

# Next Generation Meeting Insights



## Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from <https://www.audiocodes.com/library/technical-documents>.

This document is subject to change without notice.

Date Published: July-15-2024

## Security Vulnerabilities

All security vulnerabilities should be reported to [vulnerability@audiocodes.com](mailto: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
<a href="#">Meeting Insights User's Manual</a>

## Document Revision Record

LTRT	Description
12726	This is the initial 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.

## Table of Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
	Intended Audience	1
<b>2</b>	<b>Pre-Deployment Requirements</b>	<b>2</b>
<b>3</b>	<b>Signing in</b>	<b>3</b>
<b>4</b>	<b>Setting up Meeting Insights</b>	<b>5</b>
	Connecting to Microsoft 365	5
	Assigning a Meeting Insights License to Users	15
	Synchronizing Meeting Insights Users with AAD	19
	Switching Auto Synch ON OFF	20
	Automatic Synchronization from AAD is ON	20
	Automatic Synchronization from AAD is OFF	21
	Managing Users Assigned to Multiple AAD Groups	22
	Using Notifications to Manage Licenses	24
	Switching from Admin to User Mode, and Back	28
<b>5</b>	<b>Testing your Meeting Insights App</b>	<b>30</b>
<b>6</b>	<b>Recording Teams Live Events or Webinars</b>	<b>34</b>
<b>7</b>	<b>Configuring System Settings</b>	<b>35</b>
	Tools	35
	Adding Meeting Insights to Teams Client	36
	Adding App to Organization's Teams Store via TAC	37
	Adding Meeting Insights to Outlook	41
	Installation Additions	42
	Setting up Outlook Add-In	42
	Storage	47
	Tags	48
	Devices	50
<b>8</b>	<b>Configuring User Settings</b>	<b>51</b>
	User Profiles	51
	Enabling 'Automatic Triggering' in a User Profile	54
	Admin Profiles	56
	Licensed Users	57
	Recording Notifications	58
	Unlicensed Users	63
	Email Notifications	64
<b>9</b>	<b>AI Settings</b>	<b>67</b>
<b>10</b>	<b>Monitoring</b>	<b>69</b>
	Audit Trail	69
	System Activity Log	71



<b>11</b>	<b>Integrations</b>	<b>73</b>
<b>12</b>	<b>Configuring Automatic Invitation of MIA to Teams Meetings</b>	<b>76</b>
	Add a Mail-Enabled Security Group	76
	Configure an Auto-Invite Rule	80
	Test the Rule	86
	Managing the Lobby for Teams Meetings	87
<b>13</b>	<b>Producing Power BI Analytics Usage Reports</b>	<b>88</b>
	Enabling Power BI Integration in Meeting Insights	88
	Installing   Configuring Power BI Analytics	89
	Using Reports to Determine Product Usage Statistics	95
	Disabling Power BI Integration	98
<b>14</b>	<b>Enabling Actionable Recap Emails</b>	<b>100</b>
<b>15</b>	<b>About Meeting Insights Data Security</b>	<b>103</b>

# 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](#).

## 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

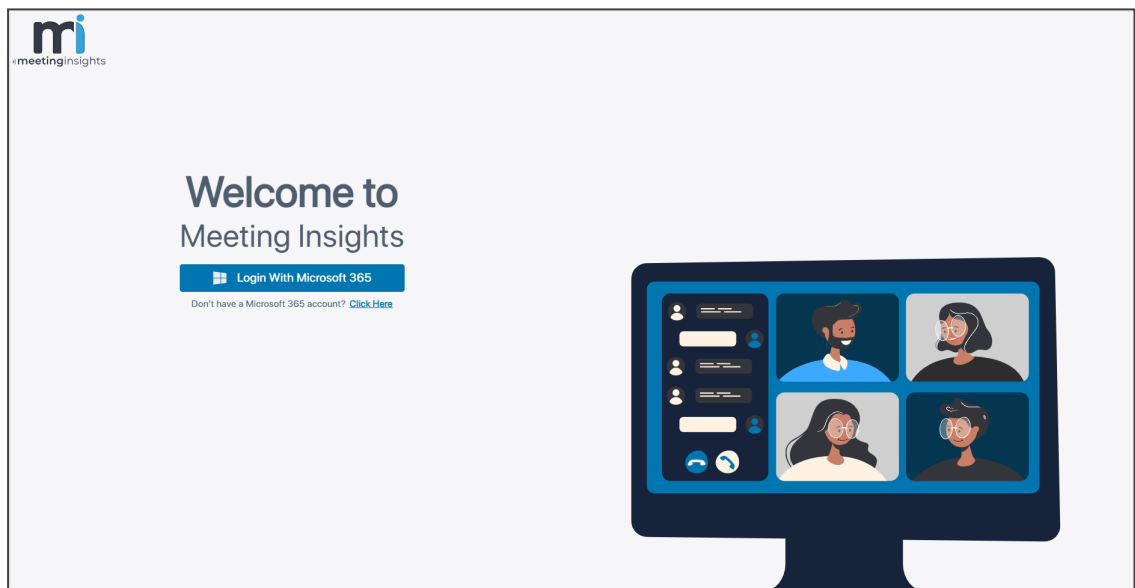
Meeting Insights enables you to sign in as admin. Admin can perform management tasks which regular users cannot. Up to five admins are allowed.









- 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 URL xxx.yyy.com provided by AudioCodes in the email (as shown in the *Live Cloud Meeting Insights for Service Providers Administrator's Guide*) and paste it into your browser's address field.



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

M365 Tenant ID		Meeting Insights Tenant ID	
b6a729e2-5de3-489d-a1e0-e4132367ea85		6fctf081-d758-442d-953a-46d8c083c8d2	
CONSENT NAME	ACTION	COMPLETED	DESCRIPTION
M365 Login	<a href="#">Grant Admin Consent</a> >		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	<a href="#">Grant Admin Consent</a> >		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	<a href="#">Grant Admin Consent</a> >		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	<a href="#">Publish</a> >		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	<a href="#">Download Script</a> 		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

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

➤ **To connect to Microsoft 365:**

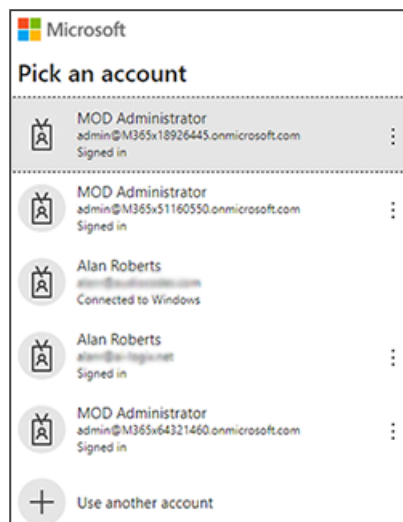
1. After signing in, the 'Connect to your M365' page is displayed (**Admin Settings > System Settings**).

M365 Tenant ID b6a729c2-5de3-489d-a1e0-e4132367ea85		Meeting Insights Tenant ID 6fctf081-d758-442d-953a-46d8c083c8d2	
CONSENT NAME	ACTION	COMPLETED	DESCRIPTION
M365 Login	<a href="#">Grant Admin Consent</a> ➤	❌	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	<a href="#">Grant Admin Consent</a> ➤	❌	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	<a href="#">Grant Admin Consent</a> ➤	❌	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	<a href="#">Publish</a> ➤	❌	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	<a href="#">Download Script</a> 📄	❌	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

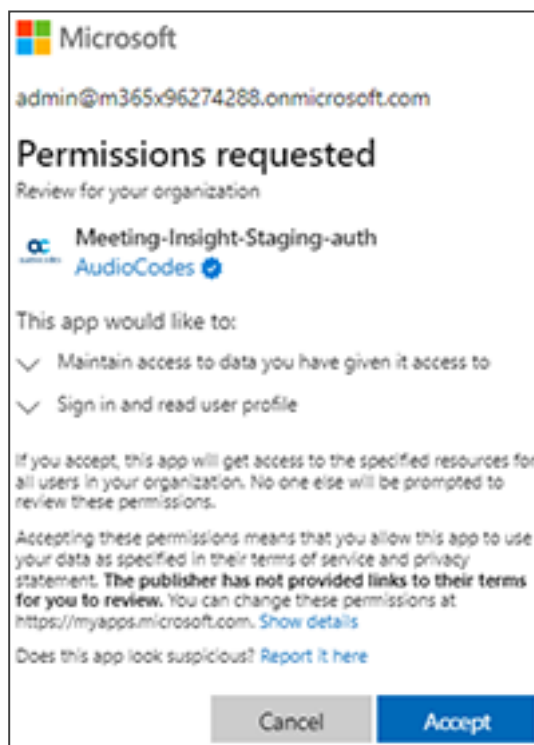


- Under the 'Completed' column, the icons  indicate consent has not been granted yet and must be granted.
- The first consent is hyper linked indicating that this consent must be granted first.
- **Microsoft 365 Administrator permissions are required to grant each consent.**

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**.

M365 Tenant ID b6a729c2-5de3-489d-a1e0-e4132367ea85		Meeting Insights Tenant ID 6fcff081-d758-442d-953a-46d8c083c8d2	
CONSENT NAME	ACTION	COMPLETED	DESCRIPTION
M365 Login	<a href="#">Grant Admin Consent &gt;</a>		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	<a href="#">Grant Admin Consent &gt;</a>		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	<a href="#">Grant Admin Consent &gt;</a>		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	<a href="#">Publish &gt;</a>		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	<a href="#">Download Script &gt;</a>		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

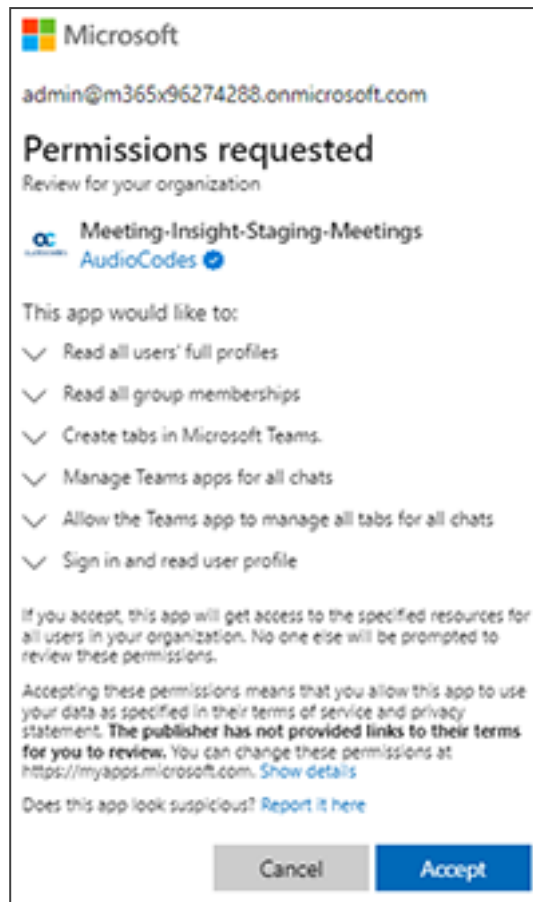
5. View the icon under the 'Completed' column. It indicates you successfully granted consent (consent was successfully completed from this page for 'M365 Login'). You've successfully provided the app permission to authenticate users with your M365 credentials; the app reroutes users to M365 for authentication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



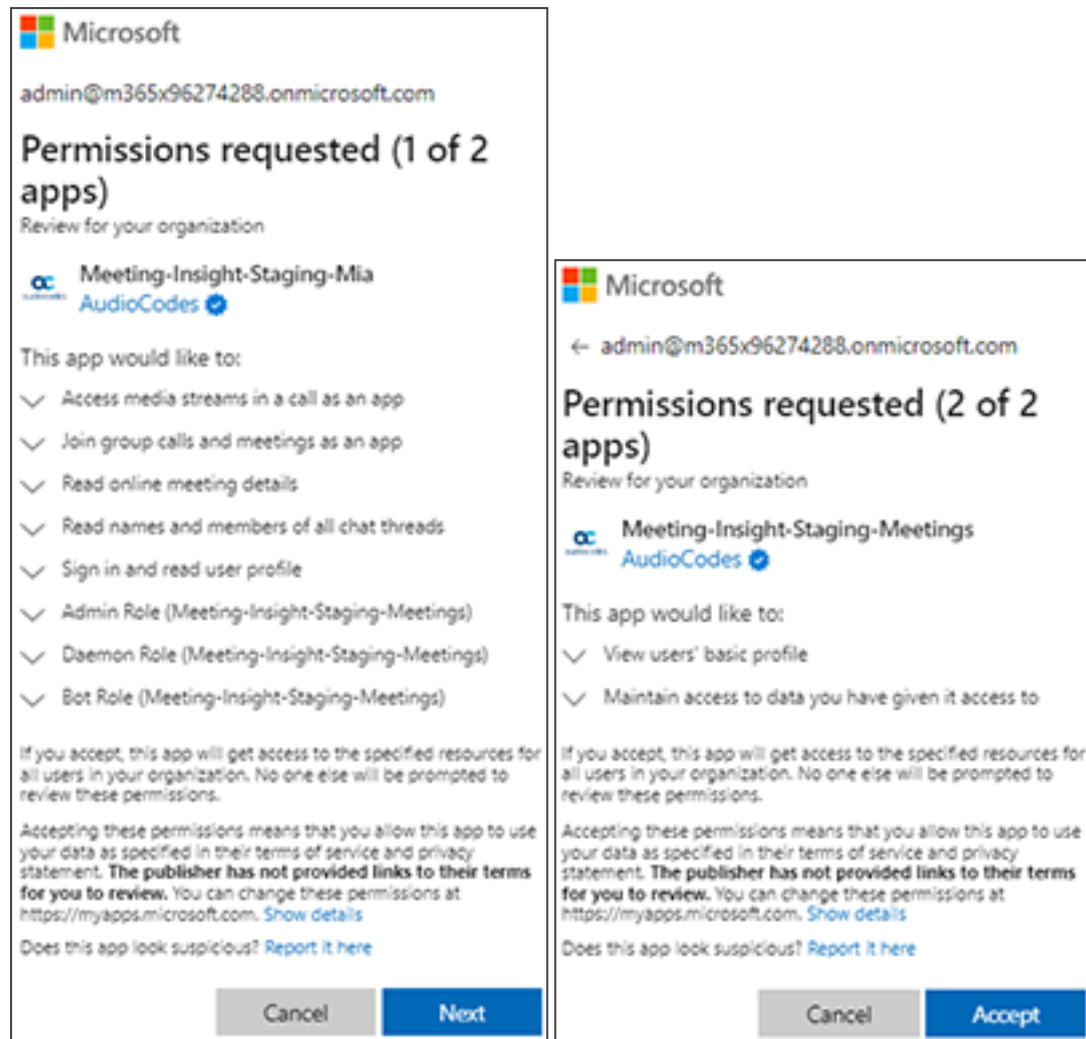


This consent provides the app with permission to read AAD groups and users, and permission for groups' users to access the app and record.

## 7. Click Accept.

M365 Tenant ID b6a729c2-5de3-489d-a1e0-e4132367ea85		Meeting Insights Tenant ID 6fcf081-d758-442d-953a-46d8c083c8d2	
CONSENT NAME	ACTION	COMPLETED	DESCRIPTION
M365 Login	<a href="#">Grant Admin Consent &gt;</a>	✓	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	<a href="#">Grant Admin Consent &gt;</a>	✓	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	<a href="#">Grant Admin Consent &gt;</a>	✗	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	<a href="#">Publish &gt;</a>	✗	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	<a href="#">Download Script</a>	✗	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

## 8. Next to the consent 'Allow Meeting Insights to Join Meetings', click **Grant Admin Consent**.



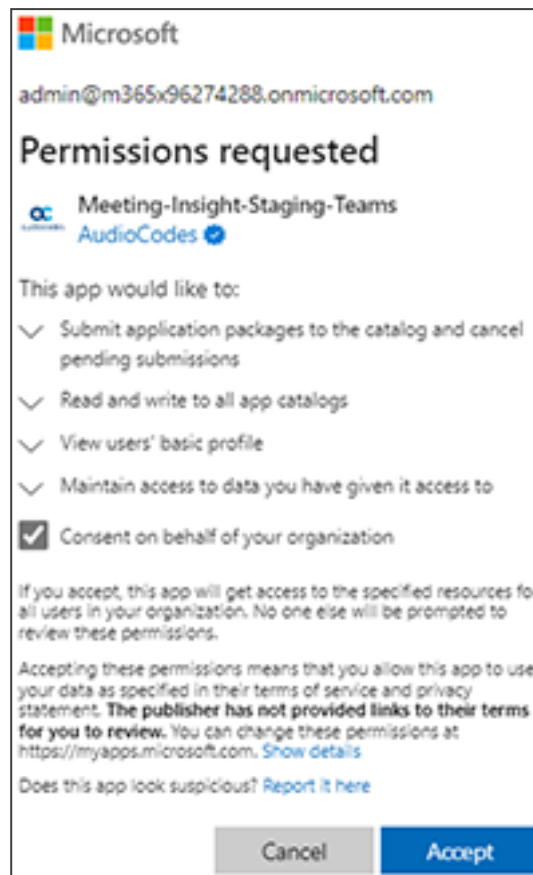
9. Click **Next** and then **Accept**.



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

M365 Tenant ID		Meeting Insights Tenant ID	
b6a729c2-5de3-489d-ate0-e4132367ea85		6fcf081-d758-442d-953a-46d8c083cd2	
CONSENT NAME	ACTION	COMPLETED	DESCRIPTION
M365 Login	<a href="#">Grant Admin Consent &gt;</a>	✔	Provide the application permissions to authenticate users with your M365 credentials, application routes 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	<a href="#">Grant Admin Consent &gt;</a>	✔	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	<a href="#">Grant Admin Consent &gt;</a>	✔	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	<a href="#">Publish &gt;</a>	✘	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	<a href="#">Download Script &gt;</a>	✘	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

10. 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.



11. 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 b6a729c2-5de3-489d-a1e0-e4132367ea85		Meeting Insights Tenant ID 6fcf081-d758-442d-953a-46d8c083c8d2	
CONSENT NAME	ACTION	COMPLETED	DESCRIPTION
M365 Login	<a href="#">Grant Admin Consent &gt;</a>	✔	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	<a href="#">Grant Admin Consent &gt;</a>	✔	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	<a href="#">Grant Admin Consent &gt;</a>	✔	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	<a href="#">Publish &gt;</a>	✔	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	<a href="#">Download Script &gt;</a>	✖	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



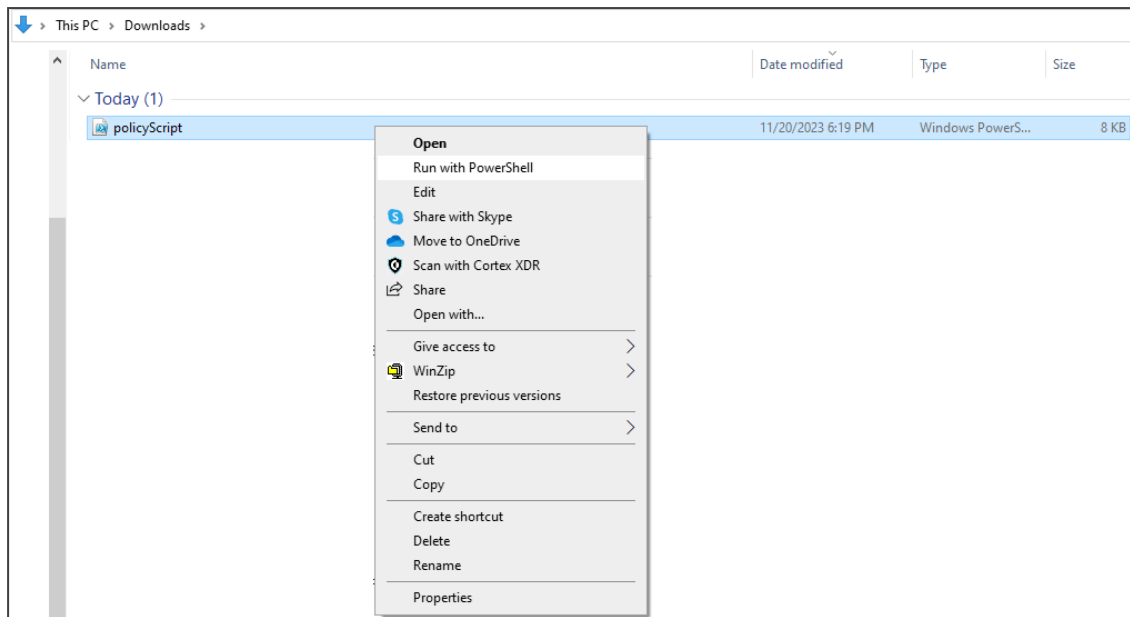
In addition to the icon ✔ under the 'Completed' column indicating you successfully granted consent (consent was successfully completed from this page for 'Publishing Meeting Insights Teams Client App in your Teams Store'), the notification **Application published in your Teams store successfully** is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

12. [Recommended] Install and pin the application for Meeting Insights users as shown [here](#).

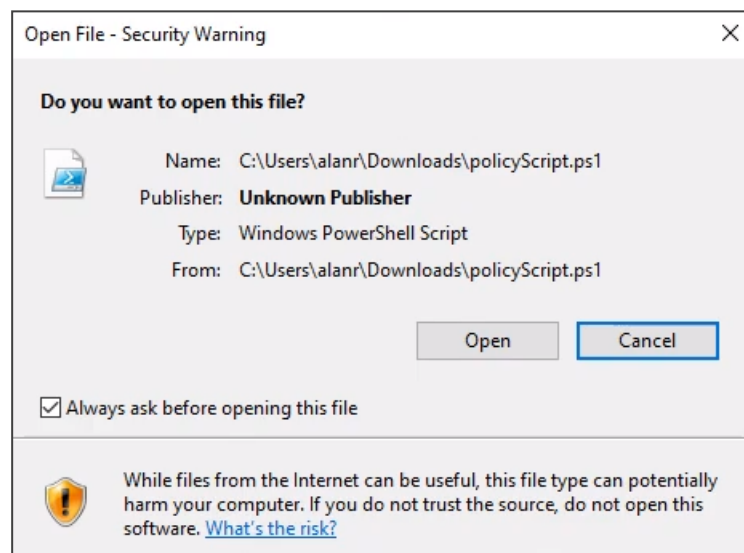
13. Next to the consent 'Allow Meeting Insights to be Added to Ongoing Meetings', click **Download Script**; the 'policyScript' file is downloaded to your PC.



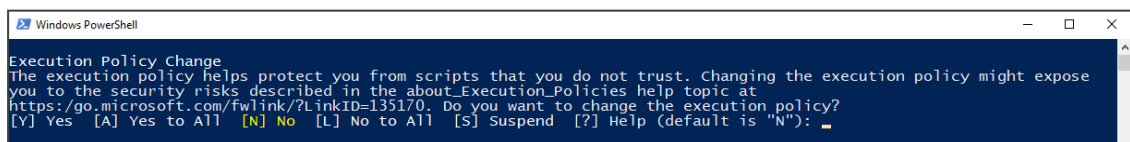
- **PowerShell must be installed on the PC and the PC must have an unrestricted execution policy for the Microsoft 365 admin to run the downloaded script.**
- Before running the downloaded script file, unblock it as the OS may block it. To unblock it, right-click the file and select **Properties**. If 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`



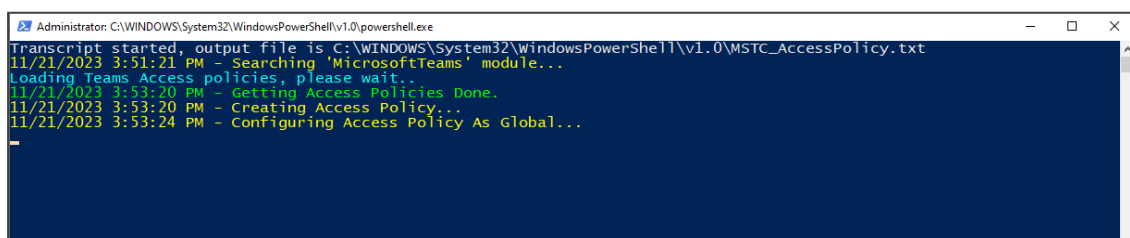
- a. Right-click the file and select **Run with PowerShell**.



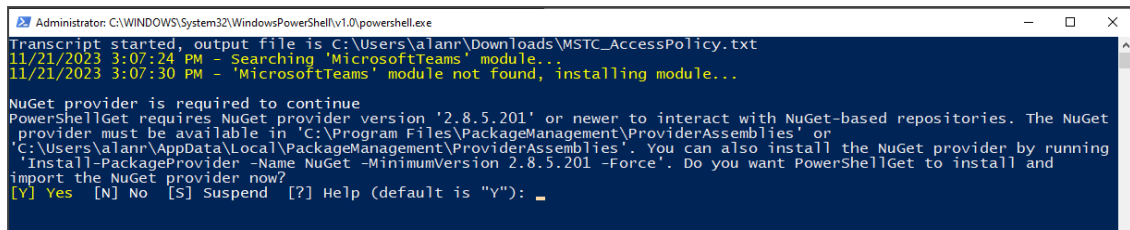
- b. Click **Open**. PowerShell opens.



- 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.



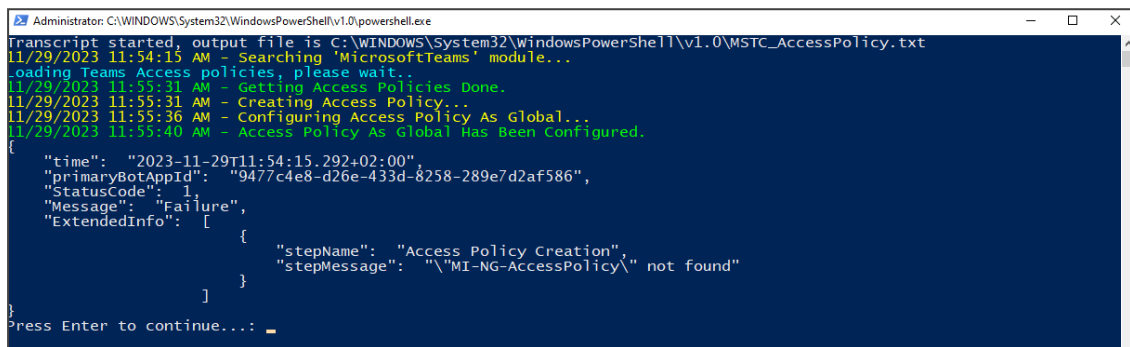
- d. Type in **Y** (Yes) if the prompt below is displayed (it isn't always displayed), and enter.



```
Administrator: C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe
Transcript started, output file is C:\Users\alanr\Downloads\MSTC_AccessPolicy.txt
11/21/2023 3:07:24 PM - Searching 'MicrosoftTeams' module...
11/21/2023 3:07:30 PM - 'MicrosoftTeams' module not found, installing module...

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\alanr\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by running
'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install and
import the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): _
```

- e. Press Enter to continue...



```
Administrator: C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe
Transcript started, output file is C:\WINDOWS\System32\WindowsPowerShell\v1.0\MSTC_AccessPolicy.txt
11/29/2023 11:54:15 AM - Searching 'MicrosoftTeams' module...
Loading Teams Access policies, please wait...
11/29/2023 11:55:31 AM - Getting Access Policies Done.
11/29/2023 11:55:31 AM - Creating Access Policy...
11/29/2023 11:55:36 AM - Configuring Access Policy As Global...
11/29/2023 11:55:40 AM - Access Policy As Global Has Been Configured.
{
  "time": "2023-11-29T11:54:15.292+02:00",
  "primaryBotAppId": "9477c4e8-d26e-433d-8258-289e7d2af586",
  "statusCode": 1,
  "message": "Failure",
  "extendedInfo": [
    {
      "stepName": "Access Policy Creation",
      "stepMessage": "\\MI-NG-AccessPolicy\" not found"
    }
  ]
}
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	<a href="#">Grant Admin Consent &gt;</a>	✓	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	<a href="#">Grant Admin Consent &gt;</a>	✓	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	<a href="#">Grant Admin Consent &gt;</a>	✓	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	<a href="#">Publish &gt;</a>	✓	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	<a href="#">Download Script &gt;</a>	✓	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 table below shows who has permission to perform what actions for highlights, bookmarks, snippets, etc.

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

	Actions	Admin	Owner	Delegate	Auto Can Edit	Participant
<b>Recap</b>	Add	√	√	√	√	X
	Edit	√	√	√	√	X
	Delete	√	√	√	√	X
	View	√	√	√	√	√
	AI trigger	√	√	√	√	If everyone can trigger, enabled by admin
<b>Transcription</b>	Edit	√	√	√	√	X
	Delete	√	√	√	√	X
	View	√	√	√	√	√
	Trigger	√	√	√	√	If everyone can trigger, enabled by admin
<b>Delete</b>		√	√	√	√	X
<b>Download</b>		√	√	√	√	X
<b>Meeting info</b>	Edit	√	√	√	√	X
	View	√	√	√	√	√



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.

## Assigning a Meeting Insights License to Users

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



**Prerequisite**

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

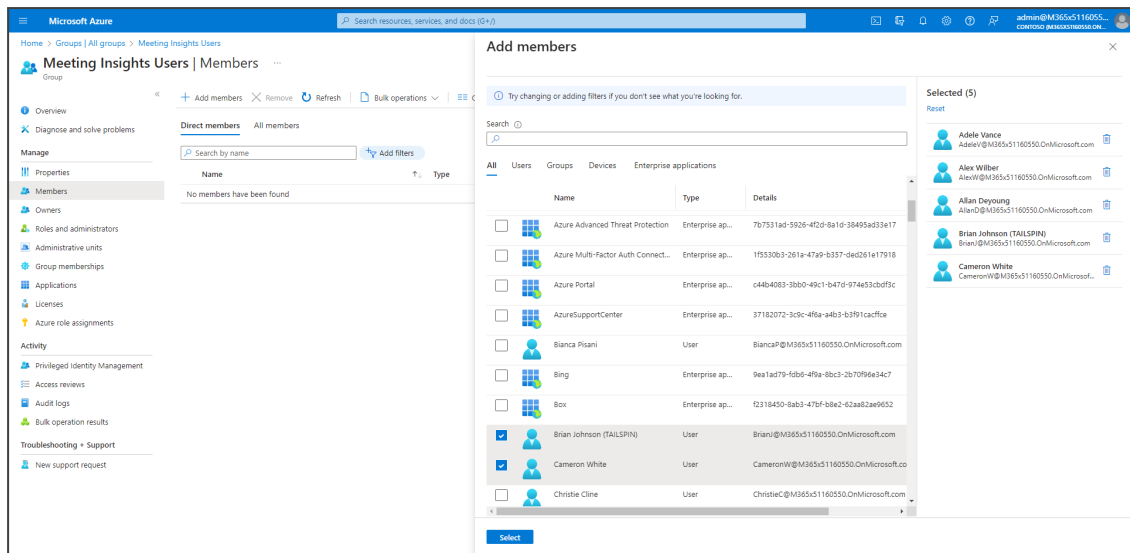
➤ **To define a group of users in AAD:**

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

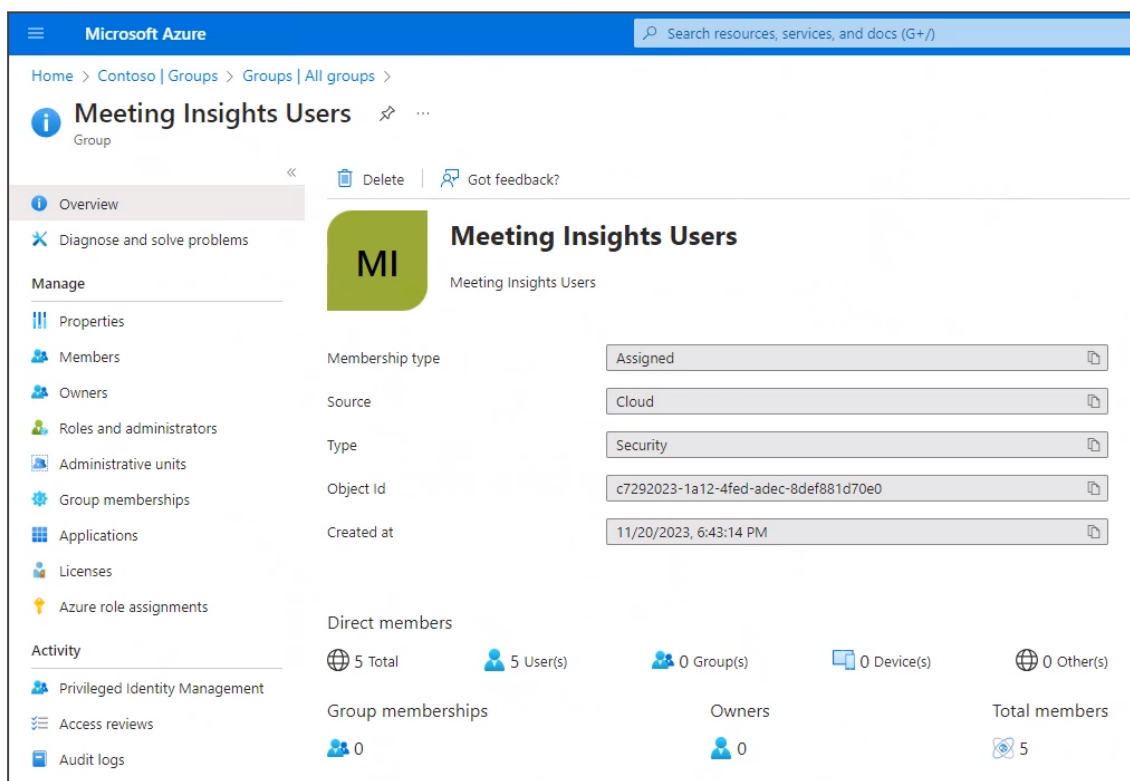
The screenshot shows the 'New Group' page in the Microsoft Azure portal. The page has a blue header with the 'Microsoft Azure' logo and a search bar. Below the header, there's a breadcrumb trail: 'Home > Groups | All groups >'. The main title is 'New Group'. Below the title, there's a 'Got feedback?' link. The form contains the following fields and options:

- Group type \***: A dropdown menu with 'Security' selected.
- Group name \***: A text input field with the placeholder 'Enter the name of the group'.
- Group description**: A text input field with the placeholder 'Enter a description for the group'.
- Microsoft Entra roles can be assigned to the group**: Two radio buttons, 'Yes' and 'No', with 'No' selected.
- Membership type \***: A dropdown menu with 'Assigned' selected.
- Owners**: A section with the text 'No owners selected'.
- Members**: A section with the text 'No members selected'.

3. [Strongly recommended] Define the group name as **Meeting Insights Users**.
4. Select members (i.e., users or groups) to assign to the group.

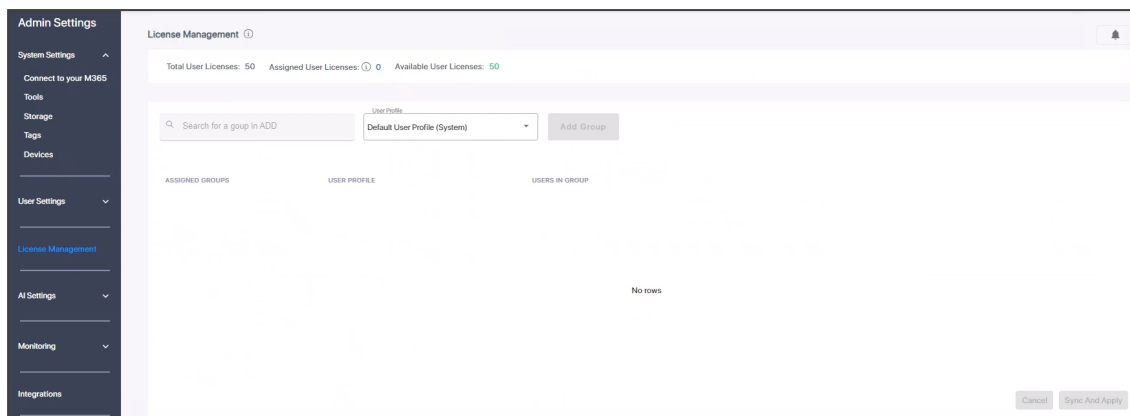


## 5. View the group details in Microsoft Azure portal.

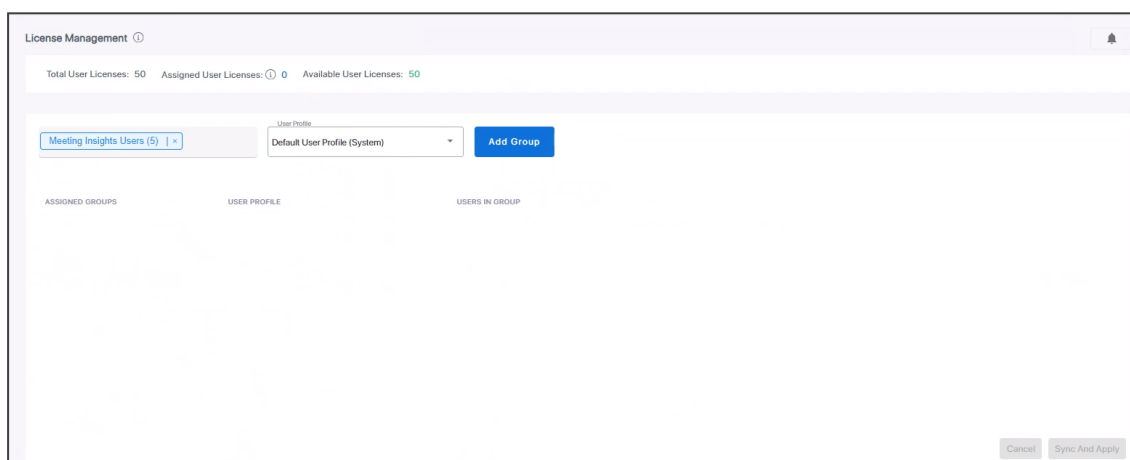


## ➤ To assign a license to the group:

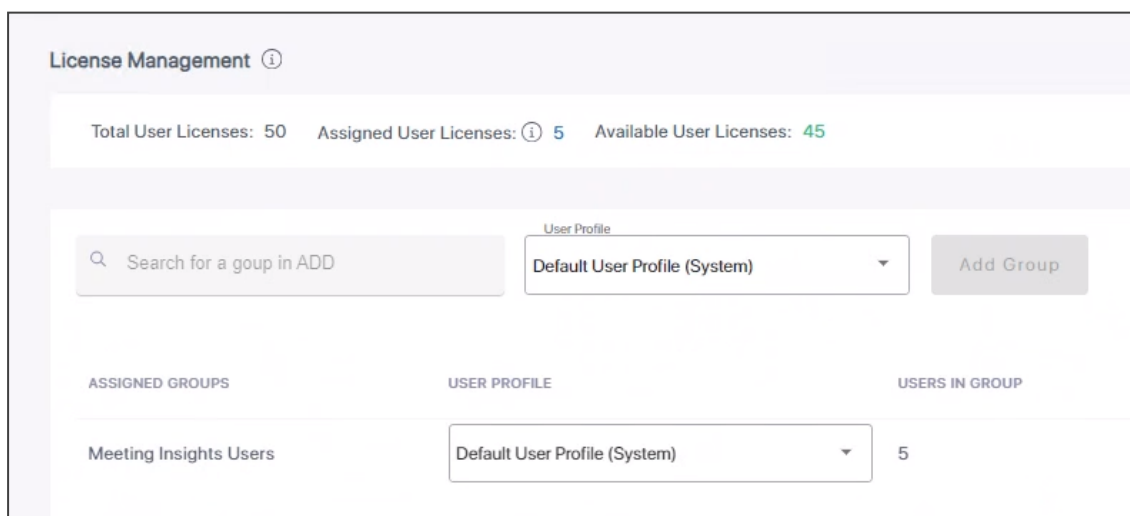
1. In Meeting Insights, click the **License Management** menu.



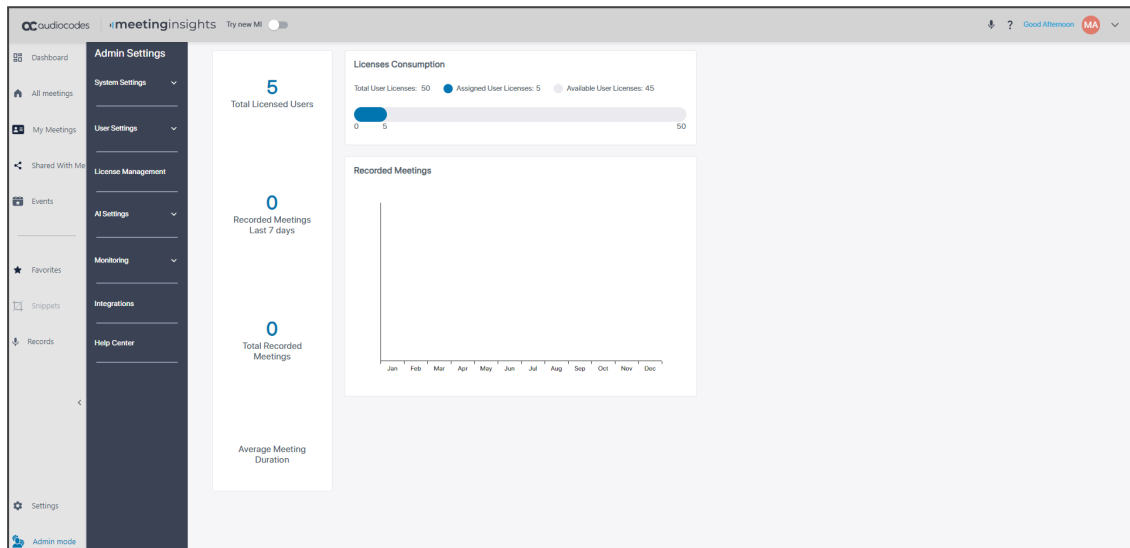
2. In the 'Search for a group in AAD' field, enter the first letters of the name of the group you defined in the previous procedure; the field is auto-populated, i.e., **Meeting Insights Users (5)**. Wait a few seconds for AAD to populate the field.



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**; a Meeting Insights license is assigned to the group; the users in the group can go ahead and use the app.



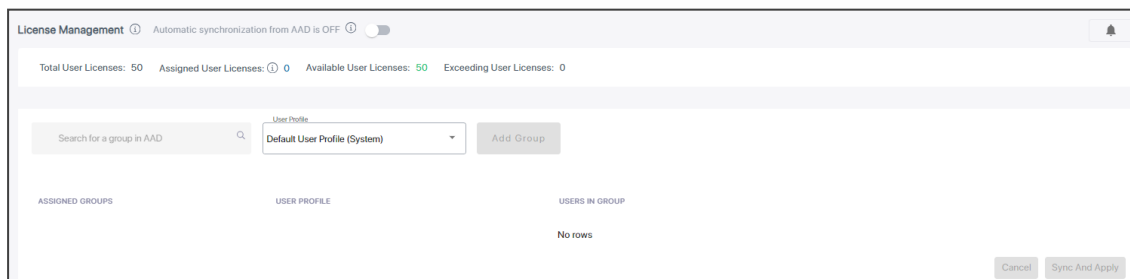
5. View the license assignment displayed uppermost in the License Management page. In the example shown in the preceding figure:
  - Total User Licenses: 50
  - Assigned User Licenses: 5
  - Available User Licenses: 45
6. [Optionally] View this information as well as usage on the Dashboard (Licenses 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.

## Synchronizing Meeting Insights Users with AAD

After configuring in Azure Active Directory a group of users that will have access to Meeting Insights and after assigning a license to the group, synchronize Meeting Insights users with AAD using the License Management page.



'Exceeding User Licenses' and the toggle shown in figure are displayed when the customer is allowed to exceed the purchased number of users.

Two modes of syncing Meeting Insights users with AAD are available:

- **Automatic.** When Meeting Insights has been allowed to exceed user numbers, the License Management page displays a toggle at the top of the page **Automatic Synchronization from AAD** that allows the admin to enable the app to automatically synchronize with users from AAD in the background. Note that a change in Azure AD can take up to five minutes to propagate into Meeting Insights but in some (rare) scenarios it can take up to 10 minutes due to internal processing of the Meeting Insights service.
- **Manual.** Admin can manually synchronizes users from AAD when **Automatic Synchronization from AAD is OFF** by clicking the **Sync and Apply** button in the License Management page. Changes in AAD will not be reflected in Meeting Insights until admin clicks the **Sync and Apply** button.

See [Automatic Synchronization from AAD is ON](#)

See [Automatic Synchronization from AAD is OFF](#)

## Switching Auto Synch ON|OFF



The License Management page displays the 'Automatic synchronization from AAD' toggle only if the customer is allowed to exceed the purchased number of users. See [here](#) for more information.

### ➤ To switch on 'Automatic synchronization from AAD':

1. Create a group in AAD and then in the License Management page, locate it, assign it a User Profile from the drop-down, and then click **Add Group**; the group is added to the page.
2. Click the 'Automatic synchronization from AAD is OFF' toggle; you're prompted 'Are you sure you want to enable Automatic Synchronization from AAD?'
3. Click YES I'M SURE; 'Automatic synchronization from AAD' is switched ON.



The system immediately synchronizes users from mapped groups and continues synchronization in the background.

4. Click the **x** in the upper right corner to close notifications.

## Automatic Synchronization from AAD is ON



The License Management page displays the 'Automatic synchronization from AAD' toggle only if the tenant is allowed to exceed the purchased number of users. See [here](#) for more details.

When 'Automatic synchronization from AAD' is displayed in the License Management page and is switched **ON**:

1. Locate a group that you created in AAD, assign the group a User Profile from the drop-down, and then click **Add Group**; the group is added to the page and the **Apply** button is activated.



- Only **Apply** is displayed because synchronization with AAD is automatically performed in the background.
- **Sync and Apply** is displayed when the toggle is not displayed and is **OFF** as described [here](#).

2. Click the **Apply** button; you're notified how many new users are assigned with the license and how many users exceed the number of available licenses; you're also reminded that if a change is made in an AAD group mapped to the application, you need to click the **Sync and Apply** button for the change to take effect in Meeting Insights.
3. Click the **x** in the upper right corner to close each notification.

### Automatic Synchronization from AAD is OFF



- A new tenant that is allowed to exceed licenses is deployed with 'Automatic Synchronization from AAD' switched to **ON**.
- The 'License Management' page displays the toggle and 'Exceeding User Licenses' only if the customer is allowed to exceed the purchased number of users. See related information [here](#).

When the 'Automatic synchronization from AAD' toggle is not displayed in the License Management page -OR- when it's displayed but is switched **OFF**:

1. Locate a group you created in AAD, assign it a User Profile and then click **Add Group**; the group is added to the page and the **Sync and Apply** button is activated.



- **Sync and Apply** is displayed when the toggle is not displayed or when it is displayed but is **OFF**; synchronization with AAD is performed manually.
- **Apply** is displayed when the toggle is displayed and is **ON**; synchronization with AAD is automatically performed in the background.

2. Click the **Sync and Apply** button; you're notified how many new users have been assigned the license | by how many users the number of available licenses has been exceeded. You may also be notified that if you make a change in an AAD group mapped to Meeting Insights, you need to click **Sync and Apply** for the change to take effect in the app.



Each time **Sync and Apply** is used, Meeting Insights also syncs all mapped groups from Azure AD.

3. Click the **x** in the upper right corner to close notifications.

## Managing Users Assigned to Multiple AAD Groups

In multifaceted corporations users are frequently assigned to multiple AAD user groups. It's recommended to create AAD groups explicitly for Meeting Insights, for setting permissions in Meeting Insights, and to add users or user groups to these Meeting Insights groups if necessary, for example:

- 'Meeting Insights Users'
- 'Meeting Insights Users with External Share'

Corporations can typically have more than 1000 user groups, so by way of example, you can create the following user groups:

- 'Meeting Insights Users' - all users/groups that should have access/license to Meeting Insights
- 'Meeting Insights Users with External Share' - all users/groups that should have permissions to share meetings externally
- 'Meeting Insights Users with Auto AI' - all users/groups that should have Auto AI enabled

### ➤ To manage user(s) assigned to multiple AAD groups:

1. Locate a group that you created in AAD, assign the group a User Profile from the drop-down, and then click **Add Group**.
2. View a notification if user(s) are assigned to multiple AAD groups.



#### Recommended

- Read the notification.
- If users are assigned to multiple AAD groups, each associated with different User Profiles having varying storage or retention settings, the longest retention policy will be applied, and storage locations may be assigned arbitrarily.
- Make sure every user belongs to a single AAD group mapped to Meeting Insights.

3. Click the link **See full list of users >**

NAME	AAD GROUPS	USER PROFILES
ST-Teams100	sub_group_1, basic_group, team-1	retention 90, Default User Profile (System)
	sub_group_1, basic_group	Default User Profile (System), retention 90
	sub_group_1, basic_group	Default User Profile (System), retention 90
Z_ST-Teams261	sub_group_2, sub_group_1, basic_group	retention 90, test-retention 180, Default User Profile (System)
Z_ST-Teams1000	sub_group_2, sub_group_1, basic_group	retention 90, test-retention 180, Default User Profile (System)
MI-Teams01	sub_group_2, basic_group, sub_group_1	Default User Profile (System), retention 90, test-retention 180
MI-Teams03	sub_group_2, basic_group, sub_group_1	Default User Profile (System), retention 90, test-retention 180
Z_ST-Teams1198	sub_group_2, basic_group, sub_group_1	Default User Profile (System), retention 90, test-retention 180
disable_user2	sub_group_2, basic_group, sub_group_1	Default User Profile (System), retention 90, test-retention 180
auto-short-name-100010	basic_group, sub_group_1	Default User Profile (System), retention 90
<a href="#">And 4 more users.</a>		

4. View the users in the groups, which groups apply, and the assigned User Profiles.



#### Recommended

- Read notifications if displayed.
- Make sure every user belongs to a single AAD group mapped to Meeting Insights.
- Meeting Insights doesn't prevent the option of a user being in multiple groups but when the 'Meeting Recordings Retention Period' field (see the figure below) is different between one and another, the period that is *longer* is applied by default.
- For example: If a user in a group has a 'Meeting Recordings Retention Period' of one year but the same user has a period of two years in another group (two different User Profiles assigned to each group), Meeting Insights gives the user a two-year Retention Period.



**User Profile Name:** Default User Profile (System)

**Description:** This profile is a default profile that includes user access to

**Permissions:** Select permissions that users associated with the profile will have

- ☐ Access User Meetings ⓘ
- ☐ External Restricted Share
- ☐ External Share with a Link
- ☐ Premium Transcription
- ☐ Can Edit Other Users Meetings

**Recording:** Enable recording options ☒ Enable

**Meeting Types:**

- ☒ User Meetings
- ☒ Import Meeting Recordings

**Select Storage:** Europe GRS

**Meeting Recordings Retention Period:** 1 Year

☐ Allow Users to Extend Recordings Retention

**Buttons:** Cancel, Apply

## Using Notifications to Manage Licenses

Admin can use notifications displayed in the License Management page to manage licenses more efficiently.

### ➤ To use notifications to manage licenses:

1. Click the bell icon  located in the top right corner of the page.



- Notifications generated *during the last admin login* are displayed under the bell.
- To view *all notifications*, click the **System Activity Logs** option under the 'Monitoring' menu.

**License Management** ⓘ Automatic synchronization from AAD is ON ⓘ ☒

Total User Licenses: 100 Assigned User Licenses: 152 Available User Licenses: 0 Exceeding User Licenses: 52

**ASSIGNED GROUPS**

ASSIGNED GROUPS	USER PROFILE	USERS IN GROUP
LMgroup	Default User Profile (System)	110
member_is_group	Default User Profile (System)	0
yehudiTest	test-retention 180	1
team-1	Default User Profile (System)	2

**Recent Activities**

- Some users are assigned to multiple AAD groups, each associated with different User Profiles having distinct storage or retention settings. When users are assigned to User Profiles with varying storage locations or retention periods, the longest retention policy will be applied, and storage locations may be assigned arbitrarily. Please ensure that all users belong to a single AAD group mapped to Meeting Insights.  
See full list of users >  
Dec 26, 2023 9:46 AM
- 1 new users were assigned with the license. Overall 52 users exceed the number of available licenses.  
Dec 26, 2023 9:46 AM
- Automatic Synchronization from AAD was switched from off to on successfully.  
Dec 26, 2023 9:46 AM



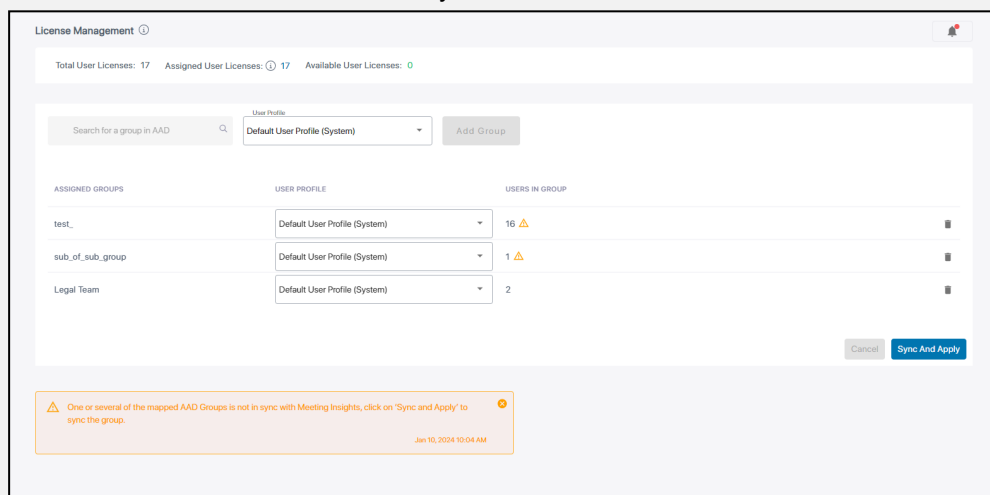
In the preceding figure, the first notification shown under Recent Activities indicates that the same user is found in two user groups with two different user profiles | two different Retention Policies, as described [here](#).

2. Scroll down in the (Recent Activities) pane until you view the **See All System Activity Logs** link, and then click the link.

System Activity Log				
Total logs: 124				<a href="#">Export To Csv</a>
<input type="checkbox"/> DATE AND TIME	LOG TYPE	ACTIVITY TYPE	LOG DESCRIPTION	
MM/DD/YYYY - MM/DD/YYYY	Select	Select		
<input type="checkbox"/> Dec 25, 2023 8:45 AM	Warning	License	1 new users were assigned with the license. Overall 52 users exceed the number of available licenses.	
<input type="checkbox"/> Dec 25, 2023 8:43 AM	Warning	License	1 new users were assigned with the license. Overall 51 users exceed the number of available licenses.	
<input type="checkbox"/> Dec 25, 2023 8:22 AM	Warning	License	1 new users were assigned with the license. Overall 50 users exceed the number of available licenses.	
<input type="checkbox"/> Dec 24, 2023 11:43 PM	Alarm Clear	AAD Connection	Connection to Azure AAD was restored.	
<input type="checkbox"/> Dec 24, 2023 11:10 PM	Alarm Clear	AAD Connection	Connection to Azure AAD was restored.	
<input type="checkbox"/> Dec 24, 2023 10:20 PM	Alarm Clear	AAD Connection	Connection to Azure AAD was restored.	
<input type="checkbox"/> Dec 24, 2023 12:28 PM	Warning	Configuration	Failed to update teams application	
<input type="checkbox"/> Dec 24, 2023 12:24 PM	Warning	Configuration	Failed to update teams application	
<input type="checkbox"/> Dec 24, 2023 12:22 PM	Warning	Configuration	Failed to update teams application	
<input type="checkbox"/> Dec 24, 2023 12:20 PM	Warning	Configuration	Failed to update teams application	
<input type="checkbox"/> Dec 24, 2023 12:16 PM	Warning	Configuration	Failed to update teams application	



- The System Activity Log page enables admins to view all *system* activities such as when the license count changes. For more information about the System Activity Log page, see [here](#).
- When 'Automatic synchronization from AAD' is ON, notifications not displayed in the License Management page are displayed in the System Activity Log. The system updates itself from AAD without user actions, i.e., the updates occur automatically in the background, without the user logging in.
- If admin adds a user to a mapped group on the AAD and 'Automatic Synchronization from AAD' is ON, the user is *automatically* added to the Meeting Insights group. In the License Management page, no notification is displayed. The System Activity Log displays the notification **1 new users were assigned with the license**.
- When 'Automatic Synchronization from AAD' is OFF, notifications (about a **Sync and Apply** action, for example) are displayed in the License Management page. The icon and the notification in the figure below indicate that a mapped AAD group is not in sync with Meeting Insights. The activated **Sync and Apply** button also indicates there's a need to synchronize.



- View in the License Management page the following notification that is displayed when adding a user group, if the number of users in the group exceeds the number of available licenses:

The screenshot shows the 'License Management' interface. At the top, it displays 'Total User Licenses: 17', 'Assigned User Licenses: 17', and 'Available User Licenses: 0'. Below this is a search bar and a dropdown menu for 'User Profile' set to 'Default User Profile (System)'. A table lists assigned groups: 'test\_', 'sub\_of\_sub\_group', and 'Legal Team', all with 'Default User Profile (System)' and user counts of 16, 1, and 2 respectively. A red warning box at the bottom states: 'The number of users in the group exceeds the number of available licenses. Please ensure that the number of users in the group does not exceed the count of available licenses. To add licenses, please contact the service provider.' The date 'Jan 10, 2024 10:25 AM' is shown at the bottom right of the warning.

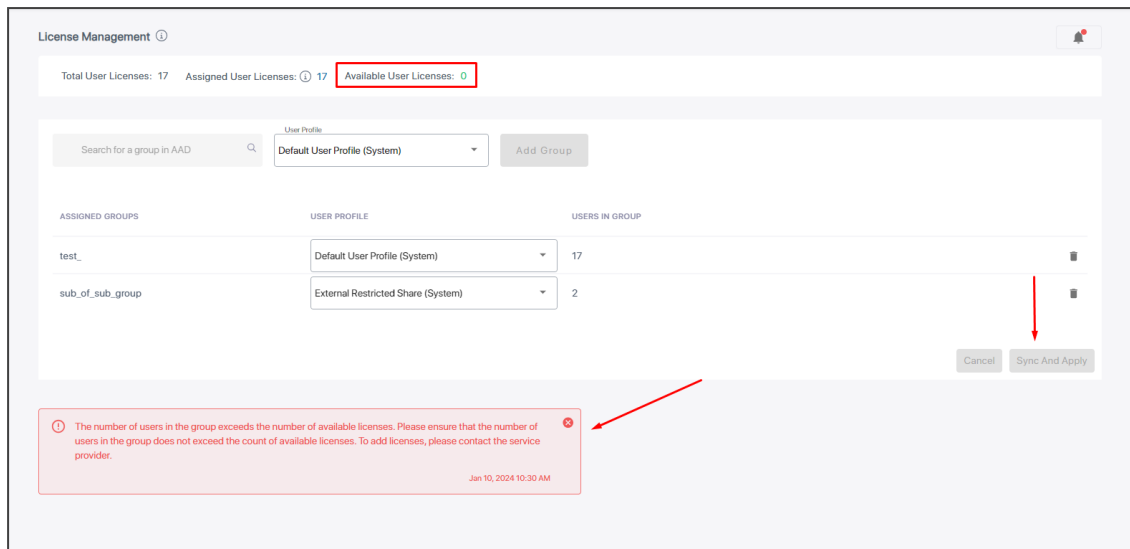
ASSIGNED GROUPS	USER PROFILE	USERS IN GROUP
test_	Default User Profile (System)	16
sub_of_sub_group	Default User Profile (System)	1
Legal Team	Default User Profile (System)	2

- The figure below shows the License Management page *before* a user group is added whose number of users exceeds the number of available licenses.

The screenshot shows the 'License Management' interface after adding a new group. The 'Assigned User Licenses' is now 18. The table lists four groups: 'test\_', 'sub\_of\_sub\_group', 'Design', and a new group with 'External Restricted Share (System)' profile and 2 users. The 'Design' group has a 'Default User Profile (System)' and 15 users. Red arrows point to the 'Design' group and the 'Sync And Apply' button.

ASSIGNED GROUPS	USER PROFILE	USERS IN GROUP
test_	Default User Profile (System)	17
sub_of_sub_group	External Restricted Share (System)	2
Design	Default User Profile (System)	15

- The figure below shows the License Management page *after* a user group is added whose number of users exceeds the number of available licenses.




The user group will not be added and the **Sync and Apply** button will not be activated.

- If this notification is received after you add a user to a user group in AAD that already exists in Meeting Insights, the user will not be added because of an insufficient number of licenses. Synchronization will not be allowed until the conflict is resolved. The user will not be added until licenses are made available or new licenses are added. Meeting Insights won't allow any operation to occur - not even (for example) editing other user groups associated with different user profiles. The **Sync and Apply** button in the License Management page will be deactivated.


## Switching from Admin to User Mode, and Back

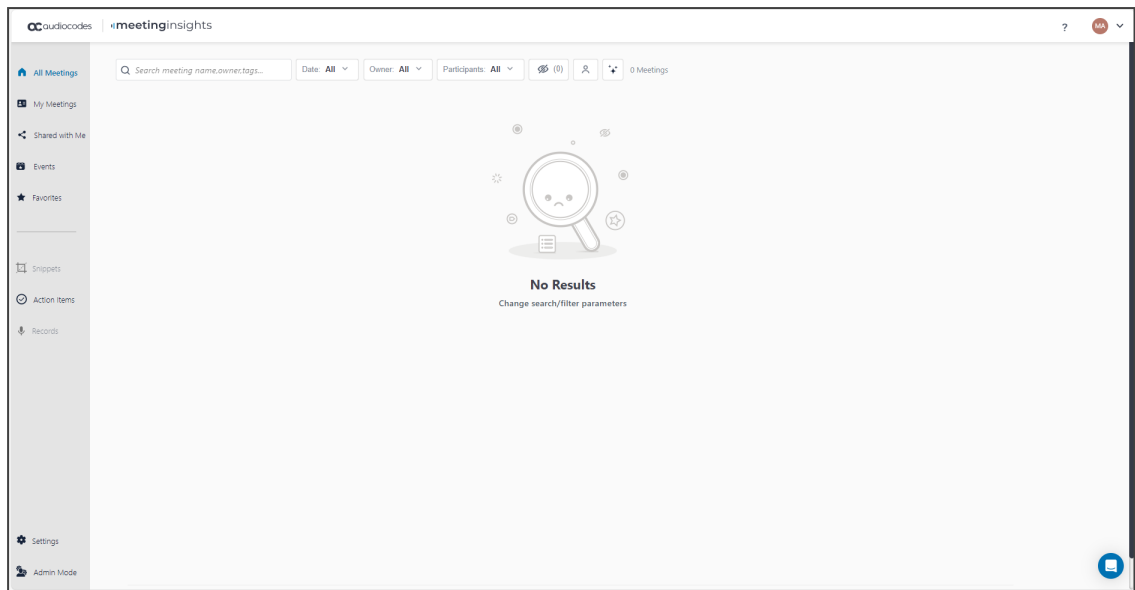
Admin can optionally switch from Admin Mode to User Mode, and then back to Admin Mode.



-  **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).

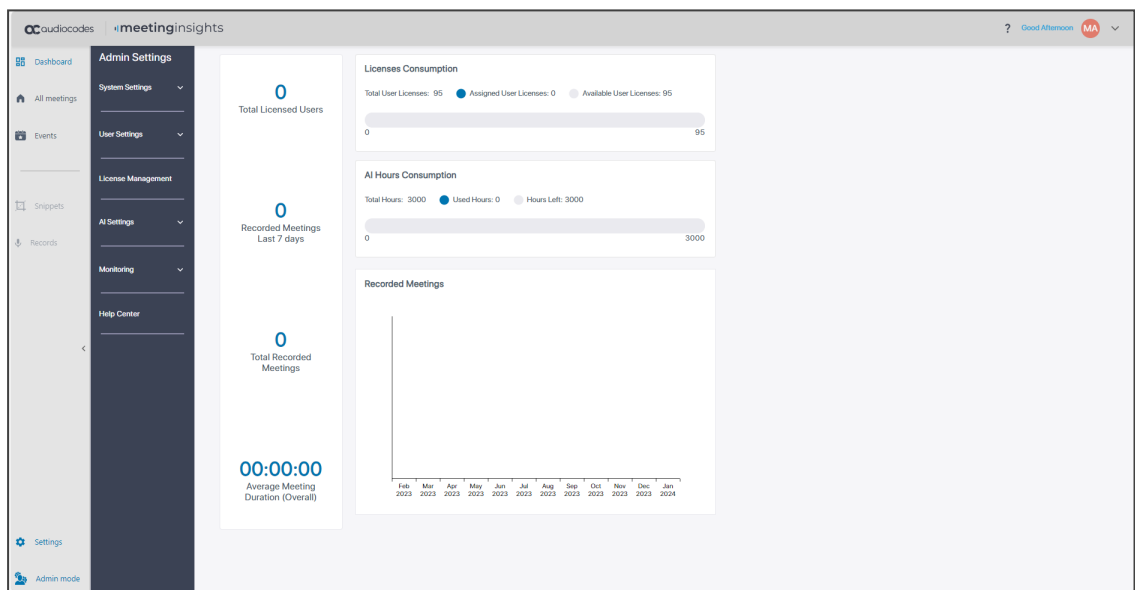
### ➤ To switch to user view:

- 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.

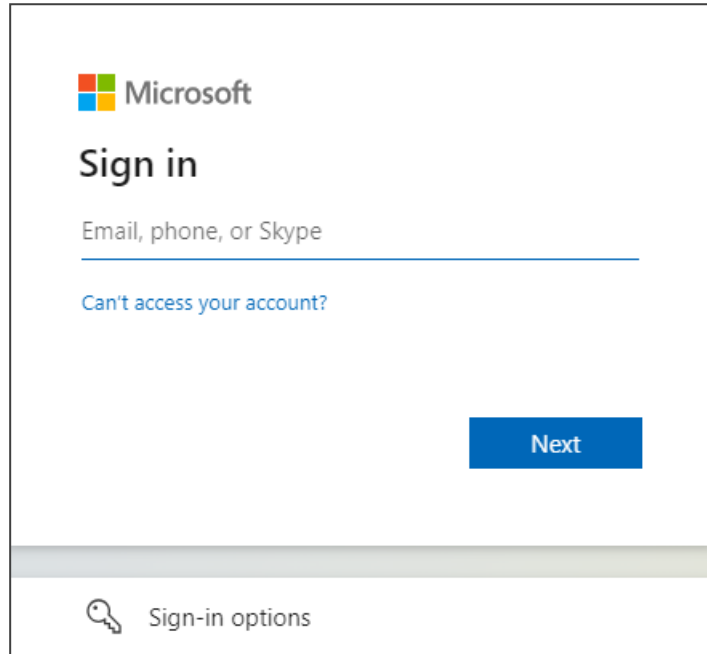


## 5 Testing your Meeting Insights App

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.

A screenshot of the Microsoft sign-in page. At the top left is the Microsoft logo. Below it is the text "Sign in". Underneath is a text input field with the placeholder text "Email, phone, or Skype". Below the input field is a link that says "Can't access your account?". At the bottom right is a blue button labeled "Next". At the bottom left is a link icon (a key) followed by the text "Sign-in options".


Microsoft

Sign in

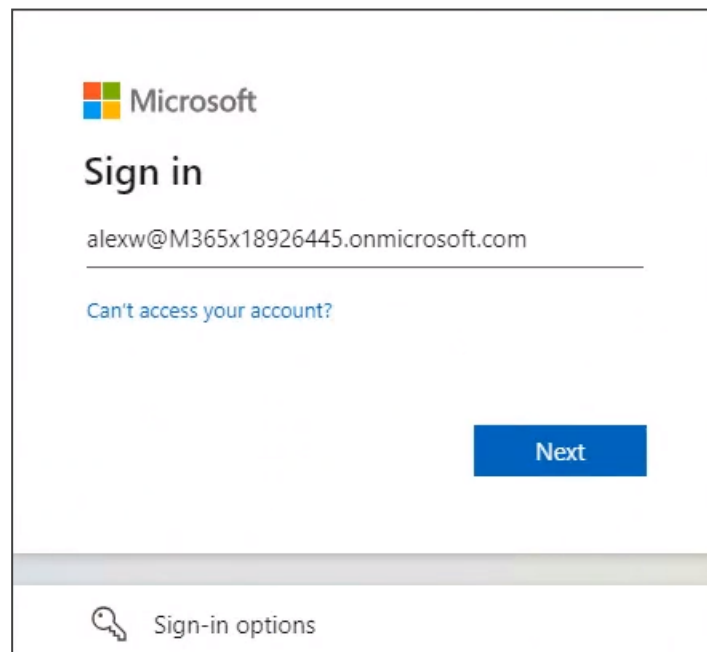
Email, phone, or Skype

[Can't access your account?](#)

Next

 Sign-in options

2. Enter the user's Teams client username.

A screenshot of the Microsoft sign-in page, similar to the previous one, but with the username "alexw@M365x18926445.onmicrosoft.com" entered in the text input field. The "Next" button and "Sign-in options" link are still present.


Microsoft

Sign in

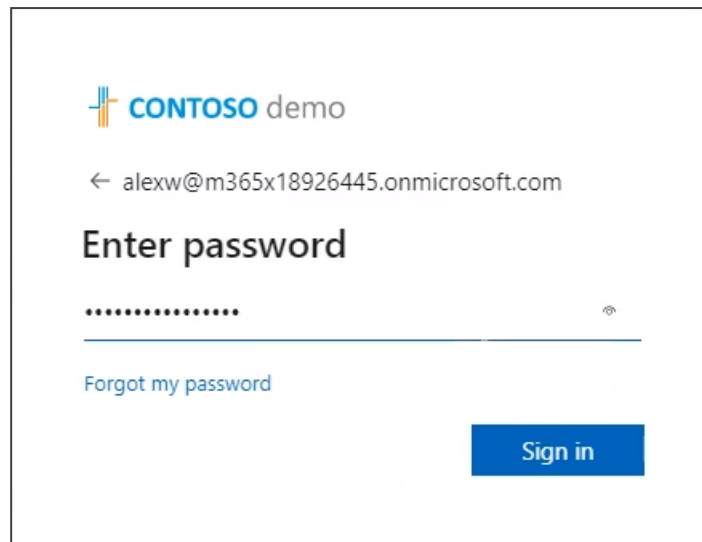
alexw@M365x18926445.onmicrosoft.com

[Can't access your account?](#)

Next

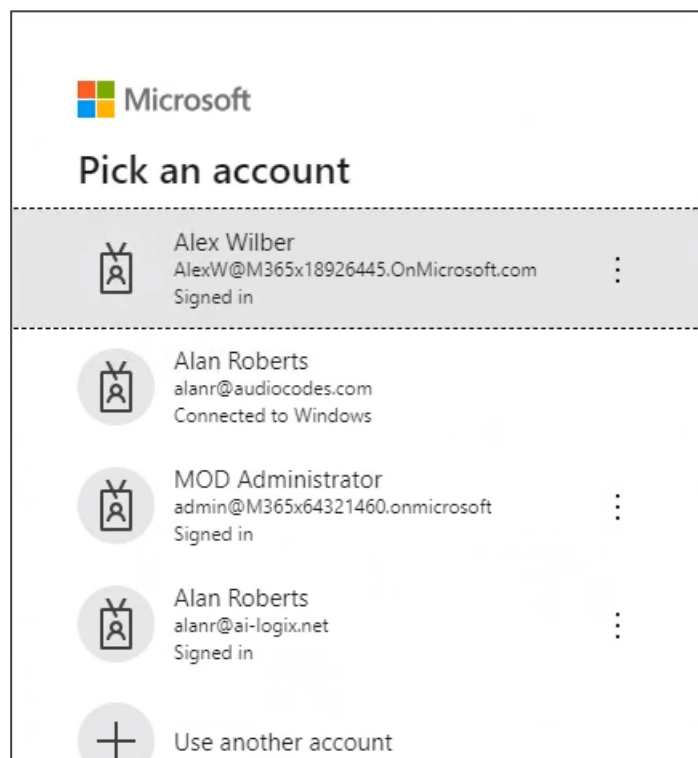
 Sign-in options

3. Click **Next**.



The screenshot shows a login interface for a demo account. At the top, it says "CONTOSO demo" with a logo. Below that, the email address "alexw@m365x18926445.onmicrosoft.com" is displayed with a back arrow. The main heading is "Enter password". There is a password input field with a masked password "....." and a toggle icon for visibility. Below the password field is a link "Forgot my password". At the bottom right is a blue "Sign in" button.

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

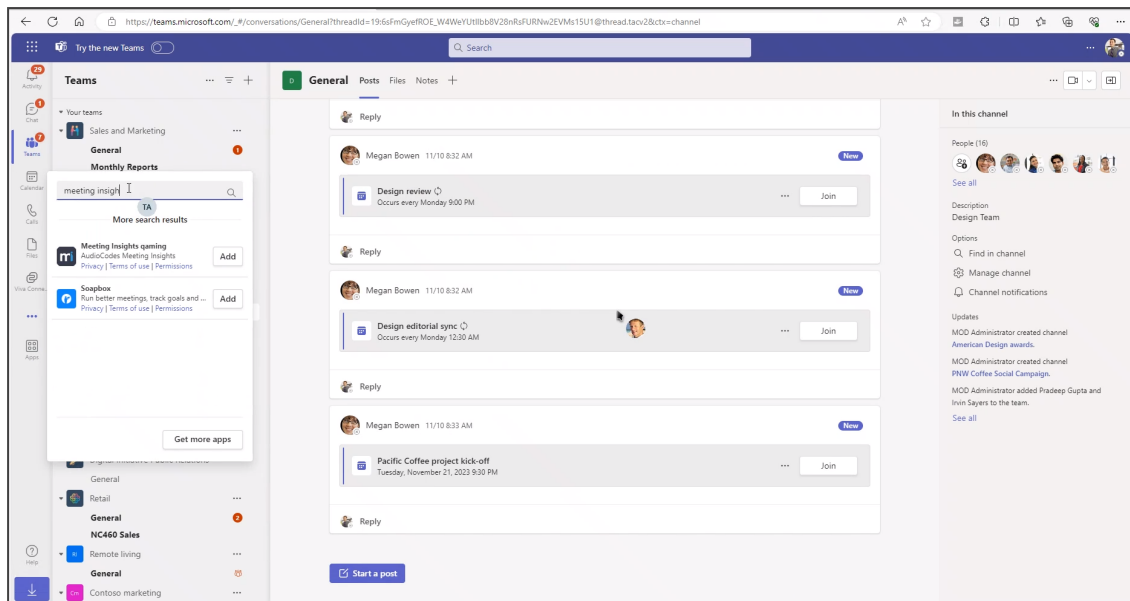


The screenshot shows the "Pick an account" screen in Microsoft Teams. At the top is the Microsoft logo. Below it is the heading "Pick an account". There is a list of accounts, each with a profile picture icon, name, email address, and status. The first account, Alex Wilber, is highlighted with a grey background. Below the list is a button with a plus sign and the text "Use another account".

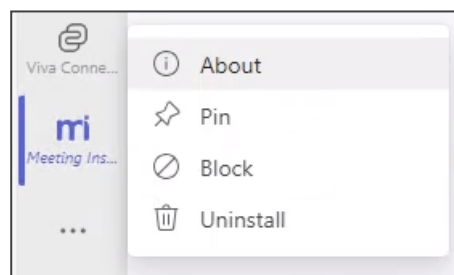
Account	Name	Email	Status
Alex Wilber	Alex Wilber	AlexW@M365x18926445.OnMicrosoft.com	Signed in
Alan Roberts	Alan Roberts	alanr@audiocodes.com	Connected to Windows
MOD Administrator	MOD Administrator	admin@M365x64321460.onmicrosoft	Signed in
Alan Roberts	Alan Roberts	alanr@ai-logix.net	Signed in

5. Click the account of the user.

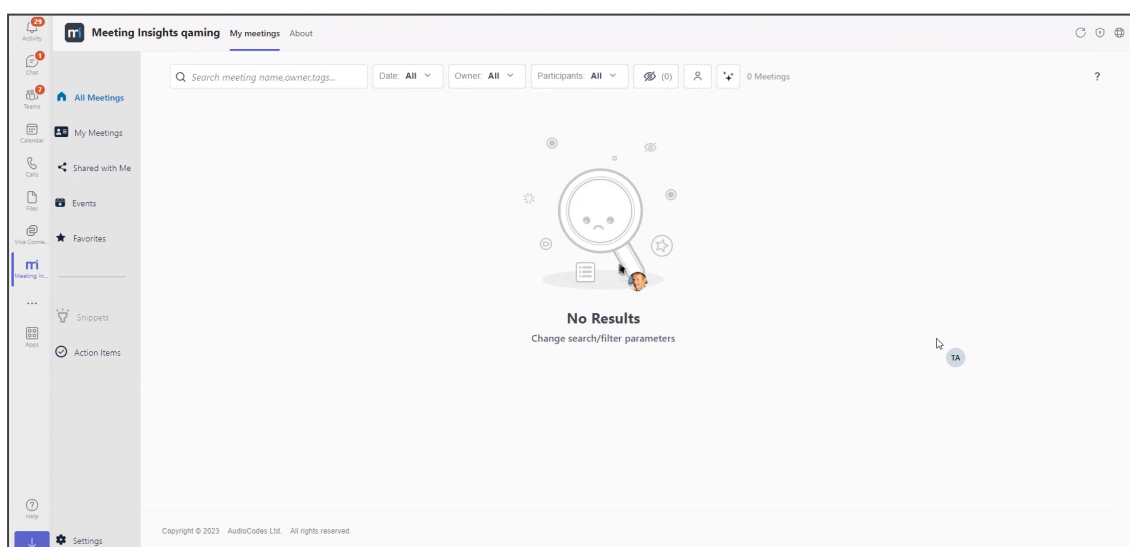




6. In the Teams web app, click the ... option in the left menu bar. In the 'Search for apps' field, enter Meeting Insights.
7. Select the **Meeting Insights** app and click the **Add** button next to it; Meeting Insights is added to the Teams client.
8. Right-click the newly added Meeting Insights icon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

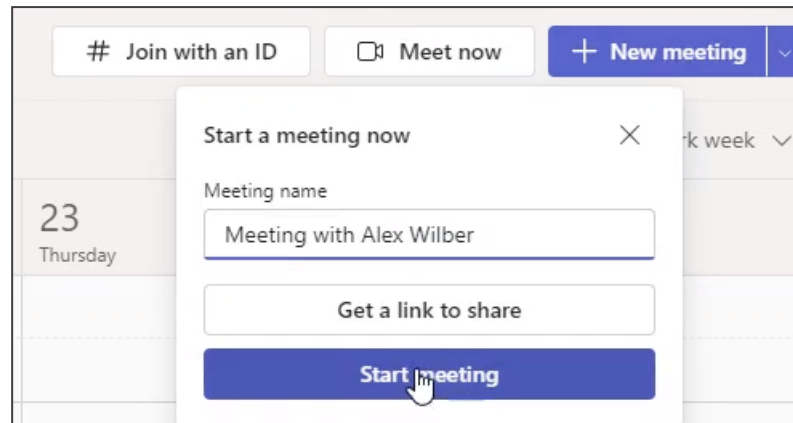


9. From the popup, select **Pin**.



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

10. Click the **Calendar** icon and in the Calendar, click **Meet Now**.



- The preceding figure shows the setup for an ad hoc meeting, i.e., without scheduling. Go to **+Apps** and select **Meeting Insights**; make sure that Meeting Insights Assistant (MIA) joins and that there's a **Meeting Insights** tab at the top of the screen.
- The instructions below describe testing a *scheduled meeting*, with MIA *joining in*.
- At the end of an ad hoc meeting or a scheduled 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.

11. Schedule a meeting for at least five minutes before a start time to allow MIA 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.

## 6 Recording Teams Live Events or Webinars

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

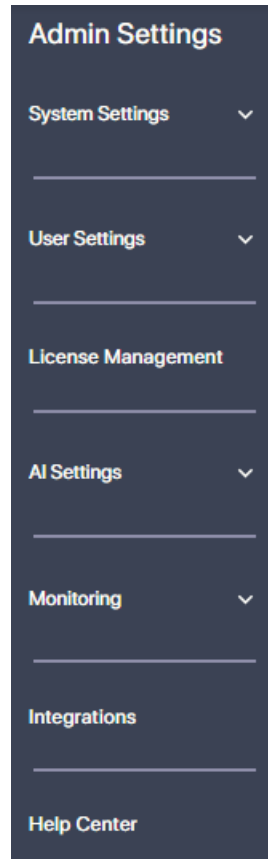
- Make sure to add the Meeting Insights Assistant (MIA) email address to the invitation or forward the invitation to MIA.



MIA can't be added as a presenter | producer.

## 7 Configuring System Settings

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



### Tools

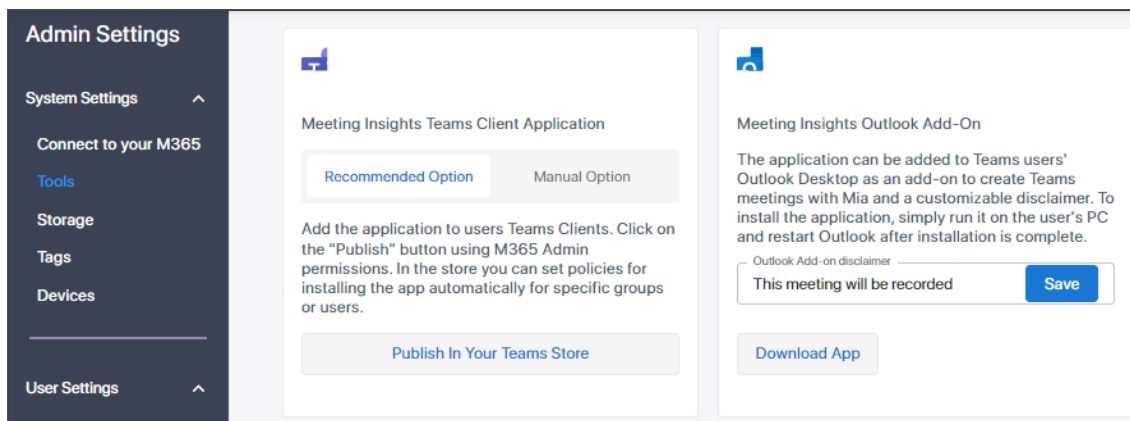
Two supplementary apps are provided by AudioCodes as installation additions:

- 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

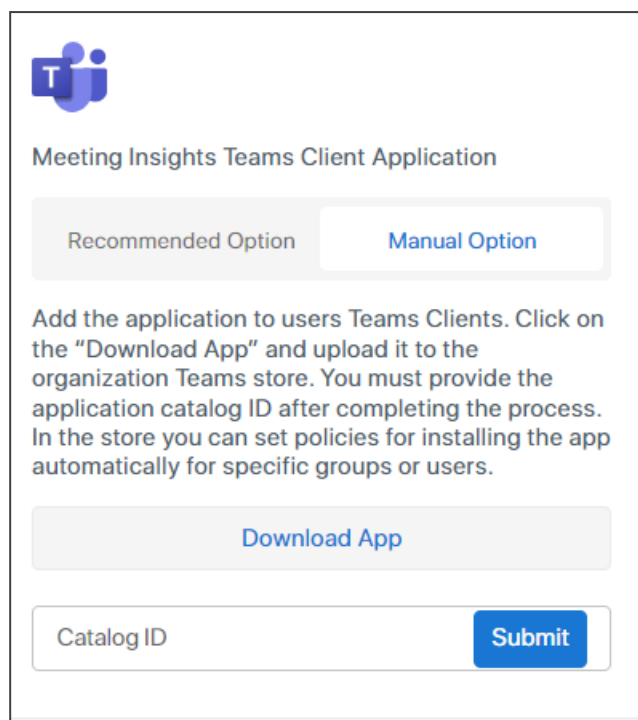
The Tools page enables the admin to add the Meeting Insights app to Teams users' Teams clients.



This step is usually performed during the initial setup in the 'Connect to your M365' page as shown [here](#) (last step).

➤ **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:
    - i. Download the app package.
    - ii. Add it manually to the Teams store; the app is allocated a catalog ID.
    - iii. Click **Manual Option**.



**Meeting Insights Teams Client Application**

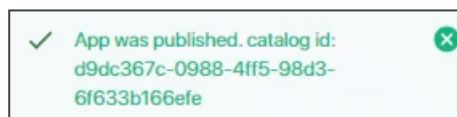
Recommended Option    Manual Option

Add the application to users Teams Clients. Click on the "Download App" and upload it to the organization Teams store. You must provide the application catalog ID after completing the process. In the store you can set policies for installing the app automatically for specific groups or users.

Download App

Catalog ID    Submit

- iv. Enter the 'Catalog ID' and then click **Submit**.



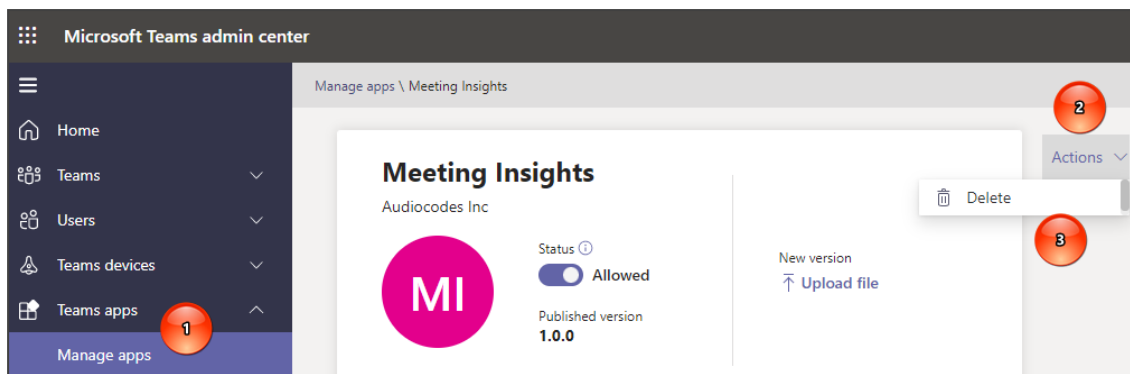
Alternatively, add the app during the initial setup in the 'Connect to your M365' page as shown [here](#) (last step).

### 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).

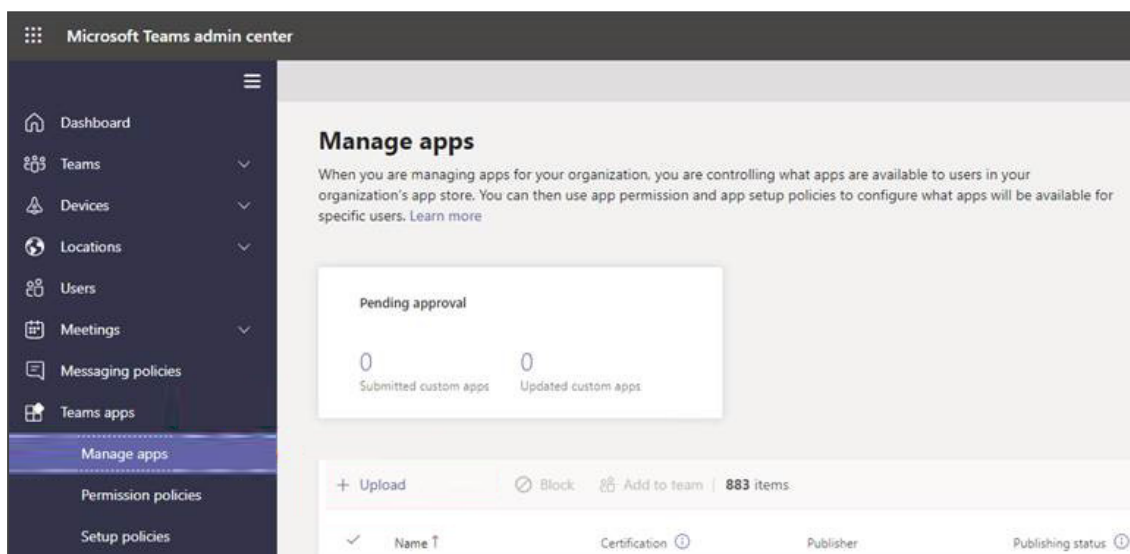
➤ **To add Meeting Insights app to Teams store via Teams admin center:**

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**:

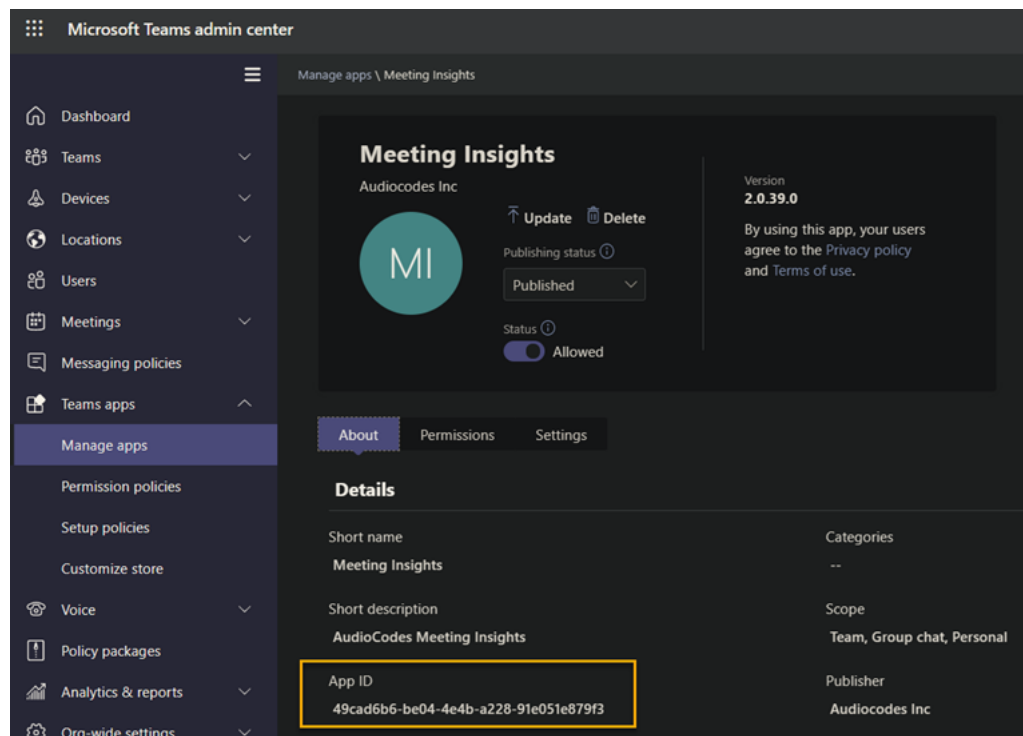


3. Upload the installation file for the Meeting Insights Teams app:

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

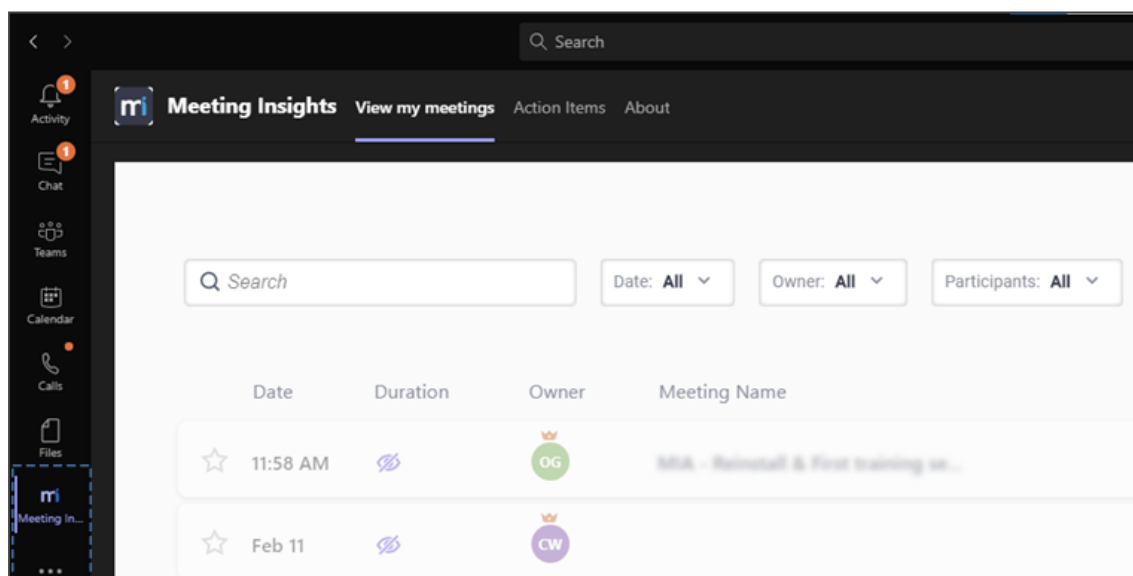


- b. In the displayed dialog box, click **Select a file**, and then browse to and select the Meeting Insights Teams app installation file (*TeamsApp.zip*) that you received from AudioCodes.
4. Provide AudioCodes with the app ID:
- a. From the left navigation menu, navigate to **Teams apps > Manage apps**.
  - 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.

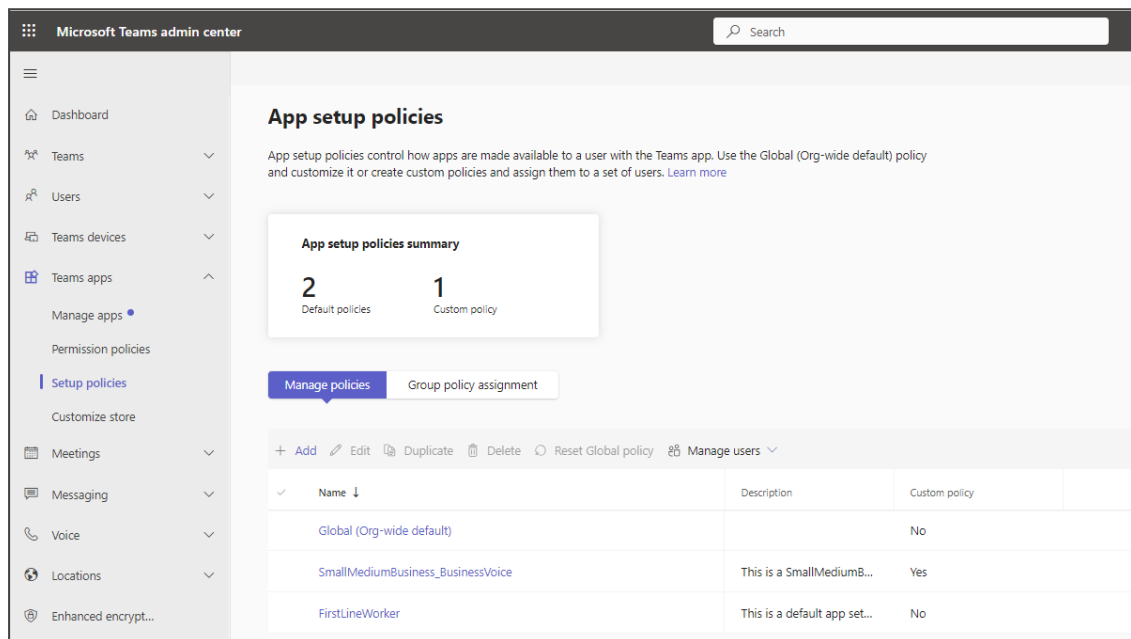


## Add and Pin Meeting Insights Teams App to the Entire Organization or to User Group(s)

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.



**Microsoft Teams admin center**

**App setup policies**

App setup policies control how apps are made available to a user with the Teams app. Use the Global (Org-wide default) policy and customize it or create custom policies and assign them to a set of users. [Learn more](#)

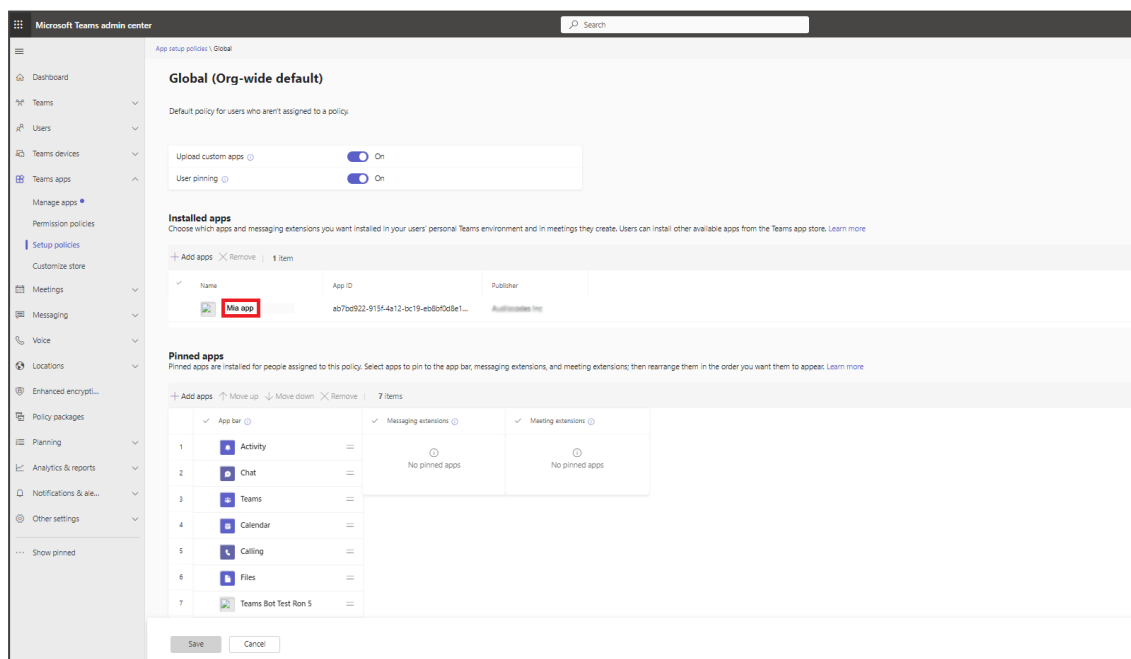
**App setup policies summary**

2 Default policies      1 Custom policy

**Manage policies**      Group policy assignment

Name	Description	Custom policy
Global (Org-wide default)		No
SmallMediumBusiness_BusinessVoice	This is a SmallMediumB...	Yes
FirstLineWorker	This is a default app set...	No

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.



**Microsoft Teams admin center**

**Global (Org-wide default)**

Default policy for users who aren't assigned to a policy.

Upload custom apps: ☐ On

User pinning: ☐ On

**Installed apps**

Choose which apps and messaging extensions you want installed in your users' personal Teams environment and in meetings they create. Users can install other available apps from the Teams app store. [Learn more](#)

Name	App ID	Publisher
Mix app	ab7bd922-9154-4a12-bc19-e08b0f0e1...	Autonomous Inc.

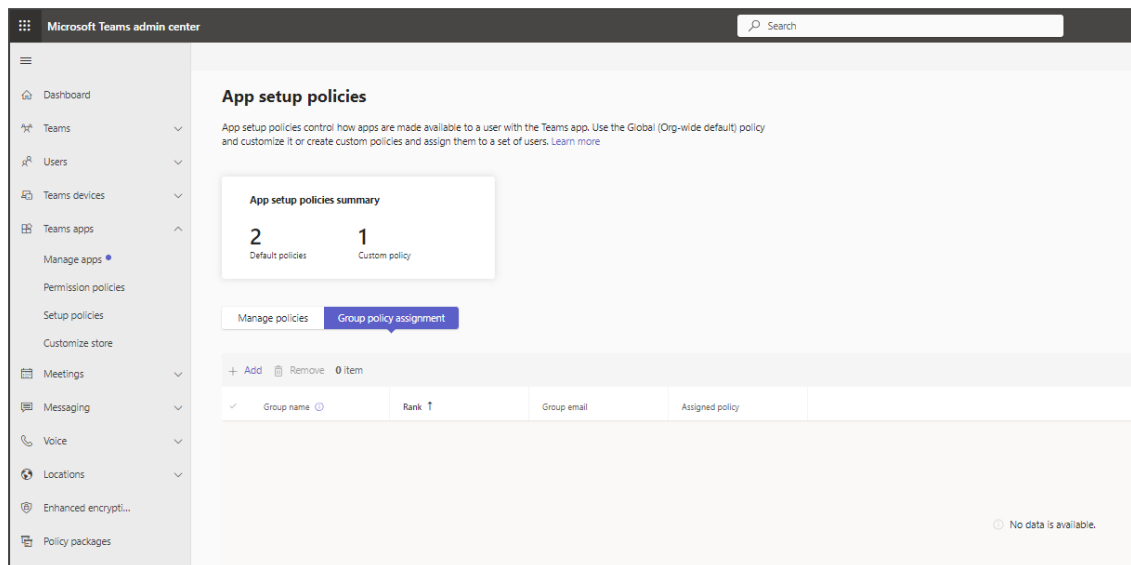
**Pinned apps**

Pinned apps are installed for people assigned to this policy. Select apps to pin to the app bar, messaging extensions, and meeting extensions; then rearrange them in the order you want them to appear. [Learn more](#)

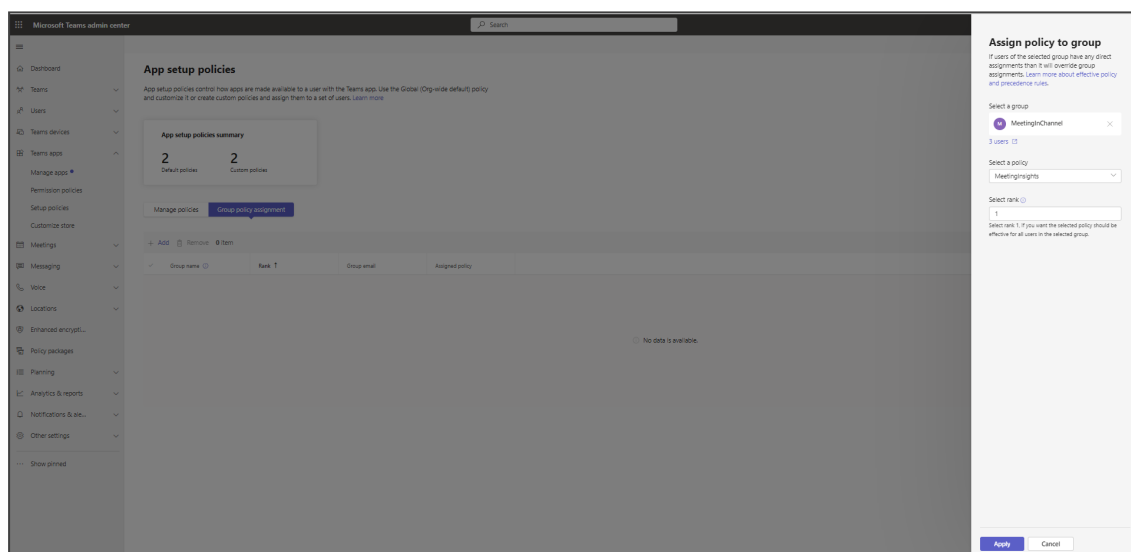
App bar	Messaging extensions	Meeting extensions
1. Activity	No pinned apps	No pinned apps
2. Chat		
3. Teams		
4. Calendar		
5. Calling		
6. Files		
7. Teams Bot Test Run 5		

Save      Cancel

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**.

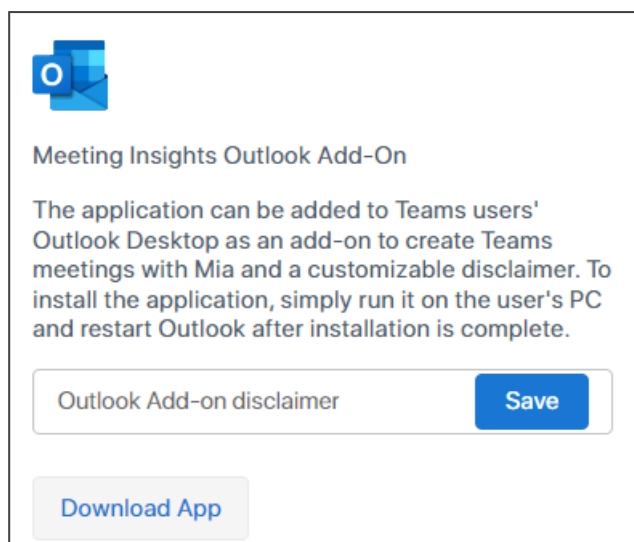


## Adding Meeting Insights to Outlook

The Tools page enables the admin to add the Meeting Insights app to Teams users' Outlook as an add-on to create Teams meetings with MIA.

### ➤ To add the Meeting Insights app:

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



2. [Optionally] Enter an Outlook add-on disclaimer and then click **Save**.
3. Click **Download App**.
4. To install the app, run it on the user's PC and restart Outlook after installation is complete.

## Installation Additions

The following supplementary application is provided by AudioCodes:

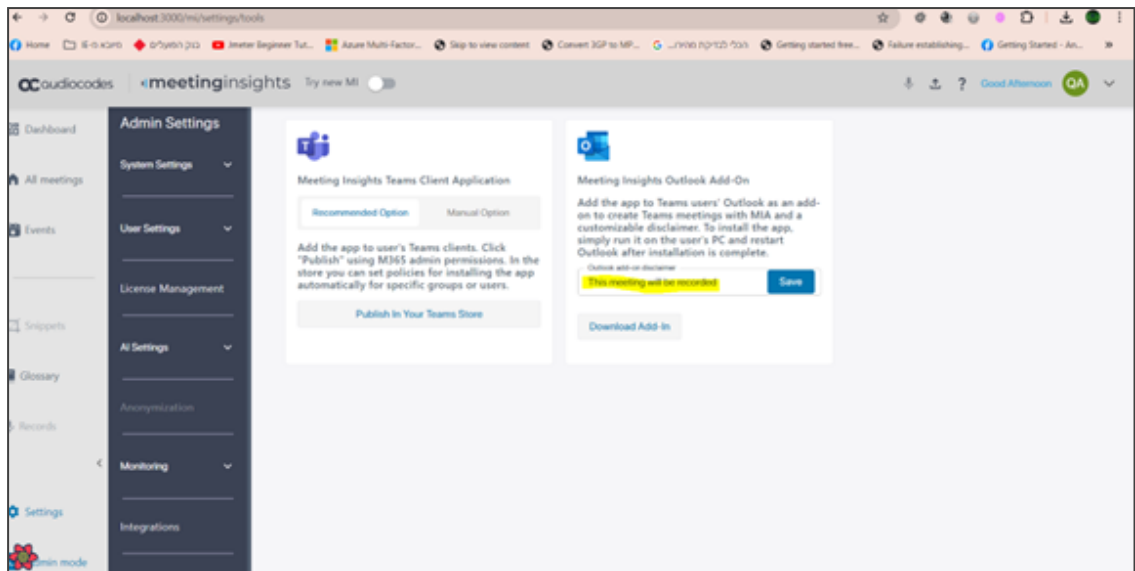
- Meeting Insights Outlook add-in, provided by AudioCodes, to make the scheduling of recorded meetings easier. See [here](#) for more information about how to set it up.

## Setting up Outlook Add-In

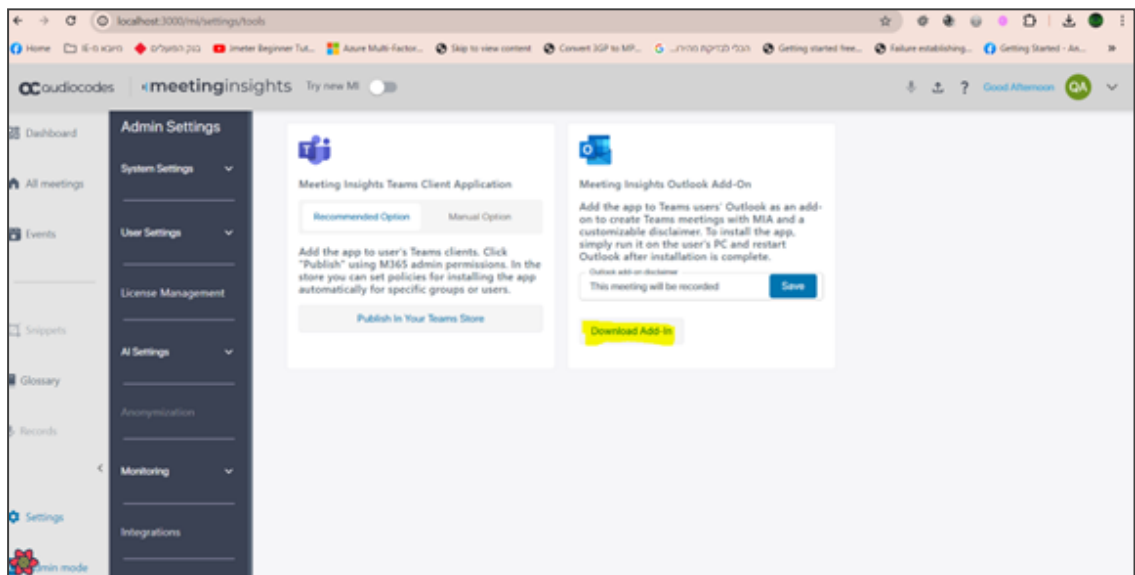
The instructions below show how to set up the Microsoft Outlook add-in. The add-in enables users to better interact with Outlook and complete tasks on messages and appointments without leaving Outlook.

### ➤ To set up Outlook add-in:

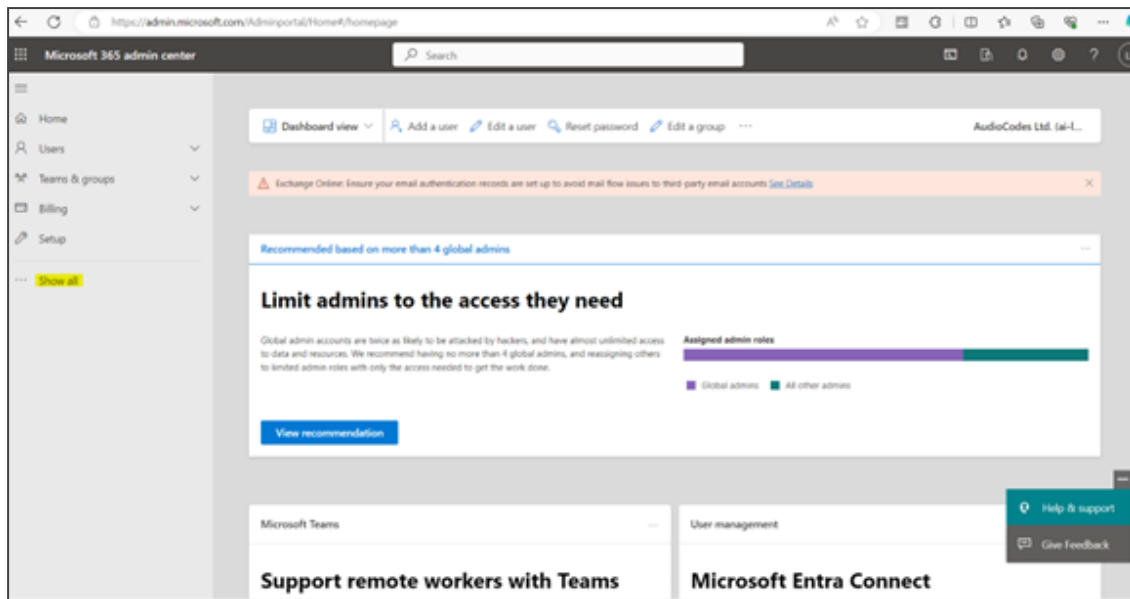
1. In the Meeting Insights 'Tools' page (**Admin Settings > System Settings > Tools**), set the disclaimer as shown here:



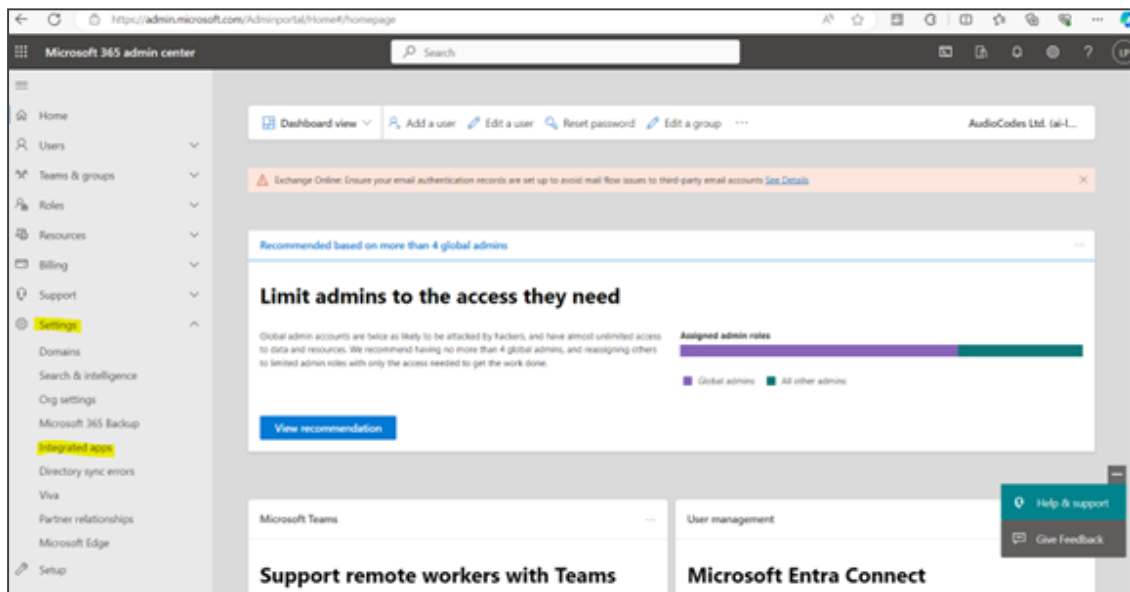
2. Download the add-in by clicking the **Download Add-In** button



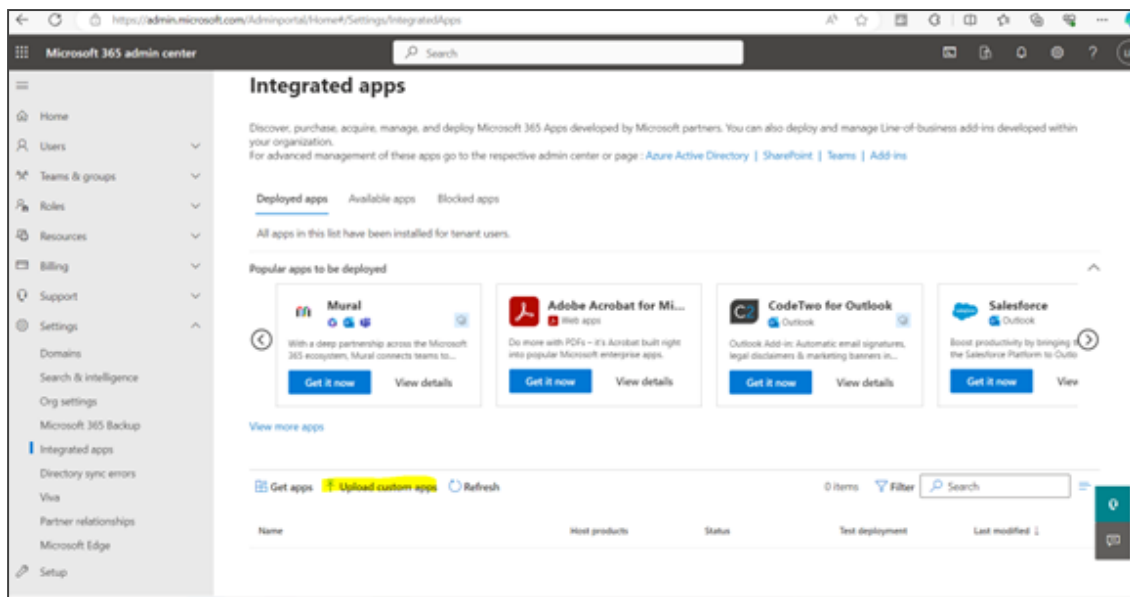
3. Log in to <https://admin.microsoft.com/> to view the Microsoft 365 admin center.



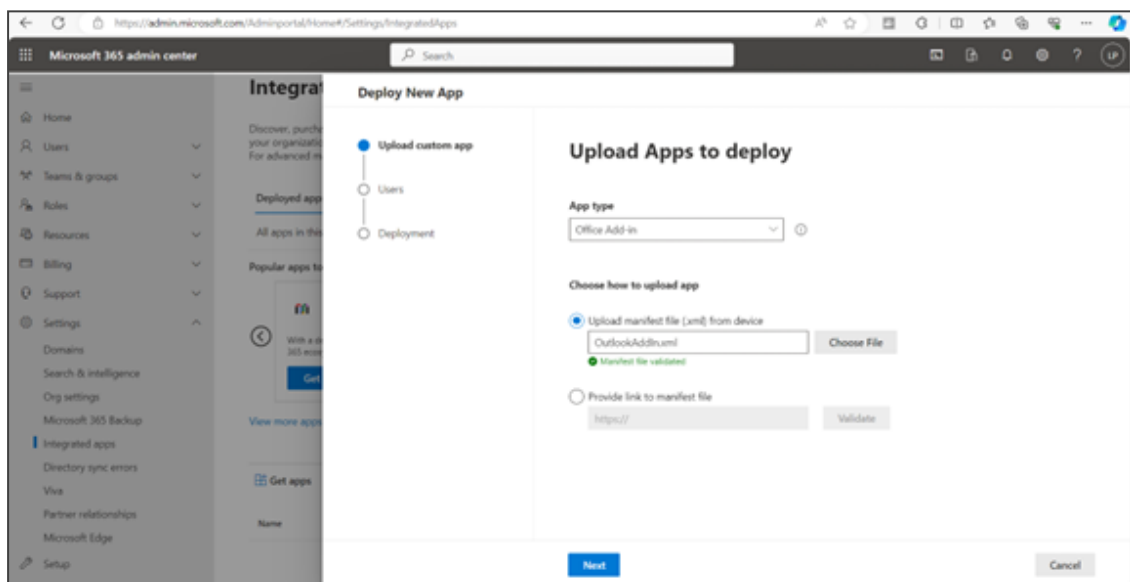
4. Click **Show All** as shown in the preceding figure.



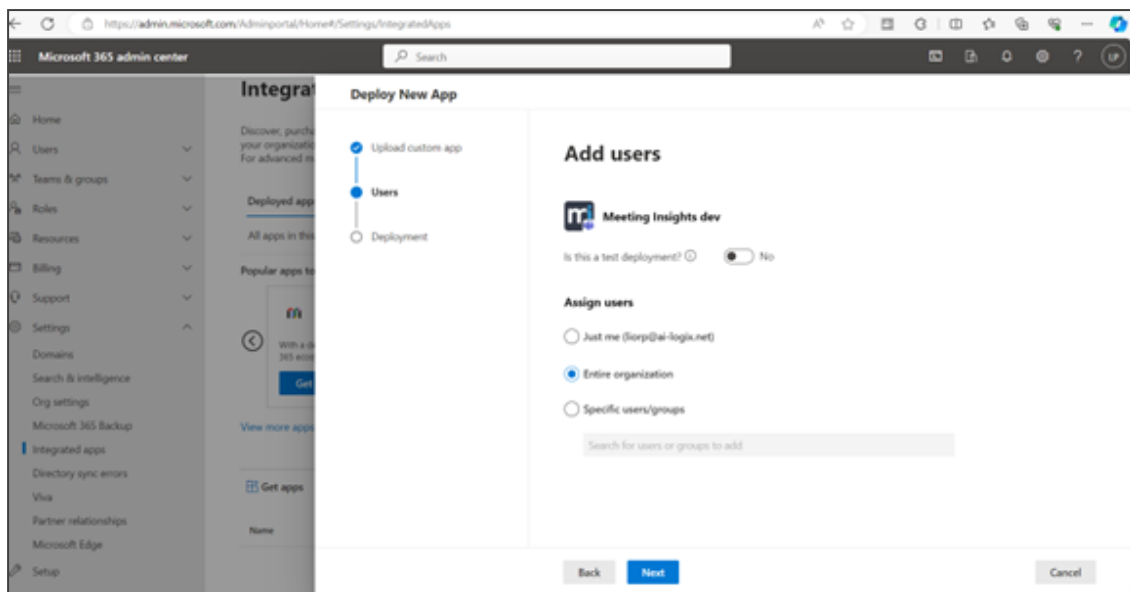
5. Expand the **Settings** menu as shown in the preceding figure and click the **Integrated apps** option.



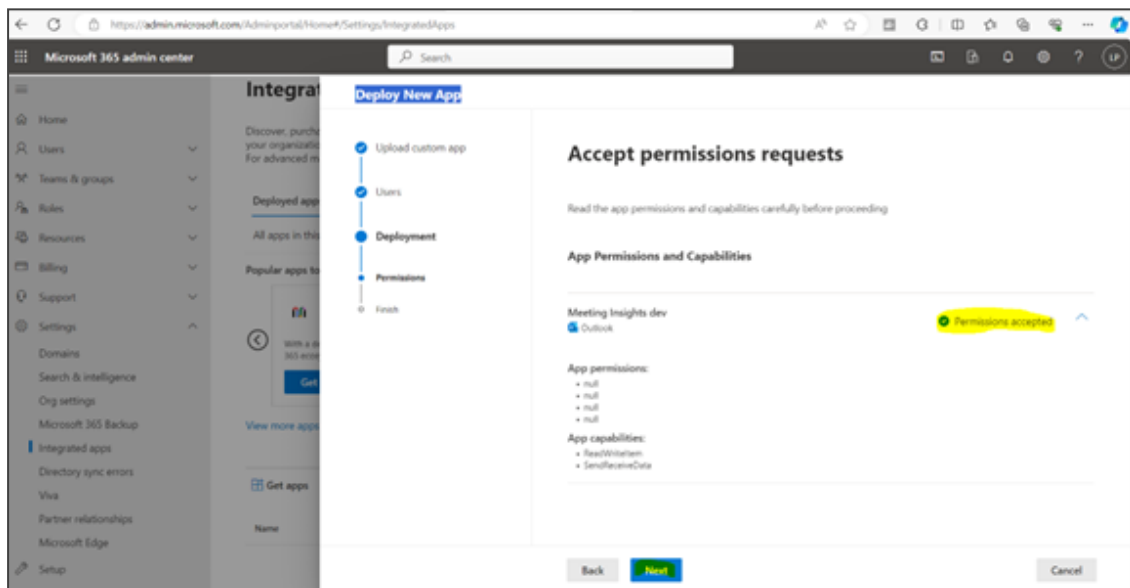
6. Click the **Upload custom apps** option.



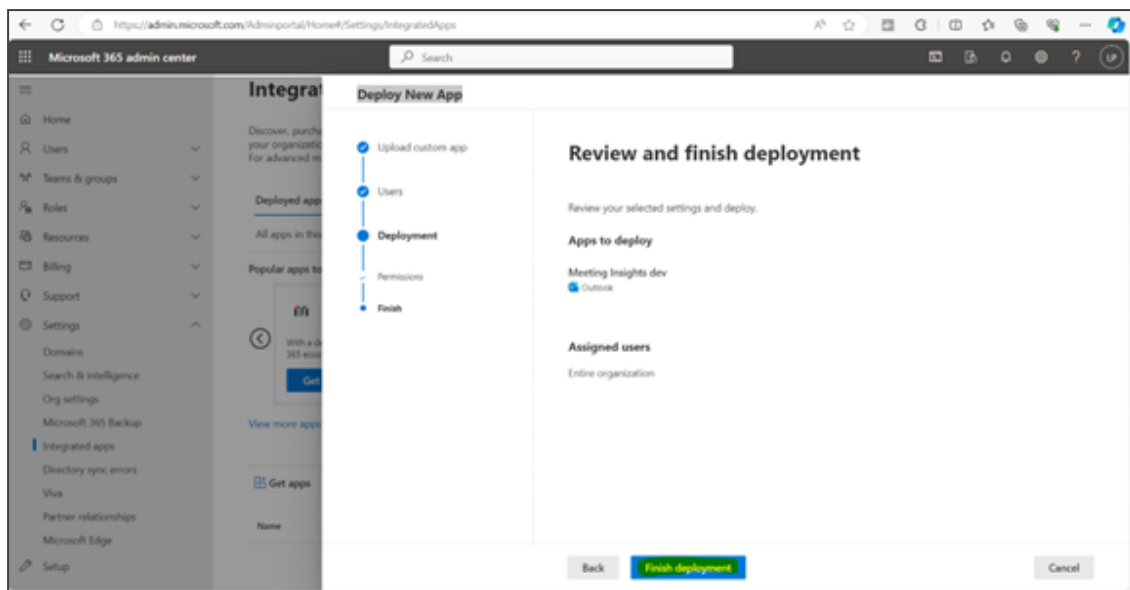
7. From the 'App type' drop-down, select **Office Add-in**, select the **Upload manifest (.xml) from device** option and then click **Choose File**. Click **Next** after xml validation.



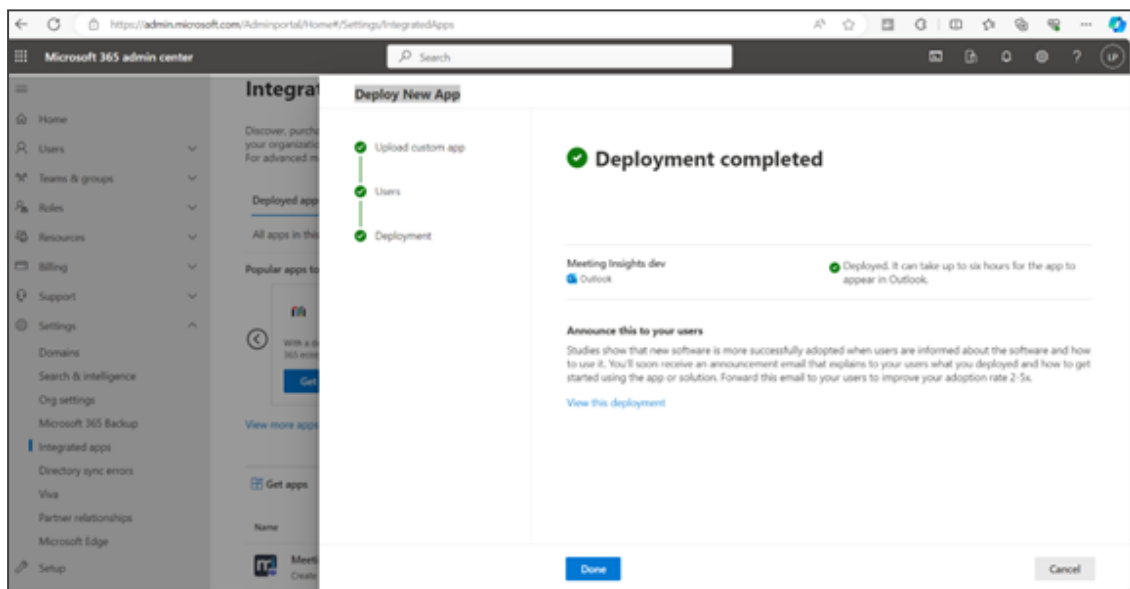
8. Select who can use the add-in and then click **Next**.



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

Azure Blob Storage is used for media recordings (audio, desktop sharing, images, etc.). Meeting Insights shows storage consumption in the Storage page under the **Consumed** column.



- The **Consumed** column is for Locally-Redundant Storage (LRS) *and* for Geo-Redundant Storage (GRS). GRS is currently not supported.
- The **Available Storage** column is for GRS only. Note that Meeting Insights doesn't limit storage.
- The **Storage Left** column is related to GRS only.



The **Name** column depicts the region in which the LRS is located. For example, 'Canada LRS' or 'Germany LRS'. The default storage is LRS.

➤ **To manage storage:**

- Under the 'System Settings' menu, click the **Storage** option.

NAME	STATUS	CONSUMED	AVAILABLE STORAGE	STORAGE LEFT
Europe LRS	#Connected	0 GB	-	-



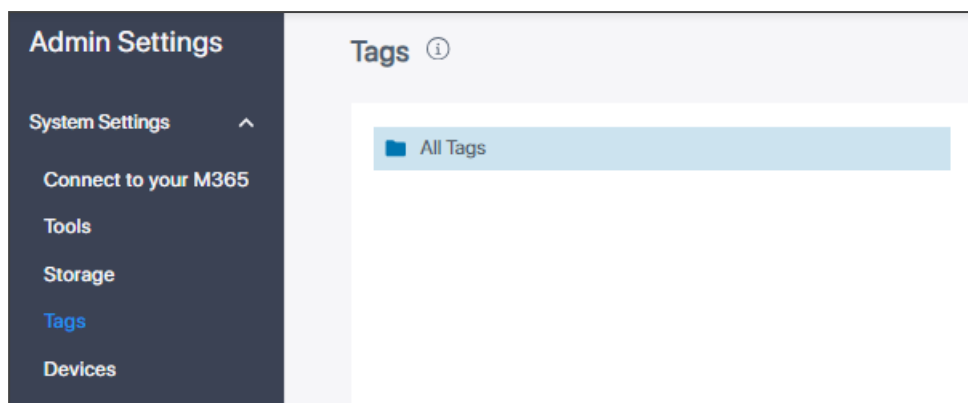
The Bring Your Own Blob Storage feature will be released in a future version.

## Tags

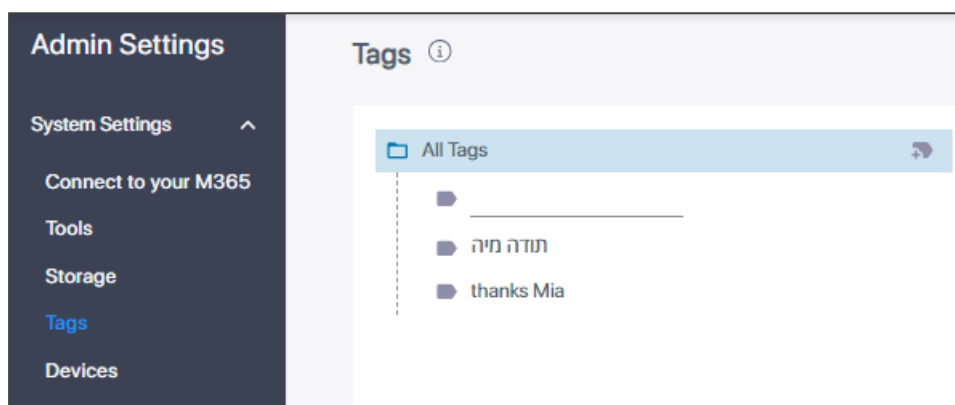
Tags can be added to meeting recordings to make it easier to search for specific information in them.

➤ **To define a tag:**

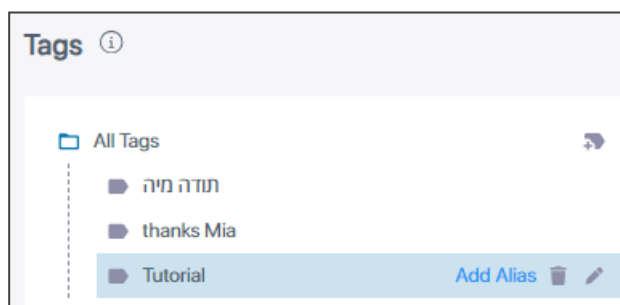
1. Under the 'System Settings' menu, click the **Tags** option.



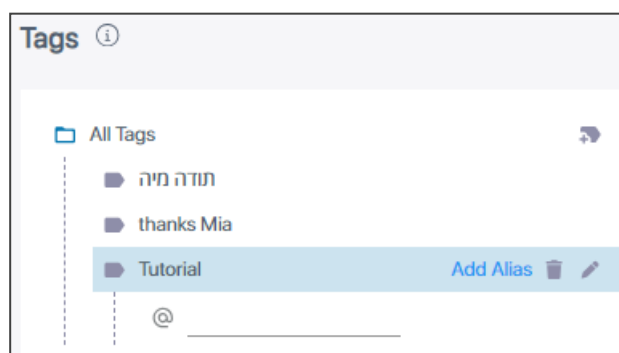
2. Point your mouse over the **All Tags** bar and then click the  icon.



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

Admins must define a conference room device for Meeting Insights to identify speakers participating physically in the room with the device, else their voice will be attributed to the room.

Admins must define a device if for example the phone in a meeting room is a Common Area Phone (CAP), unassociated with any specific user, and the attendees in the meeting want to perform recording management. If a call comes in on the phone and the device is unassociated with a 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.

### ➤ 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.

## 8 Configuring User Settings

Admin can configure the following user settings:

- [User Profiles](#)
- [Admin Profiles](#)
- [Licensed Users](#)
- [Recording Notifications](#)
- [Unlicensed Users](#)
- [Email Notifications](#)

### 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 are not assigned licenses but participated in a meeting will not have access to Meeting Insights. Meeting Insights caches their info in order to present them in meeting info to the licensed users.

See also 'Unlicensed Users' page 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 configure a user profile:

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

User Profiles		
<a href="#">+ New Profile</a>		
PROFILE NAME	GROUPS ASSIGNED	DESCRIPTION
<a href="#">Default User Profile (System)</a>	Meeting Insights Users (5)	This profile is a default profile that includes user access to their meetings
<a href="#">External Restricted Share (System)</a>		This profile enables access to user meetings and restricted external share
<a href="#">External All Share (System)</a>		This profile enables access to user meetings and both restricted and with a link share with external parties

## 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](#).

User Profiles		
<a href="#">+ New Profile</a>		
PROFILE NAME	GROUPS ASSIGNED	DESCRIPTION
<a href="#">Default User Profile (System)</a>		This profile is a default profile that includes user access to their meetings
<a href="#">External Restricted Share (System)</a>		This profile enables access to user meetings and restricted external share
<a href="#">External All Share (System)</a>		This profile enables access to user meetings and both restricted and with a link share with external parties

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

Admin Settings
System Settings
User Settings
User Profiles
Admin Profiles
Licensed Users
Unlicensed Users
Recording Notifications
Email Notifications
License Management
AI Settings
Anonymization
Monitoring
Integrations
Help Center

### Add User Profile

User Profiles include permissions and recording options that are assigned to the users associated with the profile

#### Permissions

Select permissions that users associated with the profile will have

☐ Access User Meetings ⓘ
☐ External Restricted Share
☐ External Share with a Link
☐ Premium Transcription
☐ Can Edit Other Users Meetings

#### Recording

Enable recording options

☒ Enable

##### Meeting Types

☒ User Meetings
☐ Import Meeting Recordings

##### Select Storage

United States LRS

##### Meeting Recordings Retention Period

1 Year - Default

☐ Allow Users to Extend Recordings Retention

#### AI, STT Settings

Select AI functionality that users associated with the profile will have

☒ Automatic Triggering
☐ Automatic AI
☐ Automatic STT Only

##### Language

User language can be selected during the meeting, set in advance for English only speakers. Only one option can be selected.

Select Language During Meeting

##### Insights

☐ Summary
☐ Action Items
☐ Q & A, Issues & Solutions

##### Meeting Types

☒ All Meetings
☐ Select Meeting Types

Cancel
Apply

## 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
Meeting Recording	When enabled, users in the groups assigned to the profile will be able to record the meetings they organize (they must be the meeting organizer).
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.
User Meetings	MIA will record meetings of users assigned to the profile when it is invited to the meeting and the user is the meeting organizer.
Import Meeting Recordings	Select or clear this option to give or deny the user permission ('On' or 'Off') to import meeting recordings into Meeting Insights.
Select Storage	By default, only one storage is available, with no option to select another; customers only see the system storage allocated to them, for example, Canada LRS. When more than one storage becomes available in a future version release, the option to select will become available, otherwise only storage location and type are displayed. When Bring Your Own Blob Storage (BYOS) will be added in a future version release, it will be selectable, with BYOS meeting recordings' media (files, audio, desktop sharing, images...) stored in the storage hosted by the customer, in the customer's control.
Meeting Recordings Retention	Select how long video meeting recordings will be retained for (i.e., for how many days recordings will be kept in storage); if the set limit is exceeded, recordings will be deleted.

Field	Description
Period	<ul style="list-style-type: none"> <li>■ Unlimited (default): Recordings will never be deleted. Admins must practice caution because the storage location will eventually reach full capacity.</li> <li>■ 180 Days</li> <li>■ 1 Year (365 Days)</li> <li>■ 2 Years (730 Days)</li> <li>■ 3 Years (1095 Days)</li> <li>■ Custom</li> </ul> <p>Once a day, Meeting Insights deletes recordings that exceed the retention period.</p>
Allow Users to Extend Recordings Retention	Allows users to overwrite the retention period by setting the meetings to not be deleted. In this case, the meeting will not be deleted as part of the retention period. It can be deleted manually when needed.

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' in a User Profile

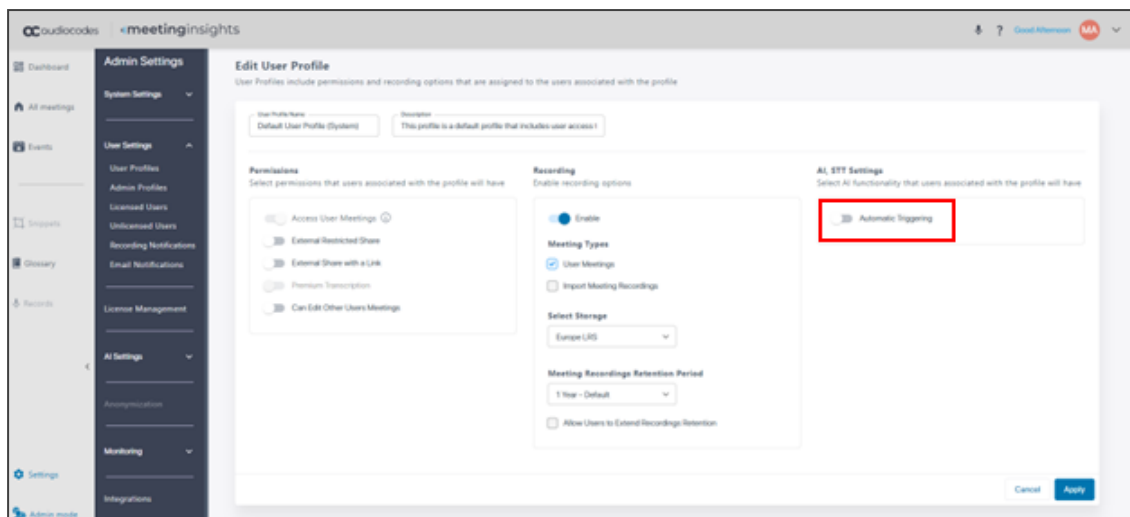
When Automatic AI triggering is enabled, you can control it in the User Profile page.



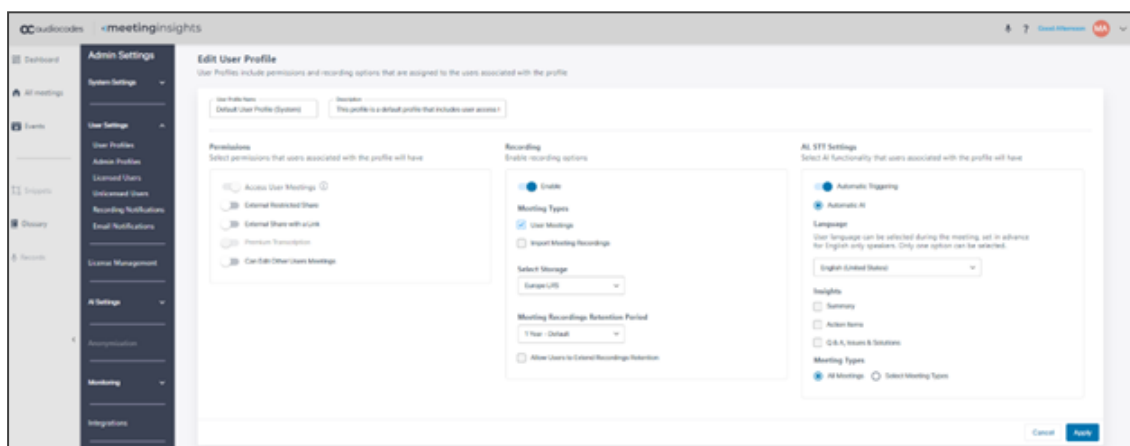
If your application excludes 'Automatic Triggering' and you would like to include the feature, contact your Service Provider.

### ➤ To enable Automatic Triggering:

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



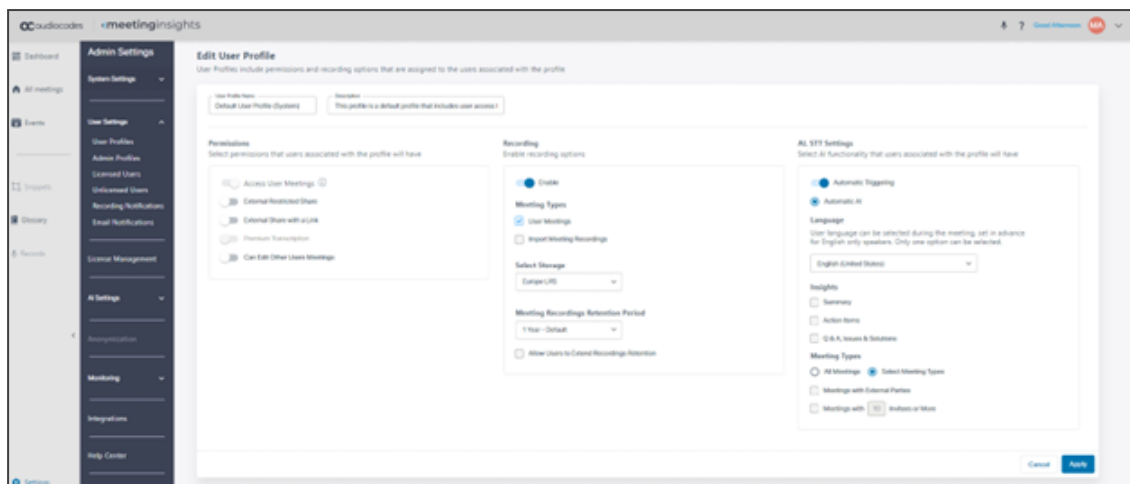
2. [Refer to the previous figure] Enable the 'Automatic Triggering' setting.



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
  - Hebrew
5. Select whether to trigger AI on 'All Meetings' or 'Select Meeting Types':
  - Meetings with External Parties
  - Large Meetings
  - Meetings with  $n$  Invitees or More





- 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.

## 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.

**Administrators (Full Access)** ⓘ

| ✕

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.

NAME	EMAIL	AAD GROUPS	USER PROFILES	REPRESENTATIVES	ADDED DATE & TIME
Brian Johnson (TAILSPIN)	BrianJ@M365x51160550...	Meeting Insights Users	Default User Profile (Syst...		Dec 3, 2023 5:04 PM
Allan Deyoung	AllanD@M365x51160550...	Meeting Insights Users	Default User Profile (Syst...		Dec 3, 2023 5:04 PM
Cameron White		Meeting Insights Users	Default User Profile (Syst...		Dec 3, 2023 5:04 PM
Adele Vance	AdeleV@M365x51160550...	Meeting Insights Users	Default User Profile (Syst...		Dec 3, 2023 5:04 PM
Alex Wilber	AlexW@M365x51160550...	Meeting Insights Users	Default User Profile (Syst...		Dec 3, 2023 5:04 PM

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.

X

Apply

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.

<input type="checkbox"/>	NAME ↕	EMAIL ↕	AAD GROUPS	USER PROFILES	REPRESENTATIVES	ADDED DATE & TIME ↕	
	Start With	Start With	Start With	Start With	Start With	MM/DD/YYYY - MM/DD/YYYY	
<input type="checkbox"/>	Brian Johnson (TAILSPIN)	Brian.J@M365x51160550...	Meeting Insights Users	Default User Profile (Syst...	Alex Wilber	Dec 3, 2023 5:04 PM	✓

## 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.

### ➤ To trigger recording notifications during meetings when recorded by Meeting Insights:

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

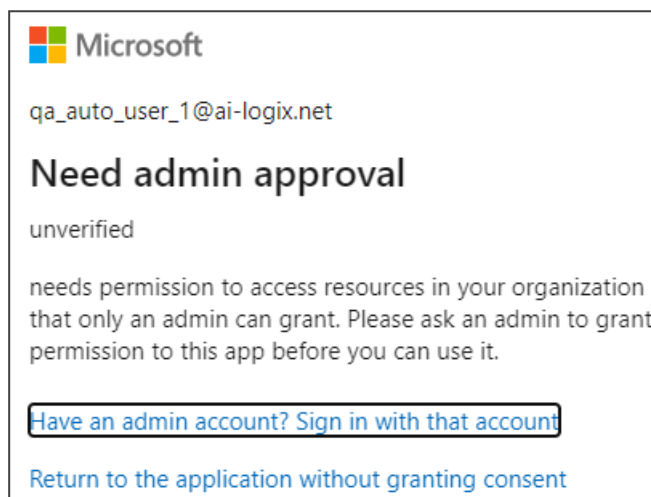
2. Make sure admin has been granted consent to allow Teams recording notifications to be triggered during meetings recorded by Meeting Insights.

- ✓ 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.

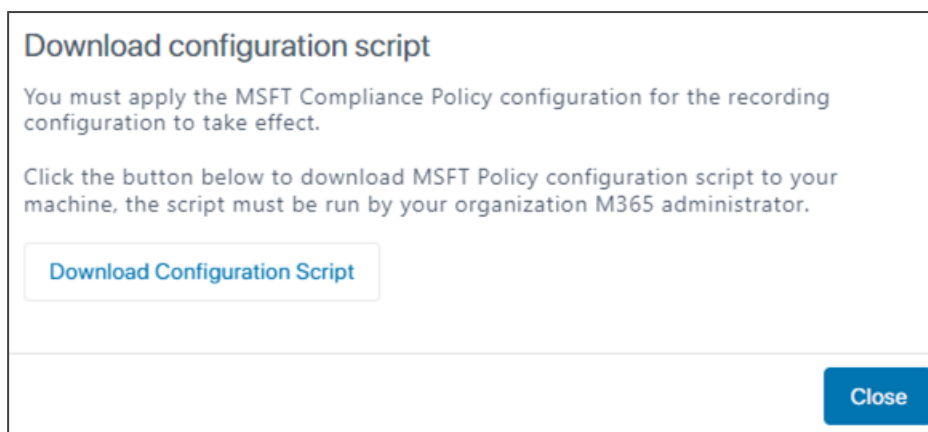
3. Click **Grant Admin Consent** > if consent has not been granted yet.



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:

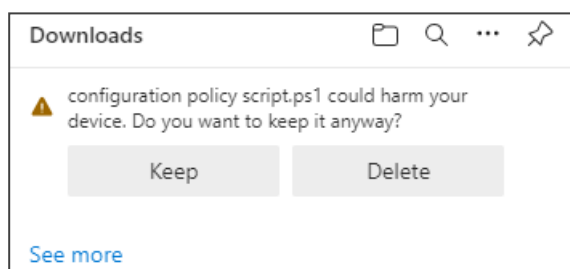


7. Click the **Download Configuration Script** button. The script must be executed by the M365 admin.



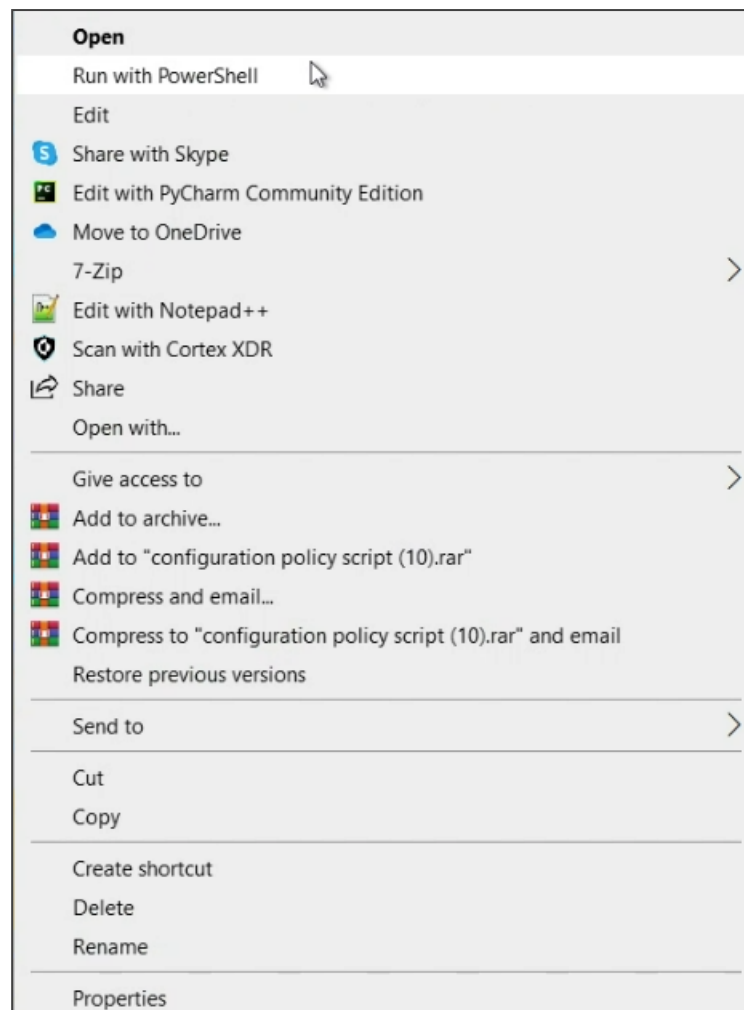
The script must be run to enable recording notifications in Microsoft. It may take time for the Microsoft configuration to take effect. Meetings of the users enabled for recording notifications will not be recorded until the configuration takes effect on the Microsoft side.

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

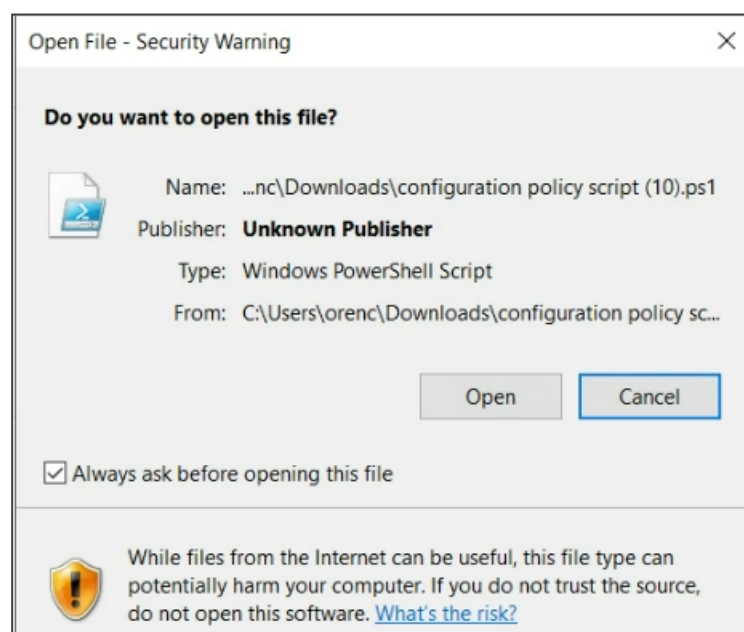


- Only Microsoft Edge displays the 'Keep' prompt.
- Chrome immediately presents the download option.

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**.

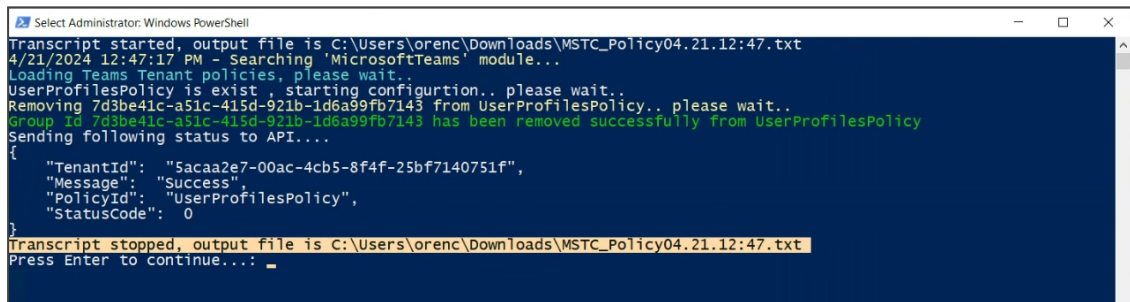


13. Click **Open**.

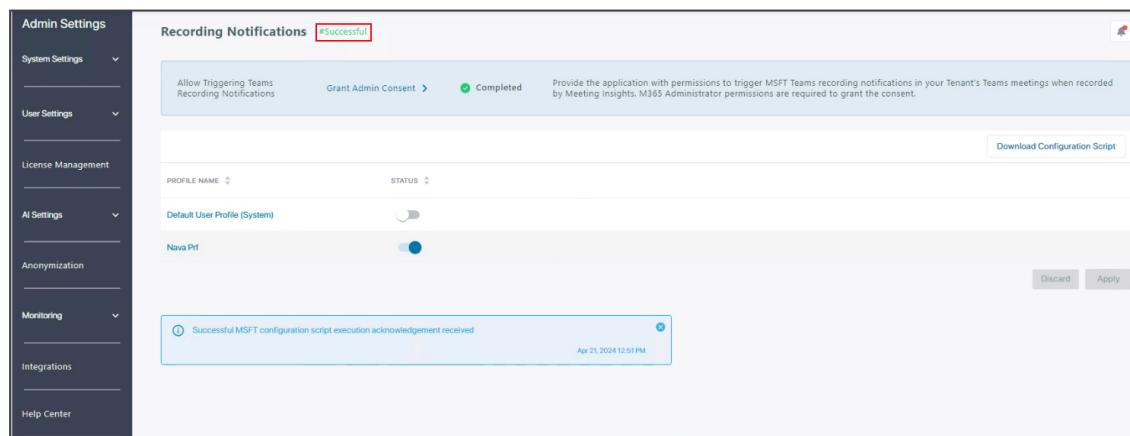


14. Click **Yes**.

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.

## 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.



- 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.

Total Accounts 3						<input type="button" value="Delete Selected Users"/> <input type="button" value="Export"/>
<input type="checkbox"/>	NAME	EMAIL	AAD OID	REPRESENTATIVES	ADDED DATE & TIME	
	Start With	Start With	Start With	Start With	MM/DD/YYYY - MM/DD/YYYY	
<input type="checkbox"/>	Raul Razo		5b10f1e8-41e2-48d9-a99d-adf81ef		Nov 6, 2023 3:10 PM	<input type="checkbox"/>
<input type="checkbox"/>	Conf Room Adams	Adams@M365x64321460.OnMicros	4770b7a9-613b-4403-902e-a48fbx		Nov 7, 2023 8:42 AM	<input type="checkbox"/>
<input type="checkbox"/>	Bianca Pisani		c06e0779-1432-44bd-a064-a7cfa5		Nov 9, 2023 2:21 PM	<input type="checkbox"/>

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.



- '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.

## Email Notifications

Provide Meeting Insights with permissions to enable Microsoft recording notifications during meetings in your Teams' tenant.

### ➤ To manage email notifications:

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

### Default User Meeting Notifications

**Owner**

AI finished: Ready or Failed ☐

Meeting Processing Failure email notification ☐

Transcription finished: Ready or Failed ☐

Weekly unpublished meetings reminder ☐

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' ☒

**Recipient**

Action item was assigned to you in a meeting you were not invited to ☐

Get meeting recap email once a meeting is published ☒

Get meeting recap UPDATE email once it is updated and sent by owner ☒

Get a notification email once a meeting is shared/unshared with you ☐

Meeting recording is ready (Video ready) ☐

Use Hebrew recap email template if recap is in Hebrew ☒

2. Configure the settings using the table below as reference.

Setting	Description
<b>Owner</b>	
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.
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'.
<b>Recipient</b>	
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.

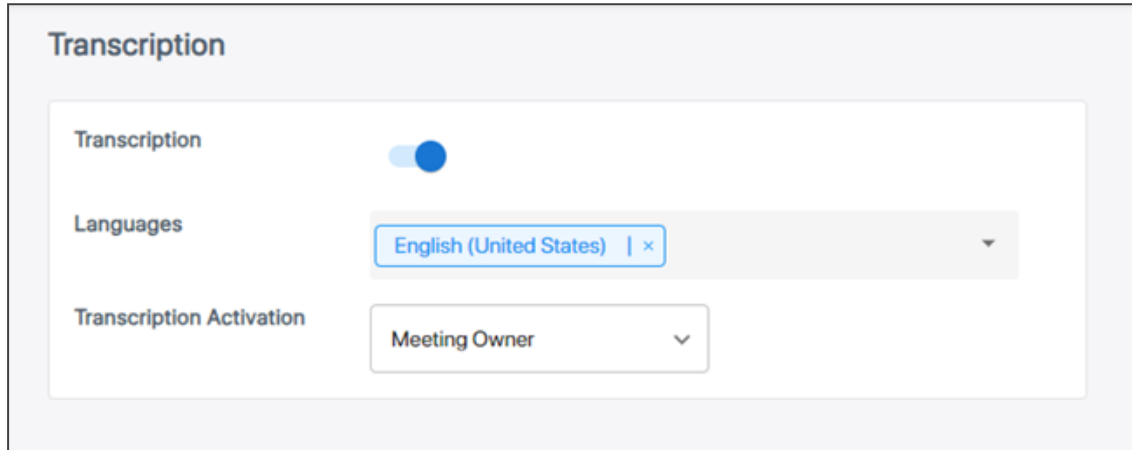
Setting	Description
Meeting recording is ready (Video ready)	Switch on   off for a notification to be sent   not sent to users indicating that the meeting recording is ready (video ready).
Use Hebrew recap email template if recap is in Hebrew	Switch on   off for a Hebrew recap email template to be used if the recap is in Hebrew.

## 9 AI Settings

Meeting Insights supports Artificial Intelligence features such as speech-to-text, allowing users to convert audio recordings of meetings to textual documentation.

➤ **To configure AI settings:**

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

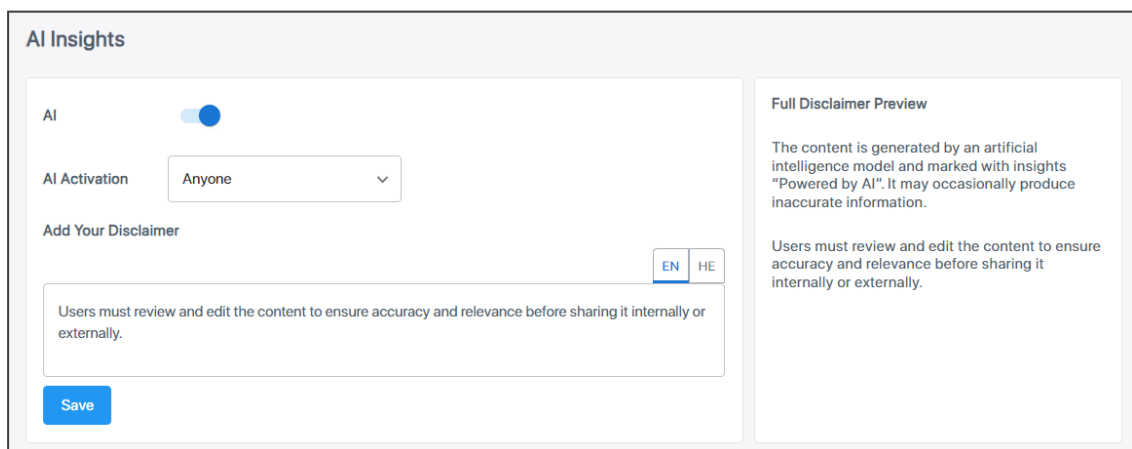


The screenshot shows the 'Transcription' settings panel. It has a title 'Transcription' at the top. Below it, there are three settings: 'Transcription' with a toggle switch that is turned on (blue), 'Languages' with a dropdown menu showing 'English (United States)' and a close button 'x', and 'Transcription Activation' with a dropdown menu showing 'Meeting Owner'.



The 'Transcription' option is enabled by default.

2. From the 'Transcription Activation' drop-down, select either:
  - **Meeting Owner** - only the meeting owner or a user with edit permissions can activate Transcription
  - **Anyone** - anyone with access to the meeting can activate the Transcription
3. Under the 'AI Settings' menu, click the **AI Insights** option.



The screenshot shows the 'AI Insights' settings panel. It has a title 'AI Insights' at the top. Below it, there are three settings: 'AI' with a toggle switch that is turned on (blue), 'AI Activation' with a dropdown menu showing 'Anyone', and 'Add Your Disclaimer' with a text area containing the text 'Users must review and edit the content to ensure accuracy and relevance before sharing it internally or externally.' There are two buttons, 'EN' and 'HE', next to the text area. At the bottom left, there is a 'Save' button. On the right side, there is a 'Full Disclaimer Preview' section with the text: 'The content is generated by an artificial intelligence model and marked with insights "Powered by AI". It may occasionally produce inaccurate information. Users must review and edit the content to ensure accuracy and relevance before sharing it internally or externally.'



- The AI Insights feature is enabled by default. It can be disabled if needed. Disabling the feature is optional.
- If the AI Insights feature is disabled, admin will view the AIs of old meetings but will not be able to trigger new.

4. From the 'AI Activation' drop-down, select either:
  - **Anyone** - anyone with access to the meeting can run AI
  - **Meeting Owner** - only the meeting owner or a user with edit permissions can run AI
5. [Optionally] Add your disclaimer and click **Save**.

## 10 Monitoring

Two menu options are available:

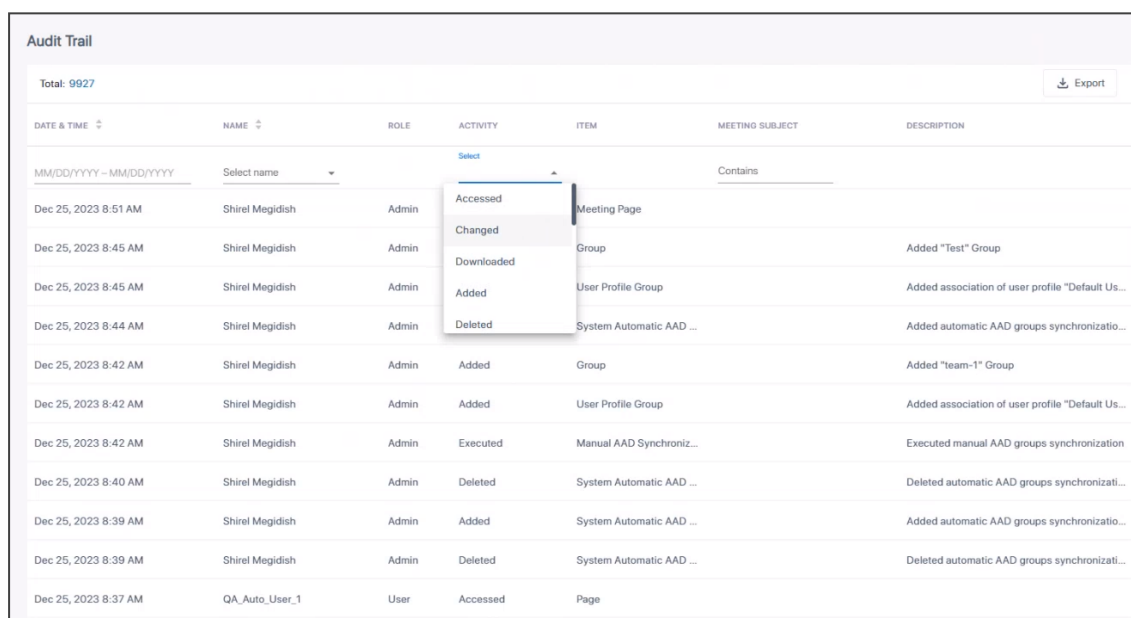
- [Audit Trail](#)
- [System Activity Log](#)

### Audit Trail

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

#### ➤ To monitor the audit trail:

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



The screenshot shows the 'Audit Trail' interface. At the top, it says 'Total: 9927' and has an 'Export' button. Below is a table with columns: DATE & TIME, NAME, ROLE, ACTIVITY, ITEM, MEETING SUBJECT, and DESCRIPTION. A filter dropdown is open over the 'ACTIVITY' column, showing options: Accessed, Changed, Downloaded, Added, and Deleted. The table contains several rows of activity logs, including actions like 'Meeting Page', 'Group', 'User Profile Group', and 'System Automatic AAD ...'.

DATE & TIME	NAME	ROLE	ACTIVITY	ITEM	MEETING SUBJECT	DESCRIPTION
MM/DD/YYYY - MM/DD/YYYY	Select name		Select		Contains	
Dec 25, 2023 8:51 AM	Shirel Megidish	Admin	Accessed	Meeting Page		
Dec 25, 2023 8:45 AM	Shirel Megidish	Admin	Changed	Group		Added "Test" Group
Dec 25, 2023 8:45 AM	Shirel Megidish	Admin	Downloaded	User Profile Group		Added association of user profile "Default Us...
Dec 25, 2023 8:44 AM	Shirel Megidish	Admin	Added	System Automatic AAD ...		Added automatic AAD groups synchronizatio...
Dec 25, 2023 8:42 AM	Shirel Megidish	Admin	Deleted	Group		Added "team-1" Group
Dec 25, 2023 8:42 AM	Shirel Megidish	Admin	Added	User Profile Group		Added association of user profile "Default Us...
Dec 25, 2023 8:42 AM	Shirel Megidish	Admin	Executed	Manual AAD Synchroniz...		Executed manual AAD groups synchronization
Dec 25, 2023 8:40 AM	Shirel Megidish	Admin	Deleted	System Automatic AAD ...		Deleted automatic AAD groups synchronizati...
Dec 25, 2023 8:39 AM	Shirel Megidish	Admin	Added	System Automatic AAD ...		Added automatic AAD groups synchronizatio...
Dec 25, 2023 8:39 AM	Shirel Megidish	Admin	Deleted	System Automatic AAD ...		Deleted automatic AAD groups synchronizati...
Dec 25, 2023 8:37 AM	QA_Auto_User_1	User	Accessed	Page		

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.

Audit Trail						
Total: 8 <span>Export</span>						
DATE & TIME	NAME	ROLE	ACTIVITY	ITEM	MEETING SUBJECT	DESCRIPTION
MM/DD/YYYY - MM/DD/YYYY	Select name		Select Changed		Contains	
Jan 10, 2024 10:04 AM	MOD Administrator	Admin	Changed	Meeting Admin Mode		ON
Jan 9, 2024 11:01 AM	MOD Administrator	Admin	Changed	Meeting Admin Mode		ON
Jan 8, 2024 3:35 PM	MOD Administrator	Admin	Changed	Meeting Admin Mode		ON
Jan 8, 2024 1:21 PM	MOD Administrator	Admin	Changed	Meeting Admin Mode		ON
Jan 8, 2024 12:25 PM	MOD Administrator	Admin	Changed	Meeting Admin Mode		ON
Jan 8, 2024 10:59 AM	MOD Administrator	Admin	Changed	Meeting Admin Mode		ON
Jan 7, 2024 3:06 PM	MOD Administrator	Admin	Changed	User Profile Group		Changed user group "Design" to be associat...
Jan 7, 2024 2:47 PM	MOD Administrator	Admin	Changed	Meeting Admin Mode		ON



- 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.

- [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).
- [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).
- [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.

- 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 -or-
- 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.

### ➤ To filter the System Activity Log:

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

Total 95 Selected 18 Select All					Export
<input checked="" type="checkbox"/>	DATE AND TIME	LOG TYPE	ACTIVITY TYPE	LOG DESCRIPTION	
MM/DD/YYYY - MM/DD/YYYY					
<input checked="" type="checkbox"/>	Nov 14, 2023 10:28 AM	warning	license	Some users are assigned to multiple AAD groups, each associated with different User Profiles having distinct storage or retention settings. When users are assigned to User Profiles with varying storage locations or retention periods, the longest retention policy will be applied, and storage locations may be assigned arbitrarily. Please ensure that all users belong to a single AAD group mapped to Meeting Insights.	<a href="#">See Full List Of Users</a>
<input checked="" type="checkbox"/>	Nov 13, 2023 5:34 PM	warning	license	15 new users were assigned with the license. Overall 15 users exceed the number of available licenses.	
<input checked="" type="checkbox"/>	Nov 13, 2023 5:34 PM	warning	license	Some users are assigned to multiple AAD groups, each associated with different User Profiles having distinct storage or retention settings. When users are assigned to User Profiles with varying storage locations or retention periods, the longest retention policy will be applied, and storage locations may be assigned arbitrarily. Please ensure that all users belong to a single AAD group mapped to Meeting Insights.	<a href="#">See Full List Of Users</a>
<input checked="" type="checkbox"/>	Nov 13, 2023 5:33 PM	info	license	18 users were unassigned from the licenses.	
<input checked="" type="checkbox"/>	Nov 13, 2023 5:32 PM	warning	license	Some users are assigned to multiple AAD groups, each associated with different User Profiles having distinct storage or retention settings. When users are assigned to User Profiles with varying storage locations or retention periods, the longest retention policy will be applied, and storage locations may be assigned arbitrarily. Please ensure that all users belong to a single AAD group mapped to Meeting Insights.	<a href="#">See Full List Of Users</a>
<input checked="" type="checkbox"/>	Nov 13, 2023 5:00 PM	warning	license	2 new users were assigned with the license. Overall 18 users exceed the number of available licenses.	
<input checked="" type="checkbox"/>	Nov 13, 2023 5:00 PM	warning	license	Some users are assigned to multiple AAD groups, each associated with different User Profiles having distinct storage or retention settings. When users are assigned to User Profiles with varying storage locations or retention periods, the longest retention policy will be applied, and storage locations may be assigned arbitrarily. Please ensure that all users belong to a single AAD group mapped to Meeting Insights.	<a href="#">See Full List Of Users</a>
<input checked="" type="checkbox"/>	Nov 13, 2023 4:59 PM	warning	license	2 users were unassigned from the license. 16 users exceed the number of available licenses.	
<input checked="" type="checkbox"/>	Nov 13, 2023 4:59 PM	warning	license	Some users are assigned to multiple AAD groups, each associated with different User Profiles having distinct storage or retention settings. When users are assigned to User Profiles with varying storage locations or retention periods, the longest retention policy will be applied, and storage locations may be assigned arbitrarily. Please ensure that all users belong to a single AAD group mapped to Meeting Insights.	

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.



Total 95 Selected 18 [Select All](#) [Export](#)

DATE AND TIME LOG TYPE ACTIVITY TYPE LOG DESCRIPTION

MM/DD/YYYY - MM/DD/YYYY

DATE AND TIME	LOG TYPE	ACTIVITY TYPE	LOG DESCRIPTION
<input checked="" type="checkbox"/> Nov 14, 2023 10:28 AM	warning	license	Some users are assigned to multiple AAD groups, each associated with different User Profiles having distinct storage or retention settings. When users are assigned to User Profiles with varying storage locations or retention periods, the longest retention policy will be applied, and storage locations may be assigned arbitrarily. Please ensure that all users belong to a single AAD group mapped to Meeting Insights.
<input checked="" type="checkbox"/> Nov 13, 2023 5:34 PM			
<input checked="" type="checkbox"/> Nov 13, 2023 5:34 PM			
<input checked="" type="checkbox"/> Nov 13, 2023 5:33 PM			
<input checked="" type="checkbox"/> Nov 13, 2023 5:32 PM			
<input checked="" type="checkbox"/> Nov 13, 2023 5:00 PM			
<input checked="" type="checkbox"/> Nov 13, 2023 5:00 PM	warning	license	Some users are assigned to multiple AAD groups, each associated with different User Profiles having distinct storage or retention settings. When users are assigned to User Profiles with varying storage locations or retention periods, the longest retention policy will be applied, and storage locations may be assigned arbitrarily. Please ensure that all users belong to a single AAD group mapped to Meeting Insights.
<input checked="" type="checkbox"/> Nov 13, 2023 4:59 PM	warning	license	2 users were unassigned from the license. 16 users exceed the number of available licenses.
<input checked="" type="checkbox"/> Nov 13, 2023 4:59 PM	warning	license	Some users are assigned to multiple AAD groups, each associated with different User Profiles having distinct storage or retention settings. When users are assigned to User Profiles with varying storage locations or retention periods, the longest retention policy will be applied, and storage locations may be assigned arbitrarily. Please ensure that all users belong to a single AAD group mapped to Meeting Insights.

Full list of users

NAME	AAD GROUPS	USER PROFILES
MOD Administrator	All Company, License to users, All Employees	license test- no recording, Default User Profile (System)
Christie Cline	License to users, All Employees	license test- no recording, Default User Profile (System)
Debra Berger	License to users, All Employees	license test- no recording, Default User Profile (System)
Alex Wilber	ming-main, All Employees	main-profile -- DONT DELETE, Default User Profile (System)
Adele Vance	ming-main, All Employees	main-profile -- DONT DELETE, Default User Profile (System)

- In a log, view for example how many times users were added or removed from a license (the count).
- (Optionally) Click the **Export** button in the uppermost right corner of the page and in the format prompt, click the **Export to Excel** button.

## 11 Integrations

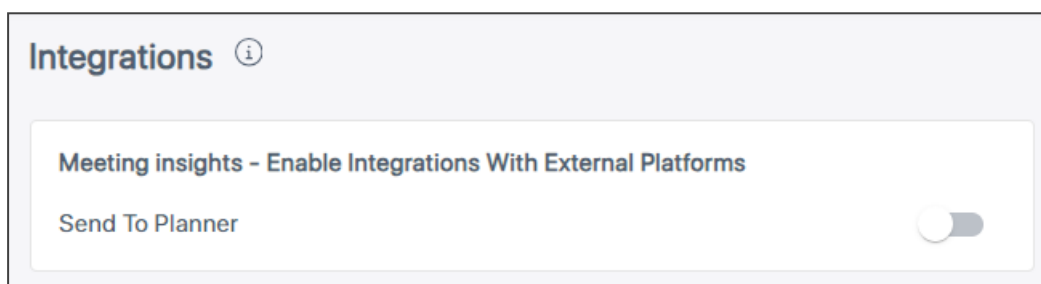
The instructions here show how to integrate Microsoft Planner with Meeting Insights.



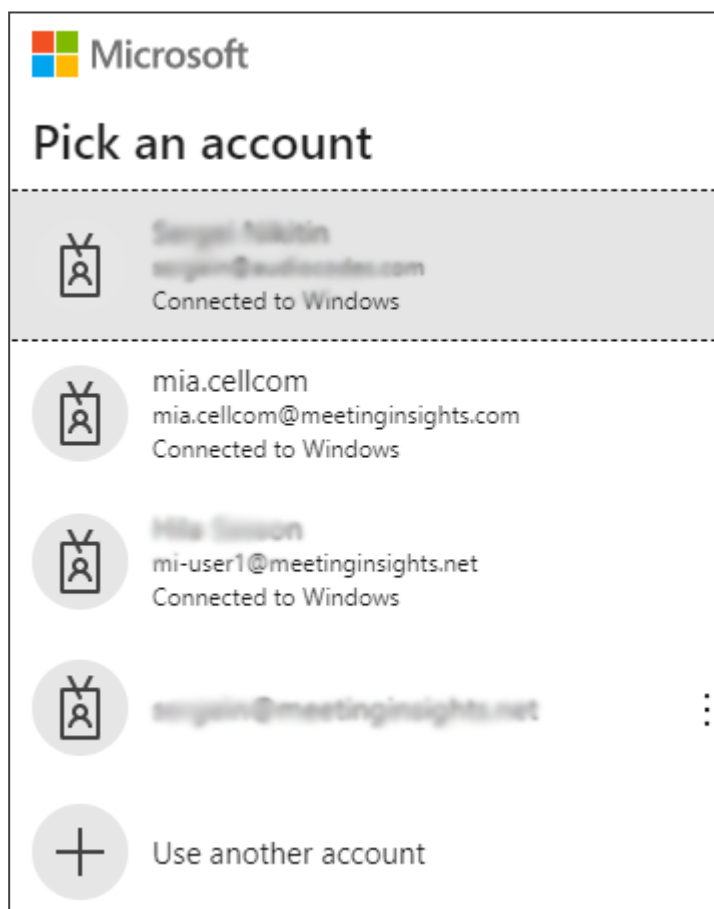
Before integrating Microsoft Planner, the logged-in user must have Meeting Insights 'admin' privileges and Azure 'tenant admin' privileges.

➤ **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.



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**.

### Add Action Item to Planner

Plan

Dorel - private

Bucket

To do

Cancel

Send to Planner

## 12 Configuring Automatic Invitation of MIA to Teams Meetings

Admins can configure automatically inviting Meeting Insights Assistant (MIA) to Teams meetings, whether organized by a specific user or by a group of users. When the user then schedules a Teams 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 meeting's organizer cannot see MIA or the disclaimer when they open the meeting invitation on their side. All other recipients of the meeting invitation view the disclaimer at the top of the body of the invitation.

Take the following three steps to configure an automatic invitation of MIA to Teams 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.

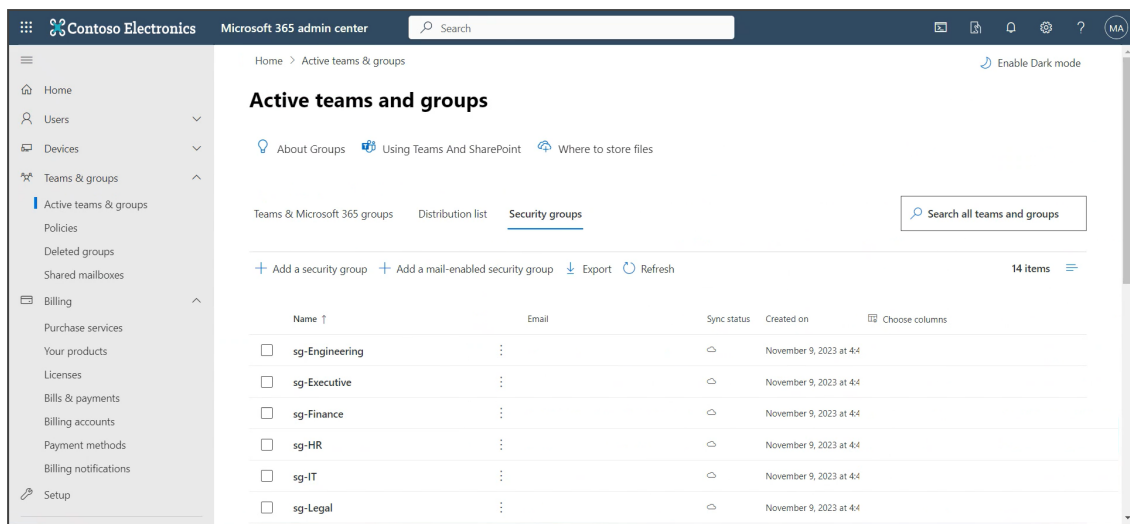
2. Define an auto-invite rule in Exchange admin center. See [here](#) how.
3. Test the rule. See [here](#) how.

### Add a Mail-Enabled Security Group

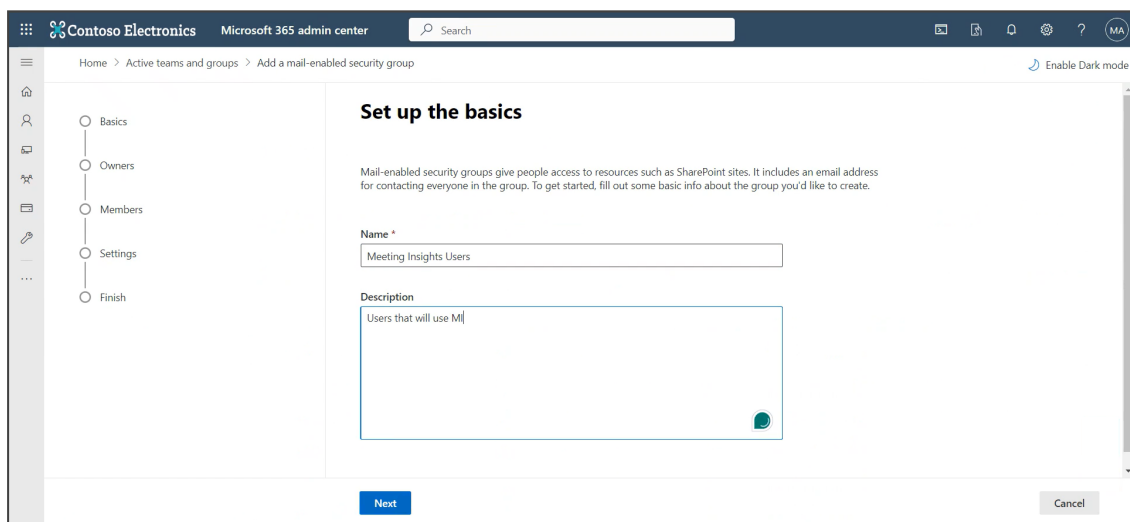
The instructions below focus on how to create a mail-enabled security group through Microsoft 365 admin center.

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

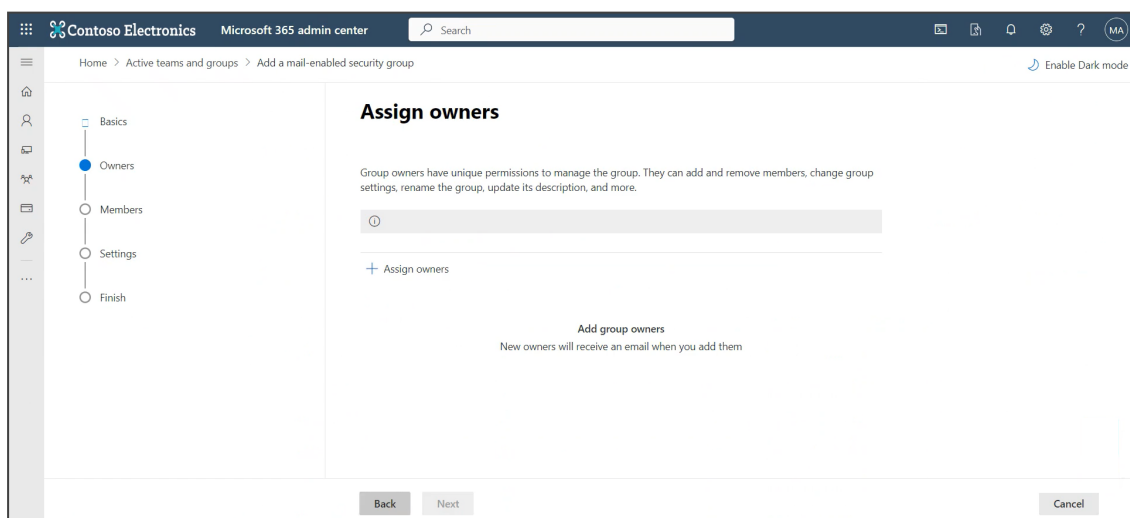
1. In Microsoft 365 admin center, go to **Teams & groups > Active teams & groups > Security Groups** tab.



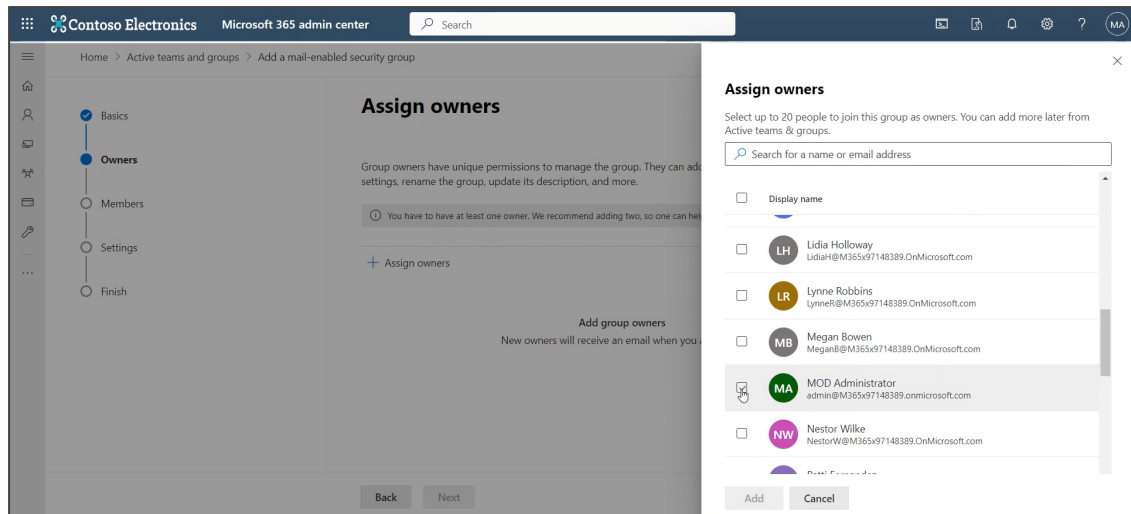
2. In the 'Active teams & groups' page shown above, click **+ Add a mail-enabled security group**.



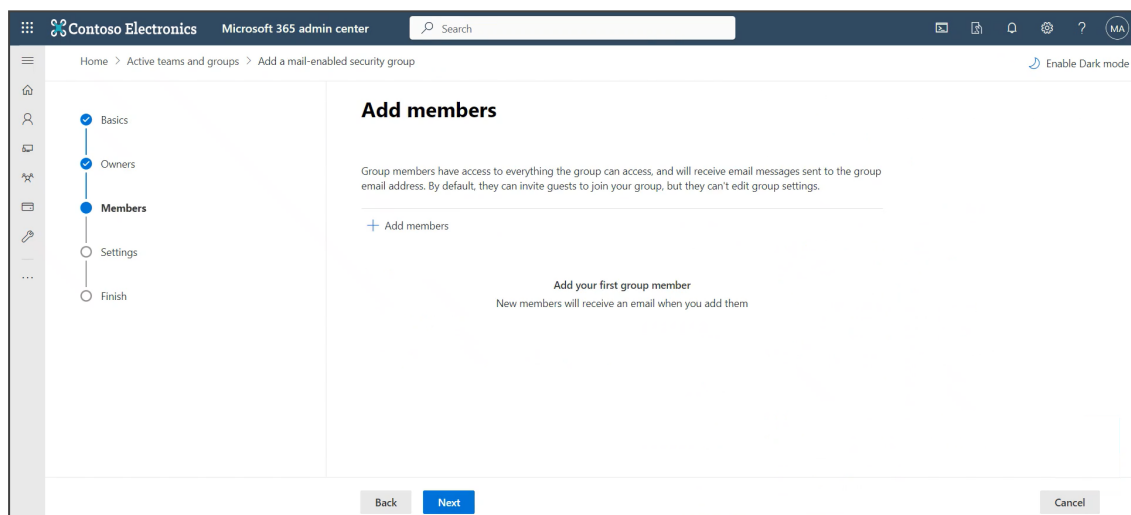
3. In the 'Set up the basics' page shown above, enter **Meeting Insights Users** in the 'Name' field, enter a 'Description' to facilitate effective management later, and then click **Next**.



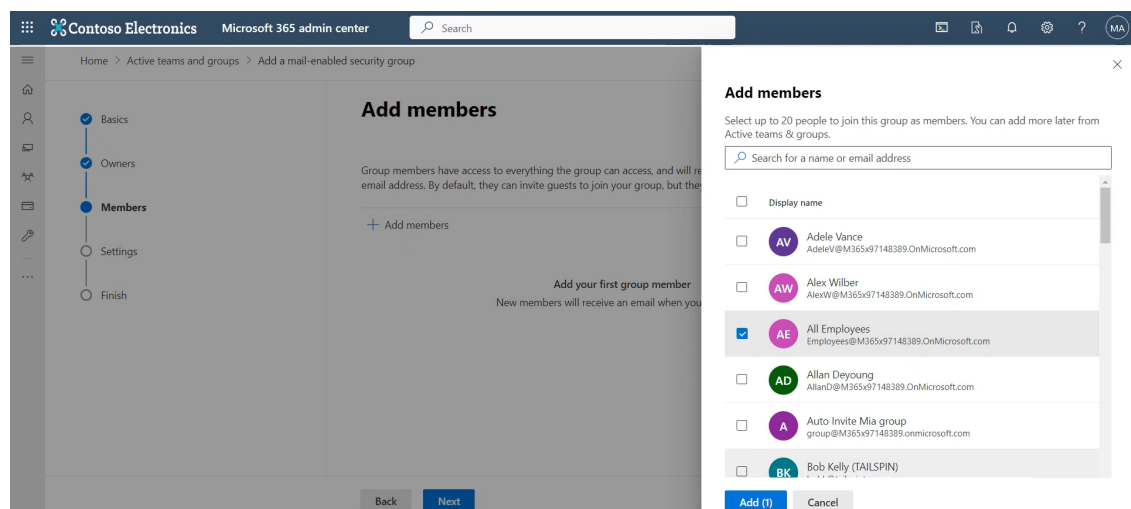
4. In the 'Assign owners' page that opens, click **+ Assign owners**.



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**.

Home > Active teams and groups > Add a mail-enabled security group

✓ Basics

✓ Owners

**Members**

○ Settings


○ Finish

## Add members

Group members have access to everything the group can access, and will receive email messages sent to the group email address. By default, they can invite guests to join your group, but they can't edit group settings.

[+ Add members](#)

☐ Display name

☐  All Employees  
Employees@M365x97148389.OnMicrosoft....

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

Contoso Electronics Microsoft 365 admin center Search

Home > Active teams and groups > Add a mail-enabled security group

✓ Basics

✓ Owners

✓ Members

**Settings**

○ Finish

## Edit settings

Mail-enabled security group

Has all the functionality of a distribution list and additionally can be used to control access to OneDrive and SharePoint.

Group email address \*  Domains

Communication

☐ Allow people outside of my organization to send email to this Mail-enabled security group

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

✓ Basics

✓ Owners

✓ Members

✓ Settings

**Finish**

## Review and finish adding group

You're almost there - make sure everything looks right before adding your new group.

**Group type**  
Mail-enabled security  
[Edit](#)

**Basics**  
Name: Meeting Insights Users  
Description: Users that will use MI  
[Edit](#)

**Owners**  
MOD Administrator  
[Edit](#)

**Members**  
All Employees  
[Edit](#)

Back

Create group

10. Click **Create group**.





## Meeting Insights Users group created

It can take up to an hour for Meeting Insights Users group to appear in your Active teams & groups list. If you don't see your new group yet, go to the [Exchange admin center](#)

### Next steps

[Add another Mail-enabled security group](#)

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

The screenshot shows the 'Active teams and groups' page. At the top, there are tabs for 'Teams & Microsoft 365 groups', 'Distribution list', and 'Security groups'. The 'Security groups' tab is selected. Below the tabs, there is a search bar and a list of security groups. The list has columns for Name, Email, Sync status, and Created on. Two groups are visible: 'Meeting Insights Users' and 'sg-Engineering'.

Name	Email	Sync status	Created on
Meeting Insights Users	MIGroup@M365x97148389.onmicrosoft.com	Syncing	February 9, 2024 at 9:07
sg-Engineering		Syncing	November 9, 2023 at 4:4

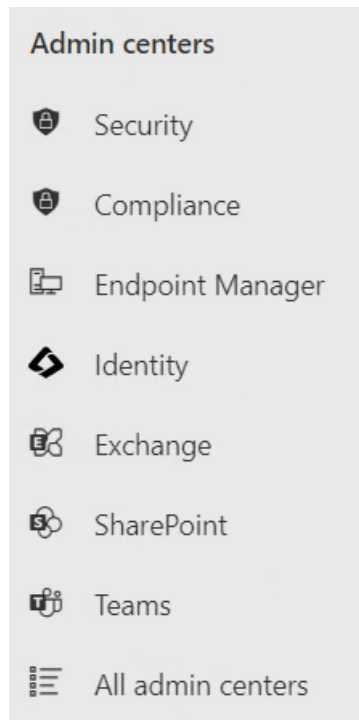
Next: Configure the 'Auto-Invite' rule as shown [here](#).

## Configure an Auto-Invite Rule

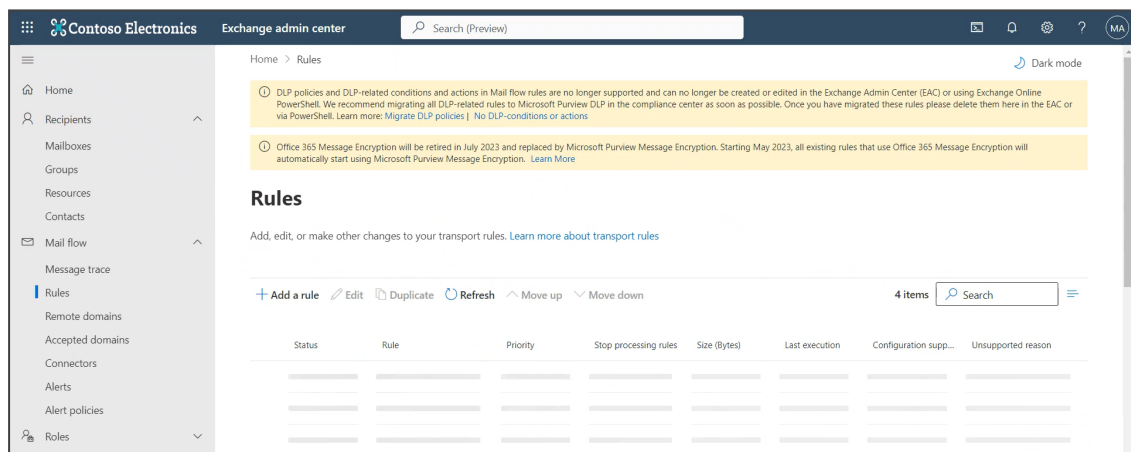
After adding a mail-enabled security group as shown [previously](#), admins can configure an 'Auto-Invite' rule from Microsoft's Exchange admin center. Configuring an Exchange rule from Microsoft 360 admin center involves defining specific conditions, including the message being a calendar event and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

### ➤ 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**.

**New transport rule**

● Set rule conditions  
○ Set rule settings  
○ Review and finish

## Set rule conditions

Name and set conditions for your transport rule

**Name \***  
Auto Invite MIA

**Apply this rule if \***  
The message properties include the message type  
The message type is 'Calendaring'

**And**  
The subject or body subject or body includes any of these ...  
The subject or body includes any of these words 'Microsoft Teams meetings' or 'Microsoft Teams'

**And**  
The sender is a member of this group  
The sender is a member of 'MIGroup@M365x97148389.onmicrosoft.com'

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** -OR- **Microsoft Teams** 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:**

**New transport rule**

Set rule conditions  
Set rule settings  
Review and finish

**Do the following \***

Apply a disclaimer to the message ▾ prepend a disclaimer ▾ + ▢

Prepend 'Disclaimer: The meeting will be recorded' and fall back to action 'Wrap' if the disclaimer can't be inserted ✎

**And**

Add recipients ▾ to the To box ▾ ▢

Add these recipients to the To box 'mia.Tania-8389@meetinginsights.com' ✎

**Except if**

The message ▾ To or Cc box contains this person ▾ + ▢

The To or Cc box contains 'mia.Tania-8389@meetinginsights.com' ✎

**Or**

The subject or body ▾ subject matches these text patterns ▾ ▢

The subject matches these text patterns '^Canceled:' ✎

**Next**

6. Click **Next**.

The screenshot shows the 'Set rule settings' page for a new transport rule. On the left, a sidebar titled 'New transport rule' contains three steps: 'Set rule conditions' (checked), 'Set rule settings' (active), and 'Review and finish'. The main content area is titled 'Set rule settings' and includes the instruction 'Set settings for your transport rule'. Under 'Rule mode', the 'Enforce' option is selected. The 'Severity' dropdown is set to 'Not specified'. There are two sections for scheduling: 'Activate this rule on' and 'Deactivate this rule on', both with date and time pickers set to 2/9/2024 at 4:00 PM. At the bottom, there is a 'Stop process' checkbox and 'Back' and 'Next' buttons.

**New transport rule**

- Set rule conditions
- Set rule settings**
- Review and finish

## Set rule settings

Set settings for your transport rule

**Rule mode**

- ☒ Enforce
- ☐ Test with Policy Tips
- ☐ Test without Policy Tips

**Severity \***

Not specified

☐ Activate this rule on

2/9/2024 - 4:00 PM

☐ Deactivate this rule on

2/9/2024 - 4:00 PM

☐ Stop process

Back Next

7. Set the rule settings as follows:

- Leave 'Rule mode' at its default **Enforce**.
- 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).
- Select 'Activate this rule on' and set it to take effect immediately.
- From the 'Match sender address in message' drop-down, select **Header**.

8. Click **Next**.

**New transport rule**

- Set rule conditions
- Set rule settings
- Review and finish**

## Review and finish

After your finish creating this rule, it is turned off by default until you turn it on from the Rules page

**Rule name**  
Auto Invite Mia

**Rule comments**

---

**Rule conditions**

**Apply this rule if**  
The message type is 'Calendaring'  
The subject or body includes any of these words 'Microsoft Teams meeting'  
The sender is a member of 'MIGroup@M365x97148389.onmicrosoft.com'

**Do the following**  
Prepend 'Disclaimer: The meeting will be recorded' and fall back to action 'Wrap' if the disclaimer can't be inserted  
Add these recipients to the To box 'mia.tania-8389@meetinginsights.com'

**Except if**

**Rule settings**

**Mode**  
Enforce

**Set date range**  
Specific date range is not set

**Priority**  
4

**Severity**  
Not specified

**For rule processing errors**  
Ignore

[Back](#) [Finish](#)

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

**New transport rule**

- Set rule conditions
- Set rule settings
- Review and finish

Transport rule created successfully

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

Contoso Electronics Exchange admin center

Search (Preview)

DLP policies and DLP-related conditions and actions in Mail flow rules are no longer supported and can no longer be created or edited in the Exchange Admin Center (EAC) or using Exchange Online PowerShell. We recommend migrating all DLP-related rules to Microsoft Purview DLP in the compliance center as soon as possible. Once you have migrated these rules please delete them here in the EAC or via PowerShell. [Learn more: Migrate DLP policies](#) | [No DLP-conditions or actions](#)

Office 365 Message Encryption will be retired in July 2023 and replaced by Microsoft Purview Message Encryption. Starting May 2023, all existing rules that use Office 365 Message Encryption will automatically start using Microsoft Purview Message Encryption. [Learn More](#)

### Rules

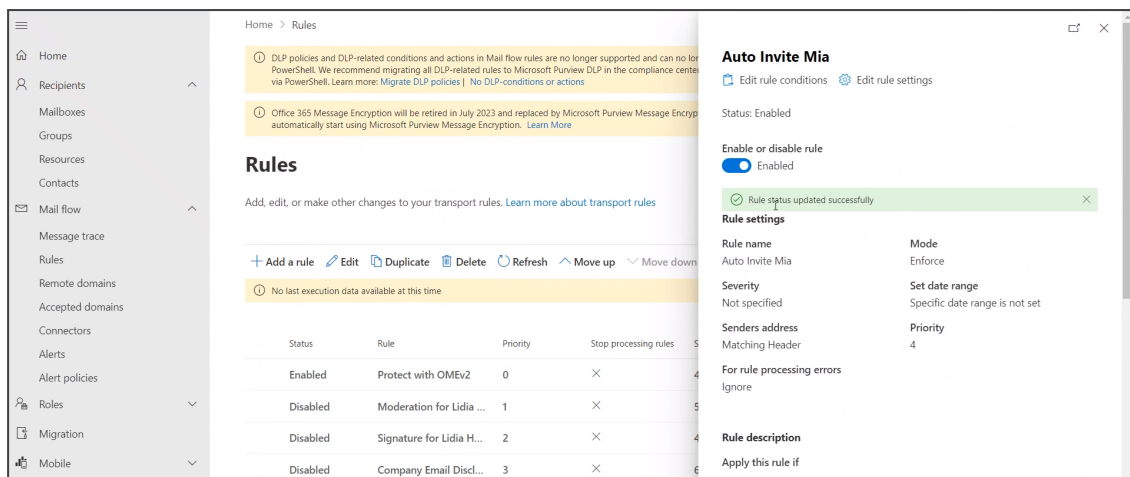
Add, edit, or make other changes to your transport rules. [Learn more about transport rules](#)

+ Add a rule Edit Duplicate Delete Refresh Move up Move down 5 items 1 selected Search

No last execution data available at this time

Status	Rule	Priority	Stop processing rules	Size (Bytes)	Last execution	Configuration supp...	Unsupported reason
Enabled	Protect with OMEv2	0	×	477		✓	
Disabled	Moderation for Lidia ...	1	×	524		✓	
Disabled	Signature for Lidia H...	2	×	471		✓	
Disabled	Company Email Discl...	3	×	642		✓	
Disabled	Auto Invite Mia	4	×	980		✓	

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

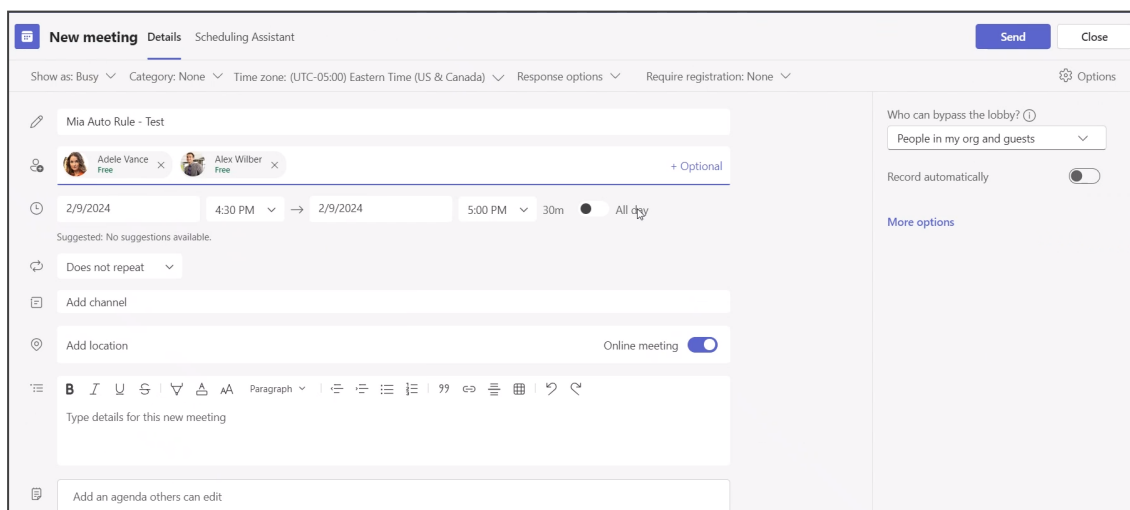


It takes up to 30 minutes for the MIA 'Auto-Invite' rule to take effect.

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.

**Meeting join & lobby**

Meeting join and lobby settings let you control how people join meetings and allow you to manage the lobby for Teams meetings.  
[Learn more about meeting join and lobby settings](#)

Anonymous users can join a meeting ⓘ ☒ On  
Find related settings at [Meetings > Live events policies](#) and [Meetings > Meeting settings](#)

Anonymous users and dial-in callers can start a meeting ⓘ ☐ Off

Who can bypass the lobby ⓘ People in my org

People dialing in can bypass the lobby ⓘ Everyone

People can join external meetings hosted by ⓘ People in my org

**Meeting engagement**

Meeting engagement settings let you control how people

Meeting chat ⓘ On for everyone  
Find related settings at [Messaging > Messaging policies](#)

External meeting chat ⓘ ☒ On

Save Cancel



## 13 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

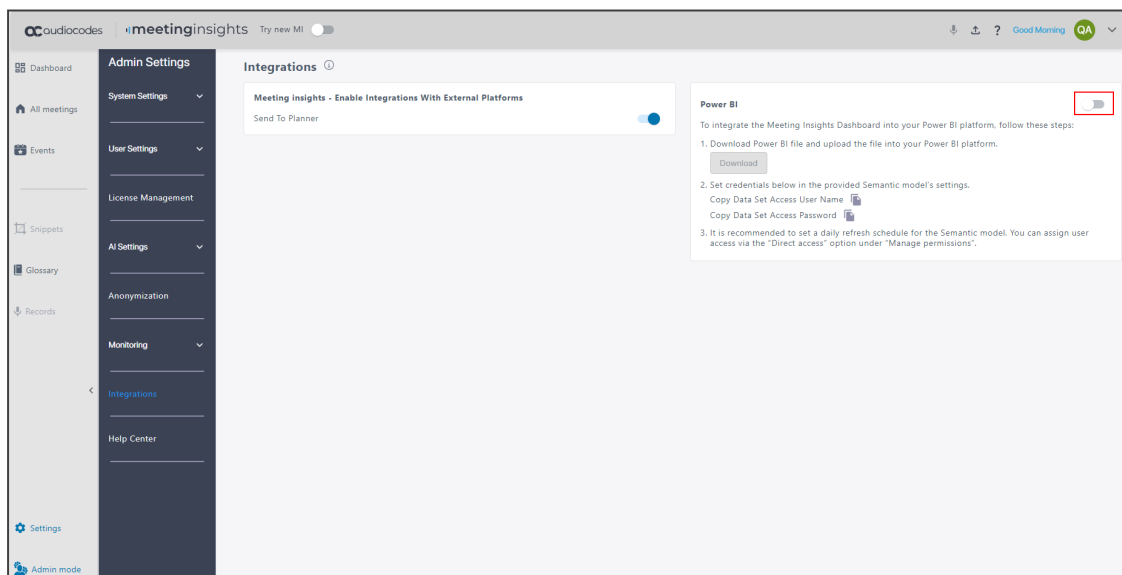
The instructions below show admin how to enable Power BI integration in Meeting Insights.



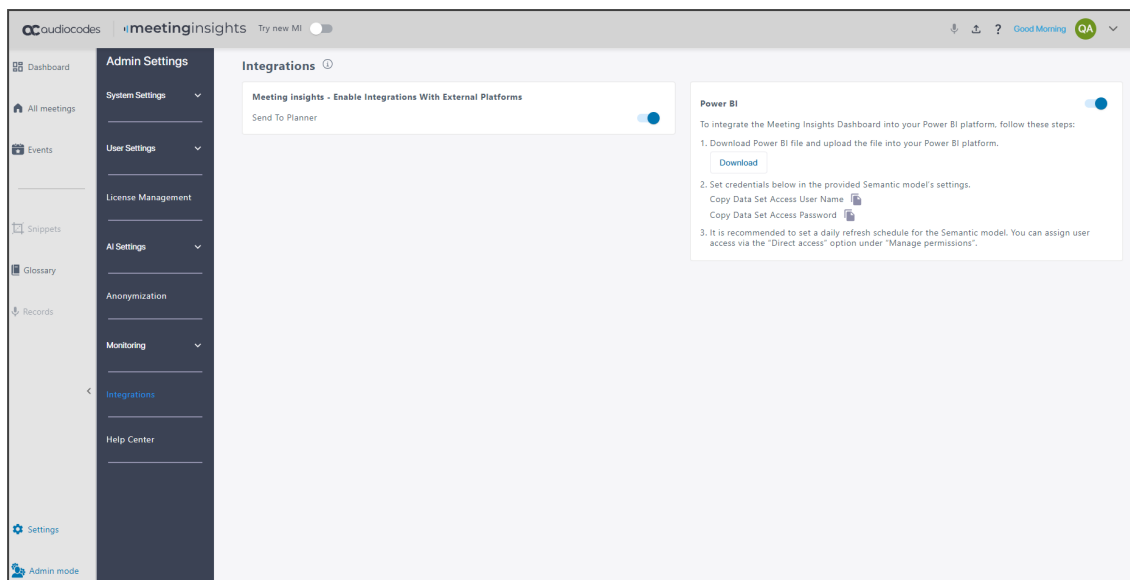
- Admin will view the integration only if it is enabled for their application.
- If you don't have it and you want to have it, contact the Service Provider.

#### ➤ 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.

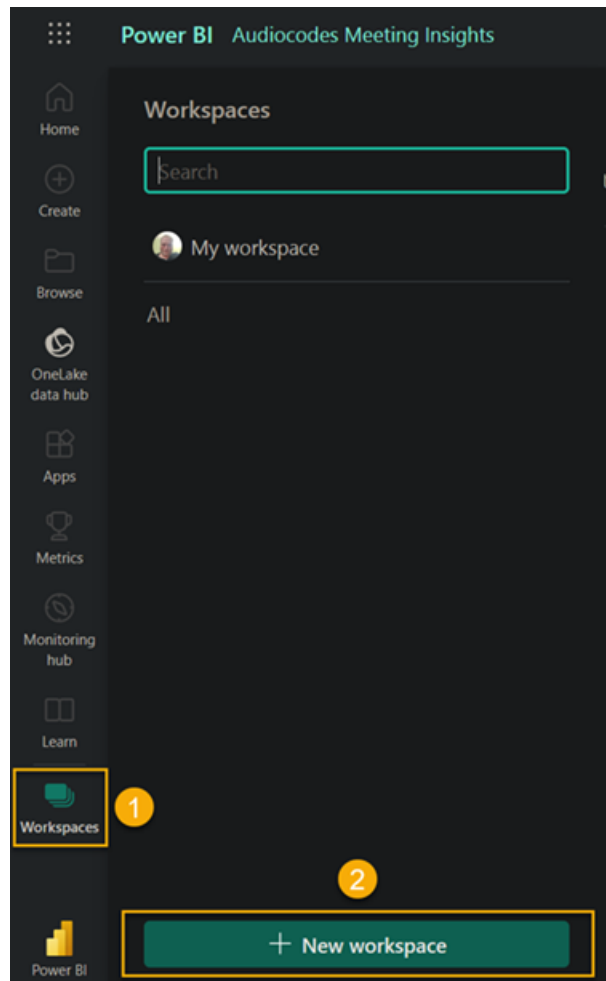


### Prerequisites

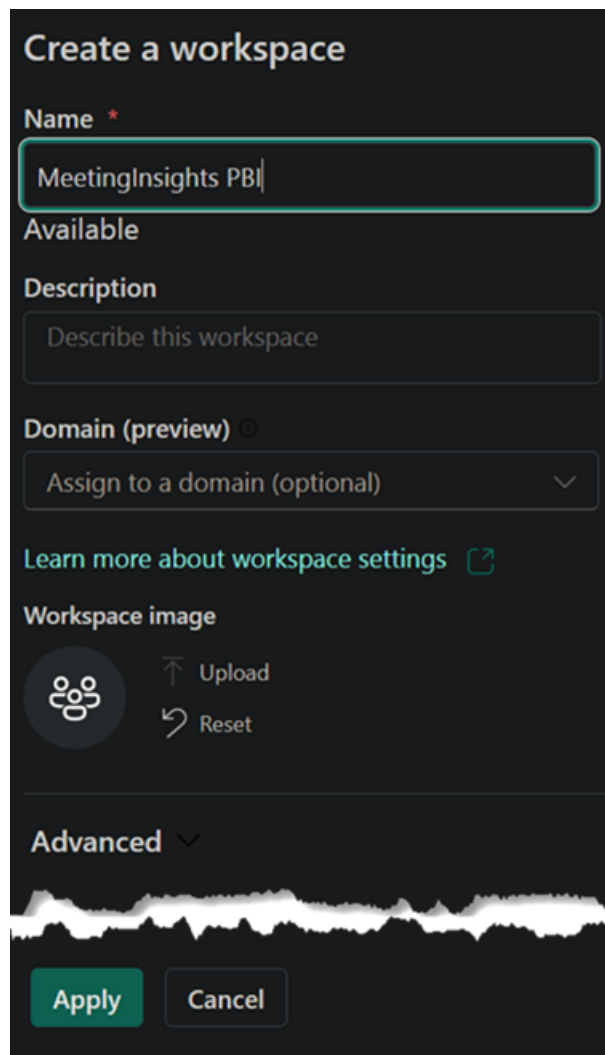
- Office 365 E5 customer account or any Office 365 licensed account with an individual Power BI Pro license attached.
- One Power BI Pro license is included with Microsoft E5 license.

### ➤ To install | configure Power BI:

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



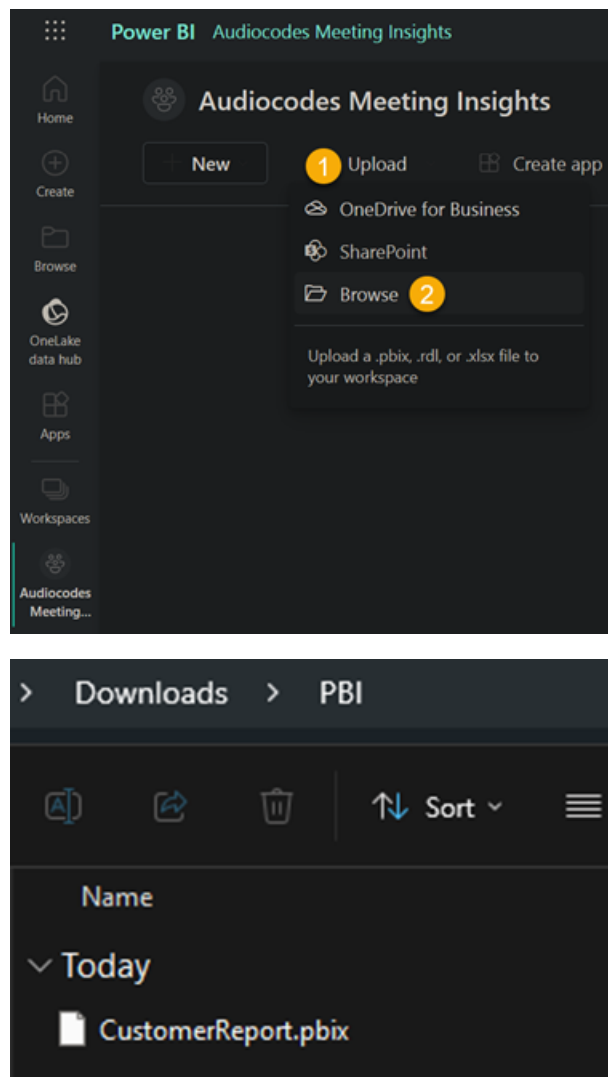
2. Click + **New workspace**.



The screenshot shows a 'Create a workspace' form with a dark theme. The form includes the following fields and options:

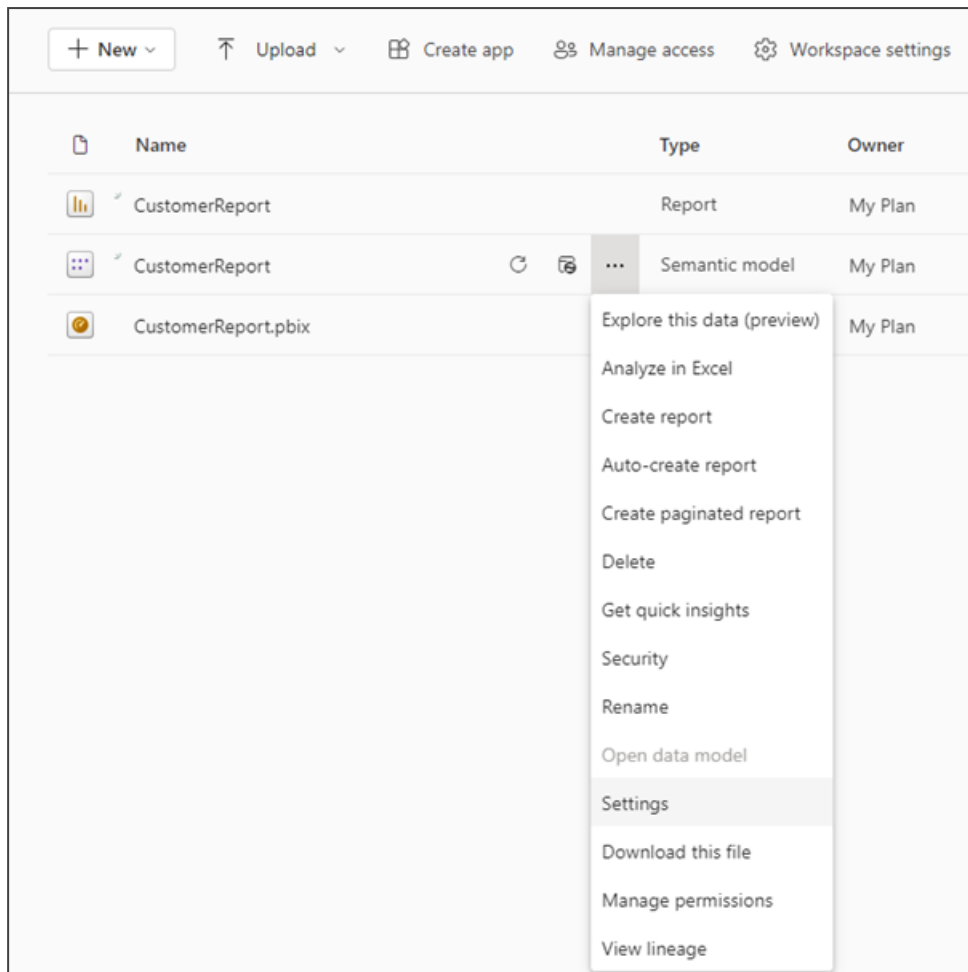
- Name \***: A text input field containing 'MeetingInsights PBI'.
- Available**: A checkbox that is currently unchecked.
- Description**: A text input field with the placeholder text 'Describe this workspace'.
- Domain (preview) ⓘ**: A dropdown menu with the option 'Assign to a domain (optional)' and a downward arrow.
- Learn more about workspace settings**: A link with an external link icon.
- Workspace image**: A section containing a circular icon with three people, an 'Upload' button with an upward arrow, and a 'Reset' button with a circular arrow.
- Advanced**: A section header with a downward arrow.
- Buttons**: 'Apply' and 'Cancel' buttons at the bottom.

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](#).

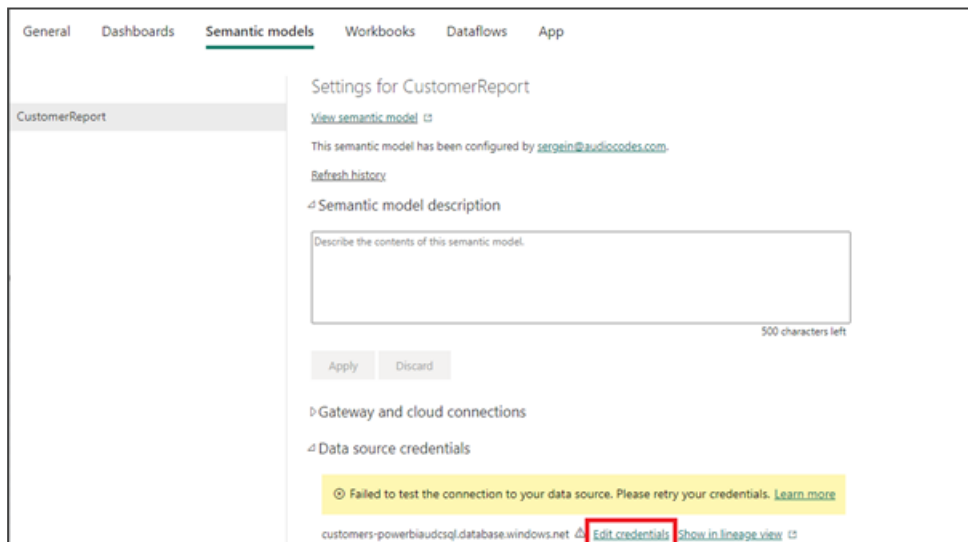
<div> <div>+ New</div> <div> <div>↑ Upload</div> <div>⊞ Create app</div> <div>⚙ Manage access</div> <div>⚙ Workspace settings</div> </div> </div>			
	Name	Type	Owner
	✓ CustomerReport	Report	My Plan
	✓ CustomerReport	Semantic model	My Plan
	✓ CustomerReport.pbix	Dashboard	My Plan



The screenshot shows the top navigation bar of the Power BI workspace with buttons for '+ New', 'Upload', 'Create app', 'Manage access', and 'Workspace settings'. Below is a table listing items:

Name	Type	Owner
CustomerReport	Report	My Plan
CustomerReport	Semantic model	My Plan
CustomerReport.pbix		My Plan

A context menu is open for the 'CustomerReport' semantic model, showing options: 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, and View lineage.



The screenshot shows the 'Semantic models' tab with the 'Settings for CustomerReport' page. The page includes a 'View semantic model' link, a message about configuration by 'sergein@audiocodes.com', a 'Refresh history' link, and a 'Semantic model description' text area (500 characters left). Below are sections for 'Gateway and cloud connections' and 'Data source credentials'. A yellow error banner states: 'Failed to test the connection to your data source. Please retry your credentials. Learn more'. At the bottom, the data source is 'customers-powerbiaudcsqldatabase.windows.net' with links for 'Edit credentials' and 'Show in lineage view'.

### Configure CustomerReport

server  
powerbiaudcsql.database.windows.net

database  
customers

Authentication method  
Basic

User name

Password

Privacy level setting for this data source  
Organizational

☐ Report viewers can only access this data source with their own Power BI identities using DirectQuery. [Learn more](#)

**Sign in** **Cancel**

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

#### Refresh

**Configure a refresh schedule**  
Define a data refresh schedule to import data from the data source

☒ On

Refresh frequency  
Daily

Time zone  
(UTC+02:00) Athens, Bucharest

Time  
[Add another time](#)

**Send refresh failure notifications to**

☒ Semantic model owner

☒ These contacts:

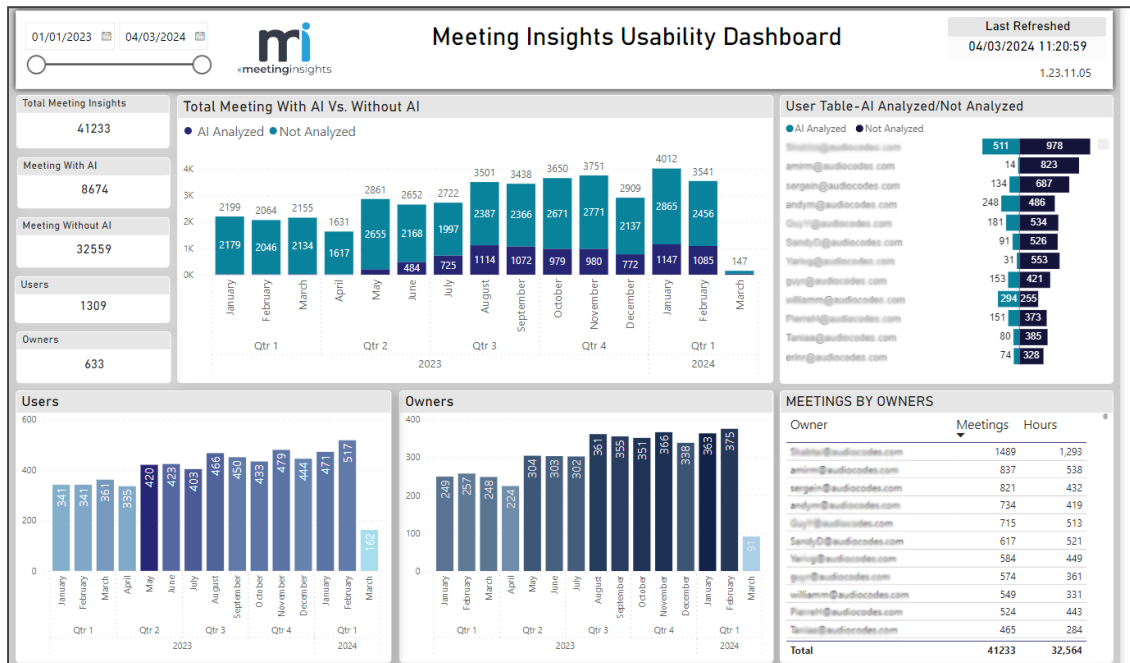
7. Go back to the Workspaces page and click **Refresh now** in the 'Semantic model' item.

Name	Type	Owner	Refreshed	Next refresh	Endorsement	Sensitivity	Included in app
CustomerReport	Report	My Plan	3/10/24, 9:24:19 AM	—	—	—	<input type="checkbox"/> No
CustomerReport	Semantic model	My Plan	3/10/24, 9:24:19 AM	N/A	—	—	<input type="checkbox"/> No
CustomerReport.pbix	Dashboard	My Plan	—	—	—	—	<input type="checkbox"/> No

## 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.

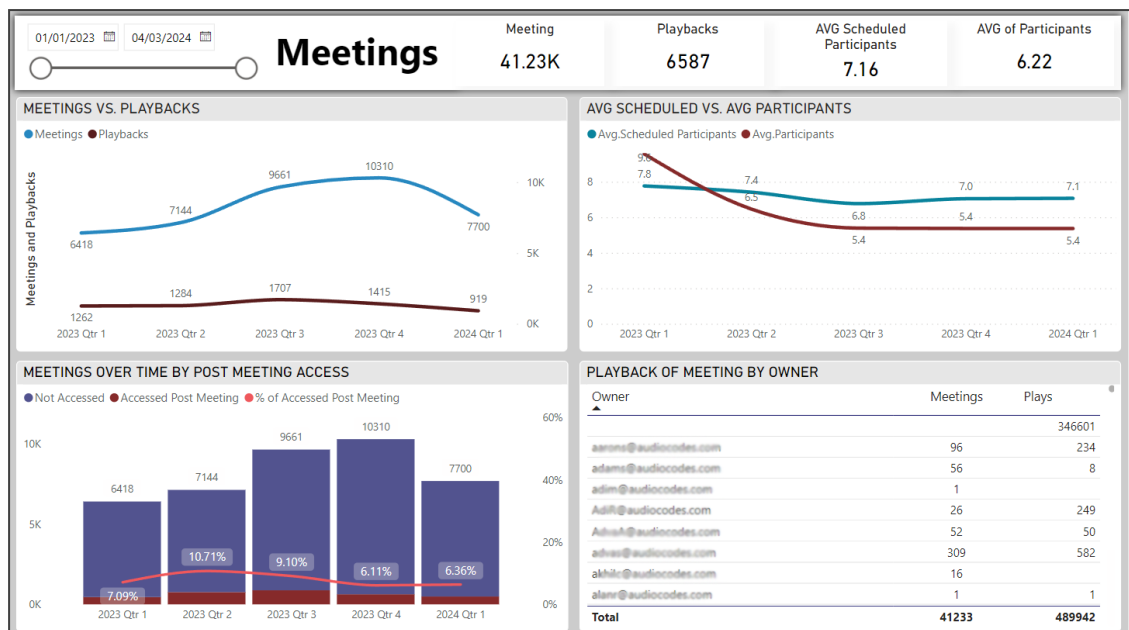
[Refer to the preceding figure] Admin can assess at a glance how many meetings with Meeting Insights *in total* were held in the enterprise over a period of time defined in the uppermost left corner of the page. Admin can moreover assess how many of those meetings were analyzed using AI, versus how many 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.

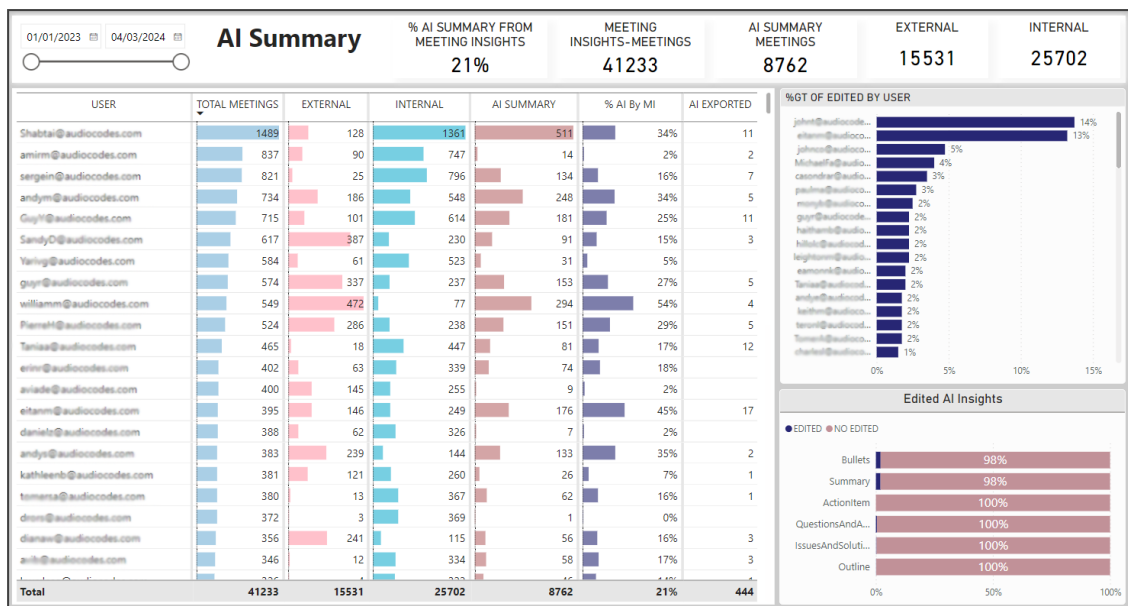
The **Average Scheduled vs. Average Participants** graph shows the # of invitees that were *invited* to meetings vs. the # of invitees that *actively participated* in those meetings. These statistics demonstrate product effectiveness, helping administrators and/or management assess whether they're getting 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 # of *external 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 # of *internal 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:

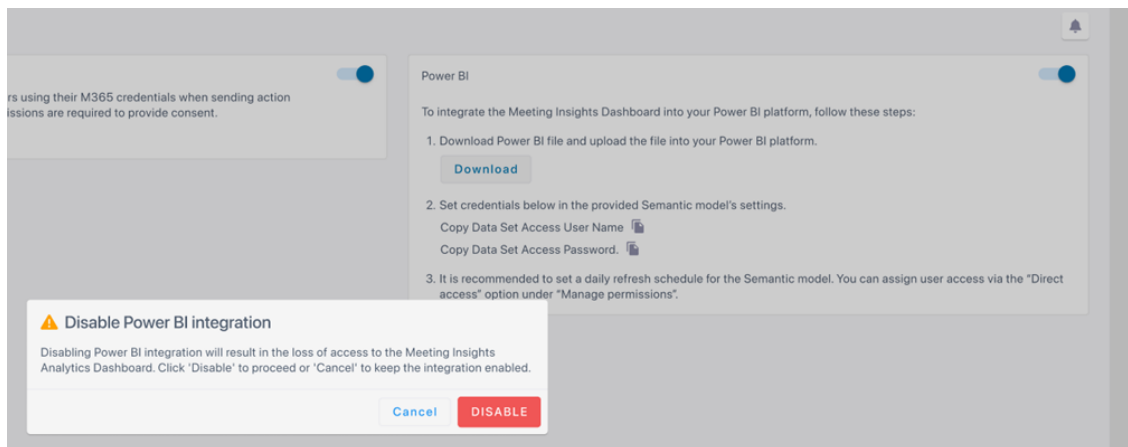
- extent to which and depth at which users are engaging with the app
- app's value proposition
- app's ROI
- benefit the organization derives from the service

## 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:



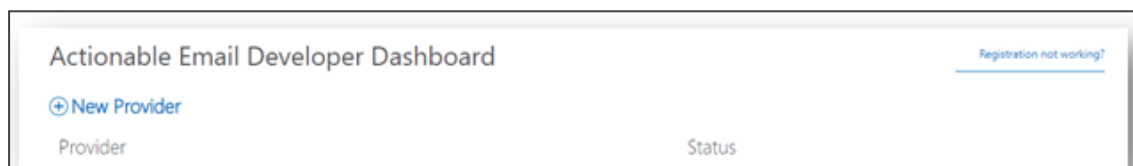
3. Click **DISABLE**.

## 14 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

- 101 -

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**.

## 15 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)
- 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>

©2024 AudioCodes Ltd.. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, and AudioCodes Room Experience are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-12751

