | owners engaged with the product over a period of time defined in the uppermost left corner of the page. The **Meetings vs. Playbacks** graph shows the # of meetings that were held in the organization vs. the # of playbacks that were run. If, for example, the playback feature was hardly taken advantage of (indicated by a significant gap between the Meetings and Playbacks curves as shown in the graph in the preceding figure), this can indicate that users | owners tend to use the product superficially, without playing back meetings. If, by contrast, the playback feature was taken maximum advantage of (the two curves *both* show high usage), it indicates that users | owners took good advantage of it. The graph therefore demonstrates feature effectiveness.

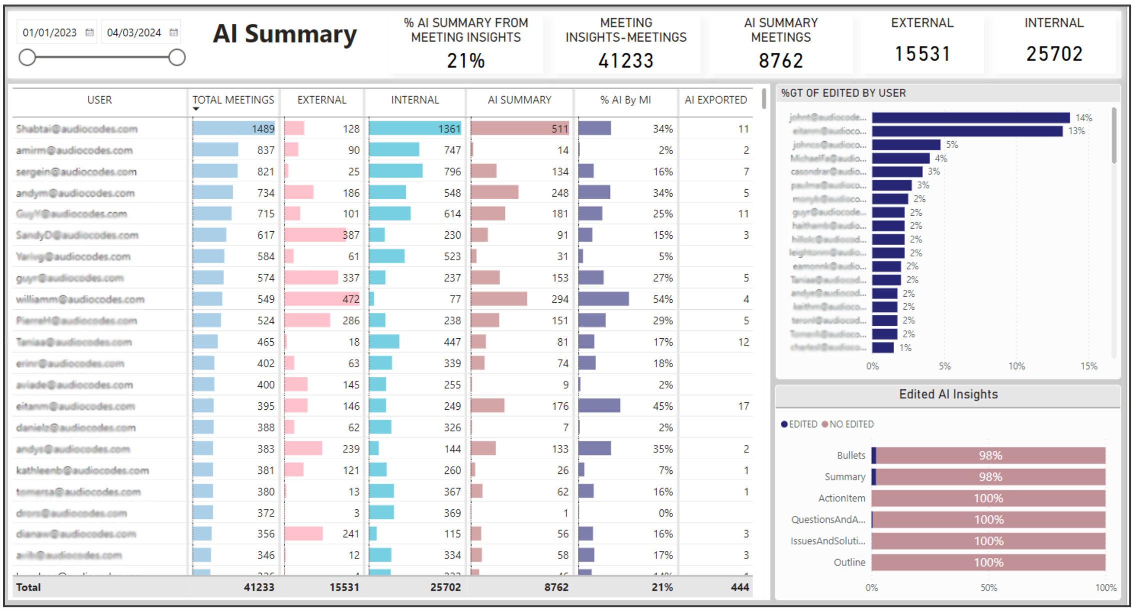
The **Average Scheduled vs. Average Participants** graph shows the # of invitees that were *invited* to meetings vs. the # of invitees that *actively participated* in those meetings. These statistics demonstrate product effectiveness, helping administrators and/or management assess whether they're getting a return (usage) from their investment.

The graph **Meetings over Time by Post Meeting Access** shows admin the # and % of users who accessed recordings of meetings after they ended, over time. This graph too demonstrates product effectiveness and the extent to which users are taking advantage of Meeting Insights' features.

The graph **Playback of Meeting by Owner** shows the extent to which Meeting Insight's *playback* feature was taken advantage of by meeting *owners*. The graph shows the behavior *per owner* as well *all owners in total*. Admin can at a glance determine:

- the # of owners vs. the # of playbacks run by them
- the # of meetings each owner had vs. the # of playbacks run by each

The figure below shows an **AI Summary** report.



[Refer to the preceding figure] Admin can use this report to quickly determine **AI Summary** usage globally and per external | internal user, over a period of time. The report can give administrators and/or management an indication of the benefit Meeting Insights' AI Summary feature is providing the organization.

The report's title bar enables admin to quickly determine *global* statistics for AI Summary (from l-r):

- **% AI Summary from Meeting Insights** shows the % of meetings in which the AI Summary feature was used. In the preceding example, the AI Summary feature was used in 21% of all meetings held during the period.
- **Meeting Insights - Meetings** shows how many Meeting Insights meetings were held over the period. In the preceding example, 41233 meetings were held.
- **AI Summary Meetings** shows for how many Meeting Insights meetings the AI Summary feature was used. In the preceding example, the feature was used for 8762 meetings.
- **External** shows the *# of external meetings* each user had with Meeting Insights over the period. In the preceding example, *all* users had 15531 external meetings with Meeting Insights.
- **Internal** shows the *# of internal meetings* each user had with Meeting Insights over the period. In the preceding example, *all* users had 25702 internal meetings with Meeting Insights.

The report's main pane enables admin to determine AI Summary usage statistics *per user* in the following columns (from l-r):

- **Total Meetings** shows the *total # of meetings* each user had with Meeting Insights over the period. The column can be ordered from most meetings to least meetings, or from least to most. Admin can easily determine which user in the organization had the most meetings using Meeting Insights, and who had the least.

- **External** shows the *# ofexternal meetings* the user had with Meeting Insights. The column can be ordered from most to least, or from least to most. Admin can easily determine which user had the most external meetings with Meeting Insights, and which user had the least.
- **Internal** shows the *# ofinternal meetings* the user had with Meeting Insights. The column can be ordered from most to least, or from least to most. Admin can easily determine which user had the most internal meetings, and which user the least.
- **AI Summary** shows the # of meetings for which AI was triggered (relative to the total # of meetings that were held over the period).
- **% AI by MI** shows the % of meetings for which an AI Summary was generated, per user. Admin can use the statistic to determine the extent to which each user used the feature over the period.
- **AI Exported** shows how many times AI was exported over the period by anyone who had access.

- Each column also displays *global usage*.
  - ✓ **% AI by MI** column displays the *total percentage*.
  - ✓ All other columns display the *total number*.

The report's **%GT of Edited by User** pane enables admin to determine per user the % of edits they performed relative to the number of meetings they had. This too can serve as an indication of the:

- extent to which and depth at which each user is engaging with the app's edit feature
- app's value proposition in terms of the edit feature
- app's ROI in terms of the edit feature
- benefit the organization is deriving from the service

The report's **Edited AI Insights** pane enables admin to determine editing patterns. In the preceding example, 2% of edits were made on bullets and 2% on the summary. Action Items, for example, were not edited at all. These patterns too can serve as an indication of the:

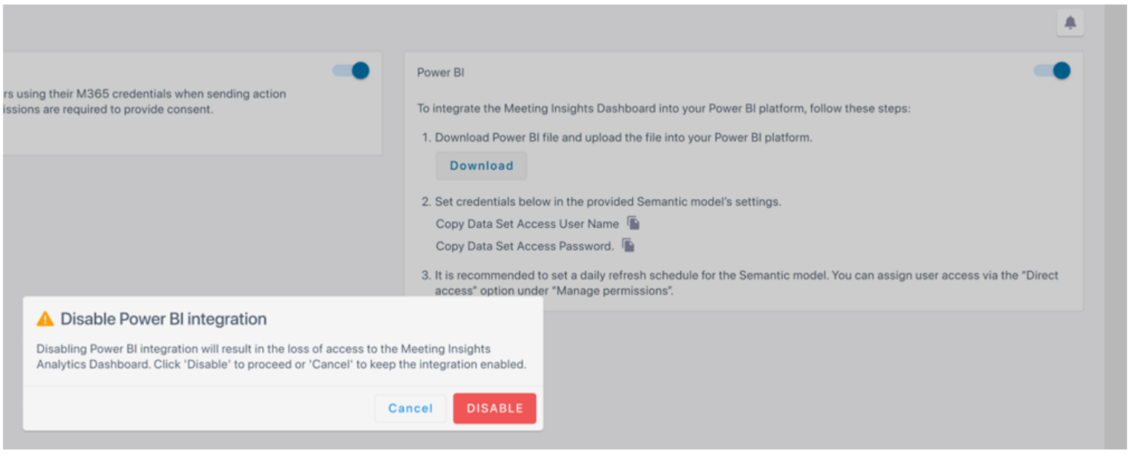
- extent to which and depth at which users are engaging with the app
- app's value proposition
- app's ROI
- benefit the organization derives from the service

Disabling Power BI Integration

Admin can optionally disable Microsoft's Power Business Intelligence (BI) Analytics in Meeting Insights.

➢ To disable Power BI in Meeting Insights:

1. In Meeting Insights, open the Integrations page.
2. Slide the Power BI switch to OFF; the following notification is displayed:



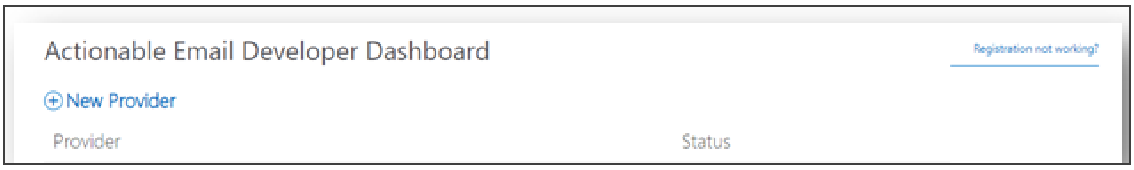
3. Click **DISABLE**.

17 Enabling Actionable Recap Emails

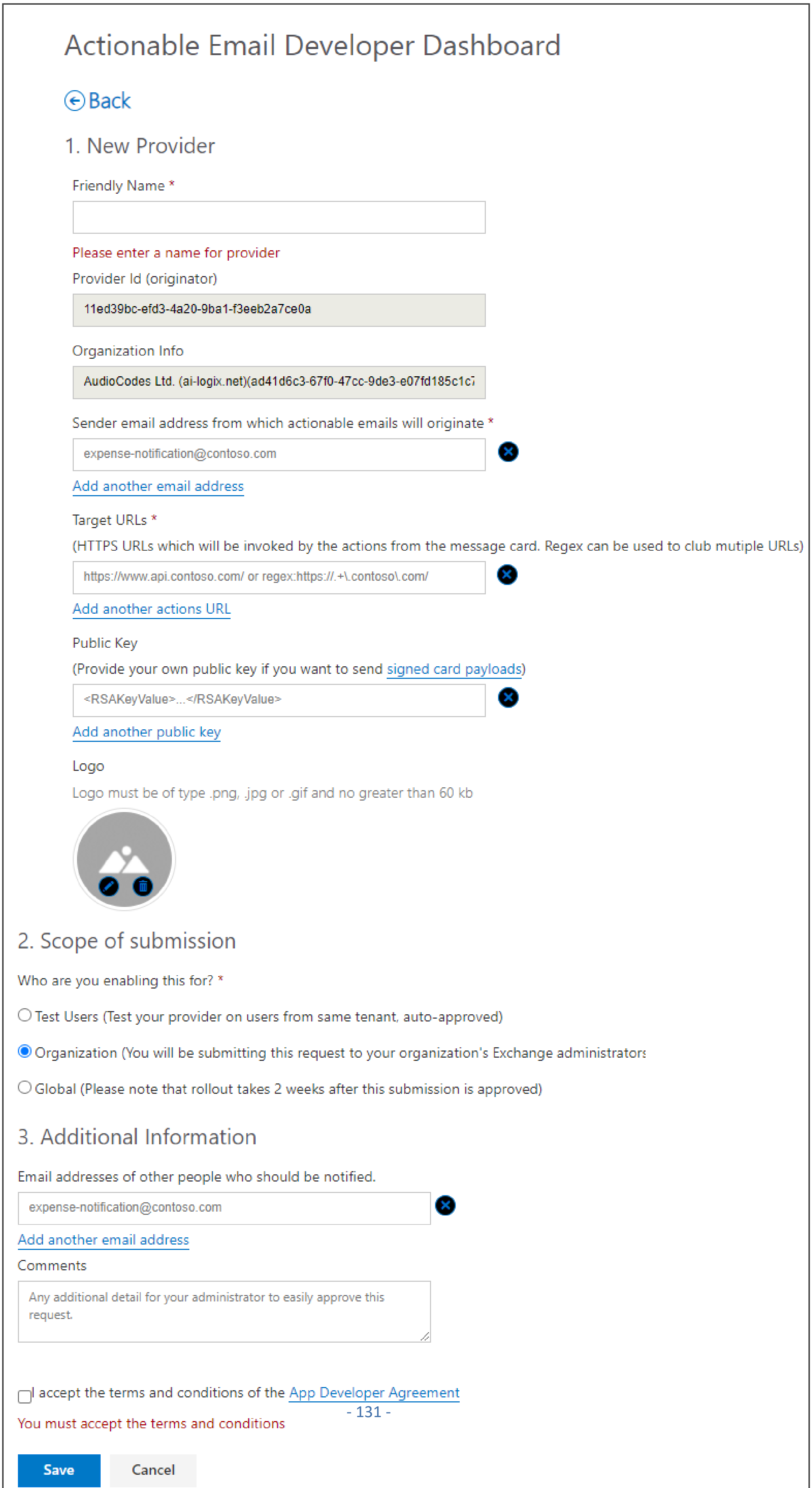
Admins can enable recipients of Action Items emails to set the status to "Done" in the email (by clicking the **DONE** button) by creating a new Outlook Office provider.

➢ To create a new Outlook Office provider:

1. Go to https://aka.ms/publishoam.
2. Log in with the Teams Tenant admin that belongs to the same Tenant as the users to whom the meeting recordings will be sent; the following appears:



3. Click **New Provider**; the following appears:


Actionable Email Developer Dashboard
Back
1. New Provider
Friendly Name *
Please enter a name for provider
Provider Id (originator)
11ed39bc-efd3-4a20-9ba1-f3eeb2a7ce0a
Organization Info
AudioCodes Ltd. (ai-logix.net)(ad41d6c3-67f0-47cc-9de3-e07fd185c1c7
Sender email address from which actionable emails will originate *
expense-notification@contoso.com
Add another email address
Target URLs *
(HTTPS URLs which will be invoked by the actions from the message card. Regex can be used to club mutiple URLs)
https://www.api.contoso.com/ or regex:https://.+\.contoso\.com/
Add another actions URL
Public Key
(Provide your own public key if you want to send signed card payloads)
<RSAKeyValue>...</RSAKeyValue>
Add another public key
Logo
Logo must be of type .png, .jpg or .gif and no greater than 60 kb
2. Scope of submission
Who are you enabling this for? *
Test Users (Test your provider on users from same tenant, auto-approved)
Organization (You will be submitting this request to your organization's Exchange administrators
Global (Please note that rollout takes 2 weeks after this submission is approved)
3. Additional Information
Email addresses of other people who should be notified.
expense-notification@contoso.com
Add another email address
Comments
Any additional detail for your administrator to easily approve this request.
I accept the terms and conditions of the App Developer Agreement
You must accept the terms and conditions
Save
Cancel

4. Under the **New Provider** group, fill in the following fields:
   - 'Friendly Name': Enter any name for the provider (e.g., "be304qf4BE").
   - 'Provider Id': (Read-only) This value is automatically generated. Please provide it to AudioCodes.
   - 'Sender email address from which actionable emails will originate': Enter MIA's email address (provided by AudioCodes) from where Action Items emails will originate.
   - 'Target URLs': Enter the URL (provided by AudioCodes) that is invoked when users click DONE in Action Items emails.
5. Under the **Scope of submission** group, select the **Organization** option.
6. Under the **Additional information** group, enter the email addresses of other people who should be notified, and then type a message for this email notification.
7. Accept the terms of use, and then click **Save**.

18 About Meeting Insights Data Security

> ⚠ Make sure security products in your network (like Firewall) don't interfere with Meeting Insights' correct operation; add the service FQDN and IP address to the appropriate whitelists, to be exempt from scanning and manipulation.

- **Encryption:** At rest (256-bit AES) and at transit (256-bit SSL / TLS 1.2 or later)
- **Authentication:** Microsoft Azure SSO
- **Azure Open AI Data privacy:** No data is used to train LLM (Azure Open AI security)
- **GDPR , CCPA, CPRA:** Compliant
- **Retention policy:** Automatic data retention policy per customer's configuration
- **App user activities:** Audit trail of user activities
- **Development:** Secured software development practices according to OWASP
- **ISO-27001 and ISO27032:** Certified
- **Data security:**
  - Encrypted at rest (disk and storage encryption)
  - Encrypted in transit, HTTPs connections
- **Platform/Hosting security:**
  - Azure subscription following MSFT Security and Compliance recommendation
- **Application security:**
  - Managed identity intercomponent authentication
  - Imperva Incapsula – web application security, DDoS mitigation, and more
- **Authentication:**
  - Azure Active Directory, Teams SSO

This page is intentionally left blank.

International Headquarters

6 Ofra Haza Street

Naimi Park

Or Yehuda, 6032303, Israel

Tel: +972-3-976-4000

Fax: +972-3-976-4040

AudioCodes Inc.

80 Kingsbridge Rd

Piscataway, NJ 08854, USA

Tel: +1-732-469-0880

Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide

Website: https://www.audiocodes.com/

Documentation Feedback: https://online.audiocodes.com/documentation-feedback

Document #: LTRT-12759