Administrator's Manual

AudioCodes Voice.AI

AudioCodes Live SmartTAP

Enterprise Service

AudioCodes Live SmartTAP

audiocodes

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: October-20-2024

Security Vulnerabilities

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

Customer Support

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

Documentation Feedback

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

Stay in the Loop with AudioCodes

Documentation Revision Record

LTRT	Description
LTRT-27607	Initial document release for Version 1.0.
LTRT-27608	Update to Section Managing Users; syntax corrections

Table of Contents

1 About SmartTAP Recordings 1

Benefits 2
Features Overview 3

2 Adding Enterprise Service 5

Prerequisites 5
Create AAD Recording Groups 5
Logging into SmartTAP Interface 8
Quick Start 15
Web Interface Elements 32
Settings Navigation Pane 32
Toolbar 33
Monitor Onboarding Process in Live Platform 34
Add Live Platform Operators 36
Add and Pin SmartTAP Teams App 43

3 Day Two Management using the SmartTAP User Interface 46

Recording Settings 47
Managing Recording Profiles 47
Adding Recording Profiles 48
Modifying Recording Profiles 66
Viewing Recording Profiles 71
Synchronizing Recording Profiles 71
Download and Run Microsoft Script 73
Disabling Recording Profile 79
Deleting Recording Profile 80
Recording Profile-Call Type Configuration Examples 81
Managing Access Profiles 82
Adding an Access Profile 83
Modifying Access Profiles 88
Viewing Access Profiles 90
Deleting Access Profiles 92
Viewing Global Admin Details 93
Interactions 94
Filtering Interactions and Active Calls Information 100
Filtering by Call Status 101
Filtering by Users and Groups 103
Filtering by Date 104
Filtering by Call Direction 106
Filtering by Call Tags 106
Filtering by Called or Calling Party 107
Filtering by Answering Party 107
Filtering by Participants 108

Filtering by Call Type 109
Filtering by Notes 110
Filtering by Release Cause 110
Saving Queries 111
Listening to Voice Interaction 112
Filtering in Time line 116
Downloading an Audio Call 117
Exporting Interaction to Excel 118
Deleting Calls 122
Customizing Columns 124
Assigning Tags to Interactions 126
Adding Notes to Interactions 129
Managing Active Calls 132
Assigning Tags to Active Calls 132
Adding Notes to Active Calls 137
Exporting Active Calls 138
My Active Call 143
System Settings 146
Connect to M365 146
Tools 148
Bring-Your-Own-Storage 153
Manage Tags 159
Branding 161
Licenses 163
Monitoring 166
Managing Users 166
Exporting Users 167
Deleting Users 169
Placing a User on Legal Hold 170
Viewing and Searching an Audit Trail 172
System Activity Log 175
Alarms 178
Recording Resource Unavailable 178
Connection Failed 179

1 About SmartTAP Recordings

- Compliance, Quality, Malicious and other use cases for Call Recording: AudioCodes Live SmartTAP is a fully secured, intelligent enterprise compliance-recording solution that empowers organizations to effortlessly capture, index and ensure the quality of all customer and internal interactions, spanning external and internal communication channels. For Microsoft Teams users, seamlessly records voice interactions to meet regulatory compliance requirements. This comprehensive solution provides organizations with the assurance of both compliance and the highest standards of communication quality.
- SmartTAP Recordings make it easier for your organization to meet and maintain compliance standards such as MiFID II, GDPR, PCI DSS, HIPAA and E-Discovery. An intelligent, cloud-based recording solution ensures that you capture and manage communications seamlessly, so you can focus on what matters most – your business. Stay compliant effortlessly with our real-time monitoring solution.
  - Automatic recording notifications for compliance with regulations.
  - Roles and permissions-based access controls.
  - Flexible retention policies with local (national) storage capabilities for GDPR Compliance.
  - Audit trail of user activities and encrypted media.

Figure 1-1: SmartTAP Page

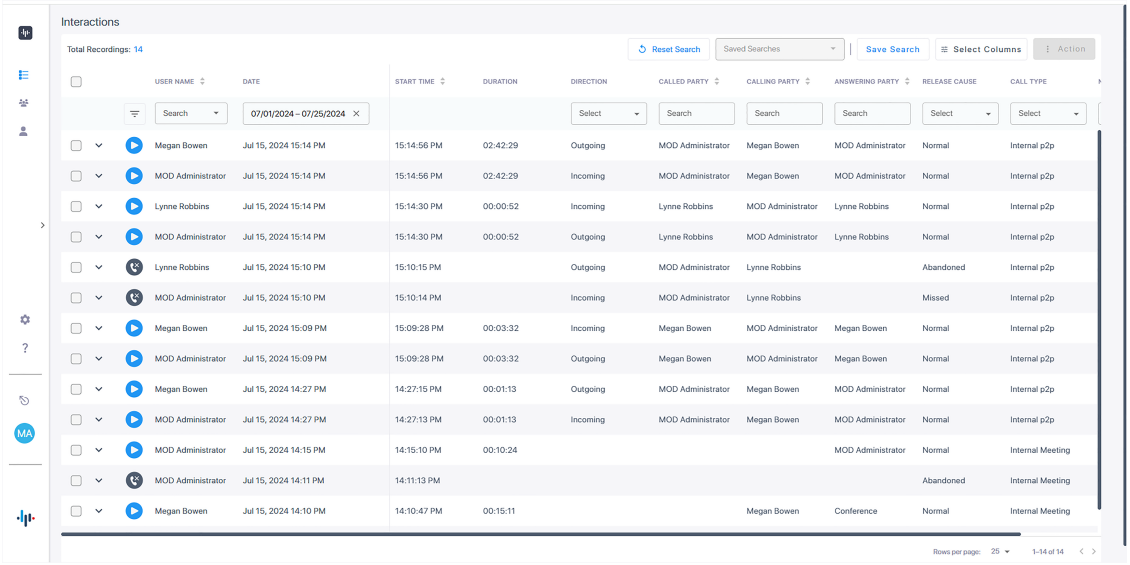
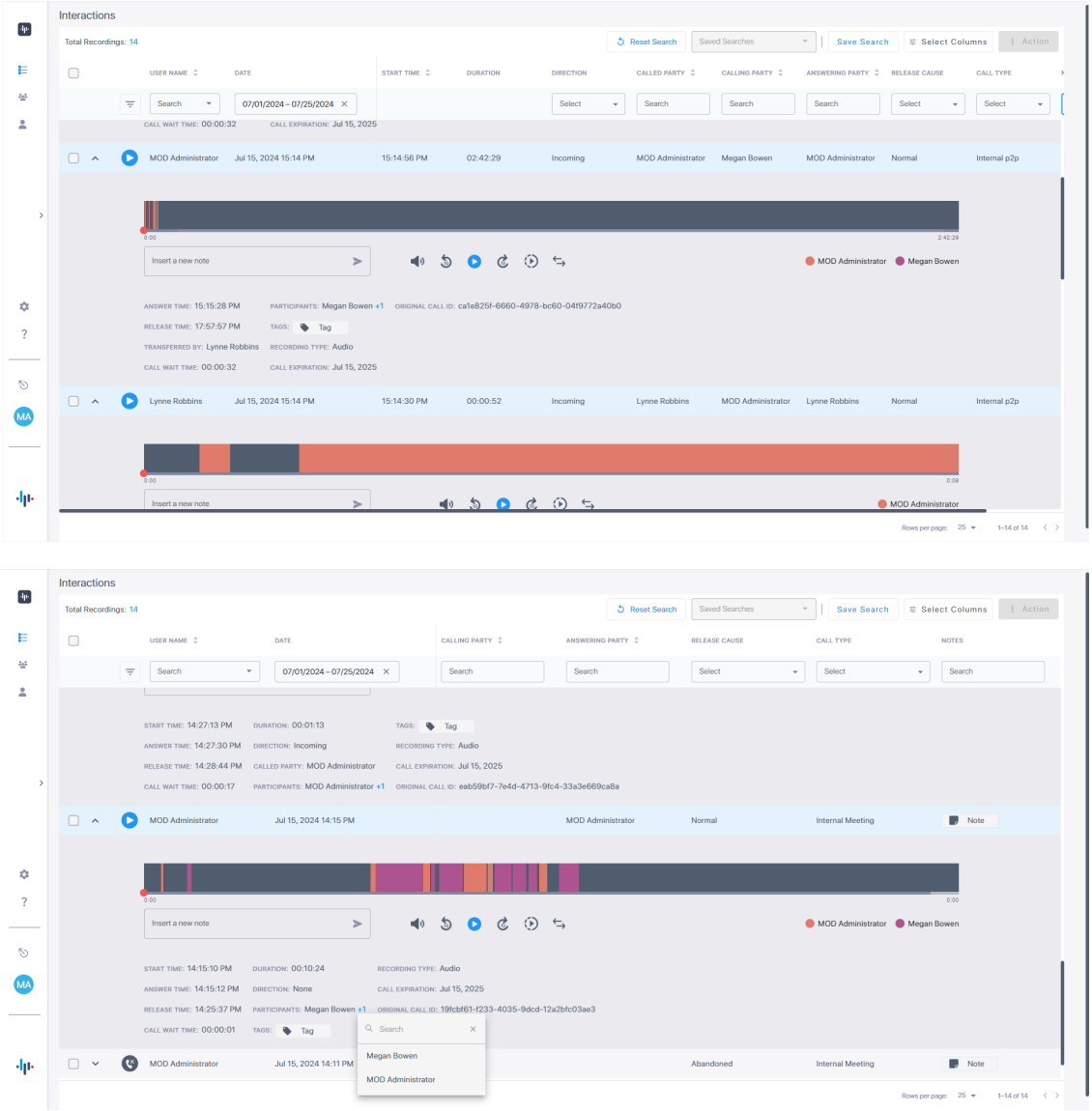


Figure 1-2: Media Player Time lines



Benefits

SmartTAP captures voice interactions that enables organizations to meet compliance regulations, and at the same time acquire business insights for measuring performance of customer interactions. Intelligence acquired through the product can be used as follows:

- Facilitates corporate strategy decision making process.
- Serves as the basis for enhancing customer satisfaction and loyalty.
- Minimizes exposure to disputes and mitigates the risk of reputation damage.
- Secures access for Live Platform operators and AudioCodes Live SmartTAP operators with Single Sign-on using Microsoft 365 Multifactor authentication.
- Compliance-grade recording and regulation-specialized features.

AudioCodes Live SmartTAP is a value-added service that is provided as part of AudioCodes Live Platform, whose core interface is used for remote monitoring of the service. Live Platform customer operators can manage the service alongside other service types in the same core interface, as well as connect to other Web interfaces used by the other service types.

Features Overview

The table below lists and describes the AudioCodes Live SmartTAP features.

Feature	Details
Quick Start	User-friendly Onboarding wizard that lets you do the following: ■ Click to consent for all connections to your M365 platform. ■ Automation script for creating Recording and Access profiles.
Compliance Recording Policy	Create recording policies for the users in the recording group on the customer's Azure tenant.
Role and permission-based access control	Role-based Single-Sign On access control based on Live Platform roles: Sysadmin, Service Provider, Channel and Customer operator.
Full time recording	Full-time audio recording
Recording Profiles	■ Define Recording Profiles for Peer-to-Peer calls, user calls with Meetings and user Queue calls ■ Define Retention period and Blob Storage account ■ Full Time Recording – Automatic audio recording. ■ Filter for PSTN, internal and external calls. Filter for Internal and External meetings. ■ Filter calls according to numbers and regular expressions. ■ Specify a time range for call recording, which includes the option to choose specific days of the week and time ranges based on the location of the server for the region.
Access Profiles	■ Configure call access for performing actions on media, such as Playing or Downloading media related to a call or viewing emails and notes related to a call. ■ Configure and Modify Recording and Access Profiles ■ Configure and modify System Configuration permissions
AudioRecording	■ Record calls of Targeted users on different devices, including

Feature	Details
	Teams desktop, web, mobile applications and phones. ■ Record the calls audio ■ Microsoft Azure Active Directory users mapping
Legal Hold of Agent recordings	Users cannot be deleted when placed on Legal Hold and their recording data is preserved.
Audit Trail	Audit trail of user activity and export of call records and audit trail reports.
Flexible and Powerful Call Search Capabilities	■ Search criteria based on username, date range, direction, called and calling party, release cause, call type and by defined notes. ■ Easily filter search results, sorting ascending or descending by clicking column header, shortcuts to the beginning page within the results screen. ■ Search for calls based on Calling (Caller ID), Called or Answering Party ■ Search for calls based on assigned Call Tag and whole words appearing in Notes. ■ Export Call metadata to Excel file.
Flexible retention policies	■ Number of retention periods can be added and applied to specific AAD User Groups. ■ Recordings are automatically deleted based on retention period.
Security	■ Media encryption with HTTPS/TLS/RTP.
Azure Blob Recordings Storage	Configure multiple storage accounts on Microsoft Azure Blob which is used for high-scale and secure object storage for cloud-native workloads, archives, data lakes, high-performance computing, and machine learning.
Call Tagging	User definable tags like Customer Name, Account Number, Malicious Call can be easily assigned to the call.
Personal App in Microsoft Teams	AudioCodes Live SmartTAP can be added to Microsoft Teams as a Teams App. Once setup can be uploaded to the customer organization’s App Store and run on Teams desktop or Teams mobile clients.

2 Adding Enterprise Service

- Prerequisites below
- Logging into SmartTAP Interface on page 8
- Quick Start on page 15
- Monitor Onboarding Process in Live Platform on page 34
- Deploy SmartTAP Teams App in Customer Teams client

Prerequisites

The following are the prerequisites for deploying the AudioCodes Live SmartTAP service:

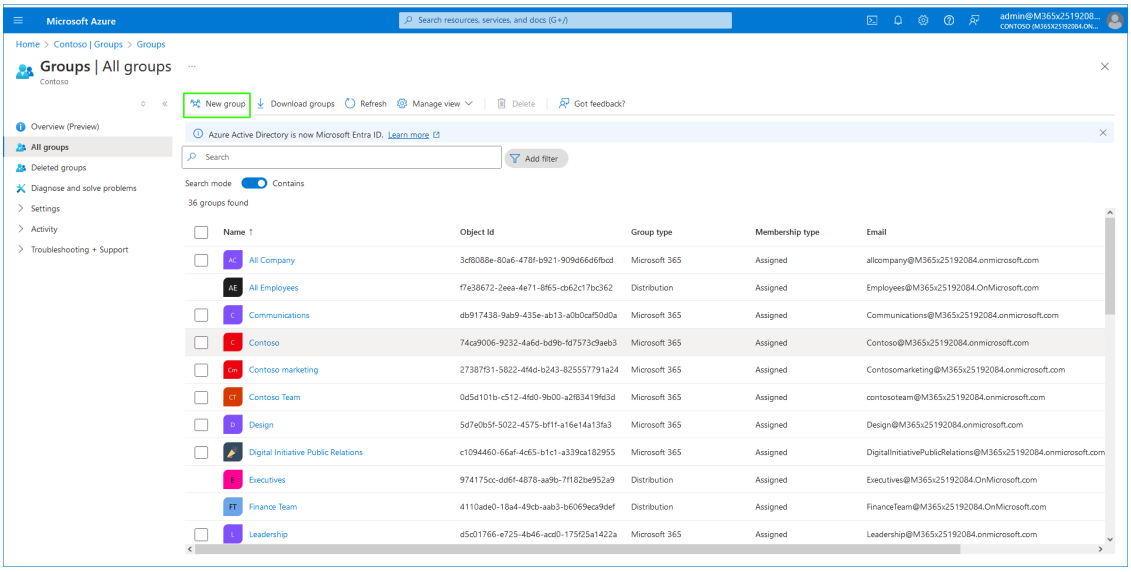
- Create AAD Recording Groups below

Create AAD Recording Groups

You need to create recording groups including targeted users for whom you wish to record. You then attach these groups to Recording Profiles in the Quick start wizard and in Day Two. Users may belong to multiple groups; however they can only be attached to a single Recording profile.

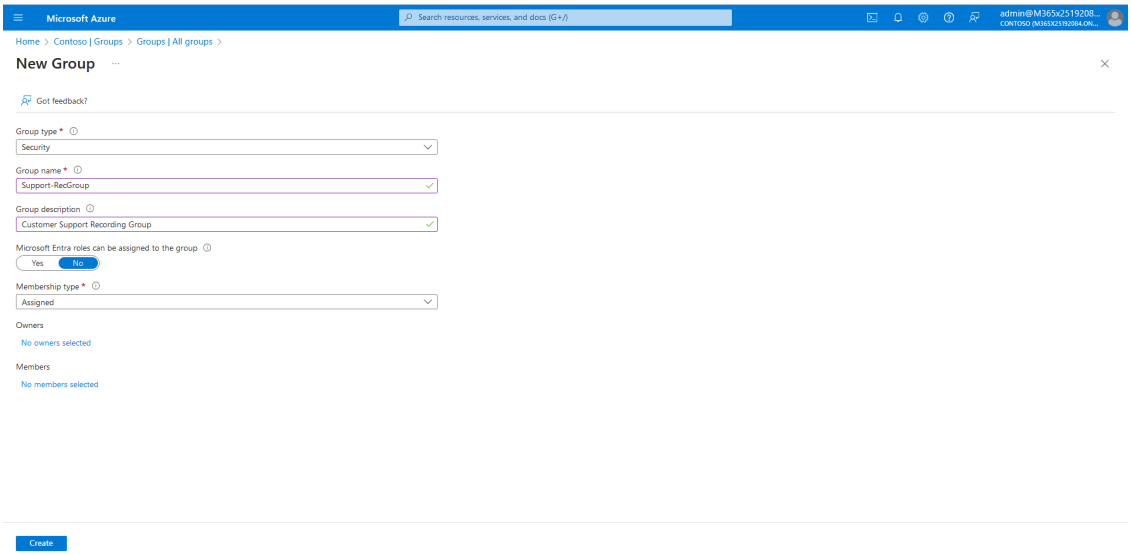
➢ **To create a recording group:**

1. In the customer Azure portal Navigation pane, select **Groups**.



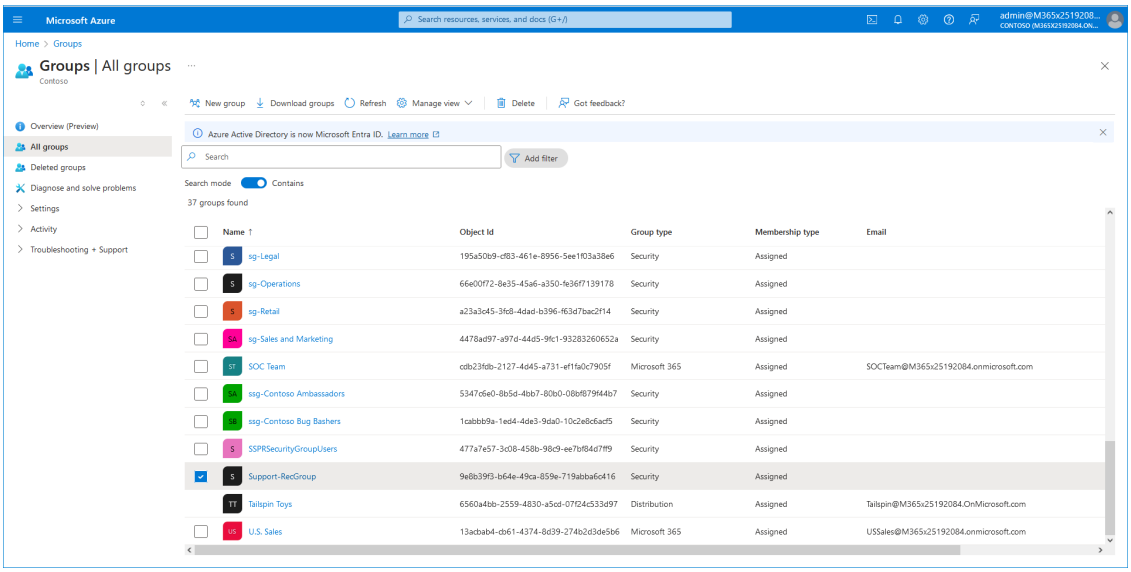
2. Click **New group**.
3. Enter the group details:
   - Group type: **Security** (default)
   - Group name: for example, Rec-Group

- Assign AD roles: **No** (default)
- Membership type: **Assigned** (default)

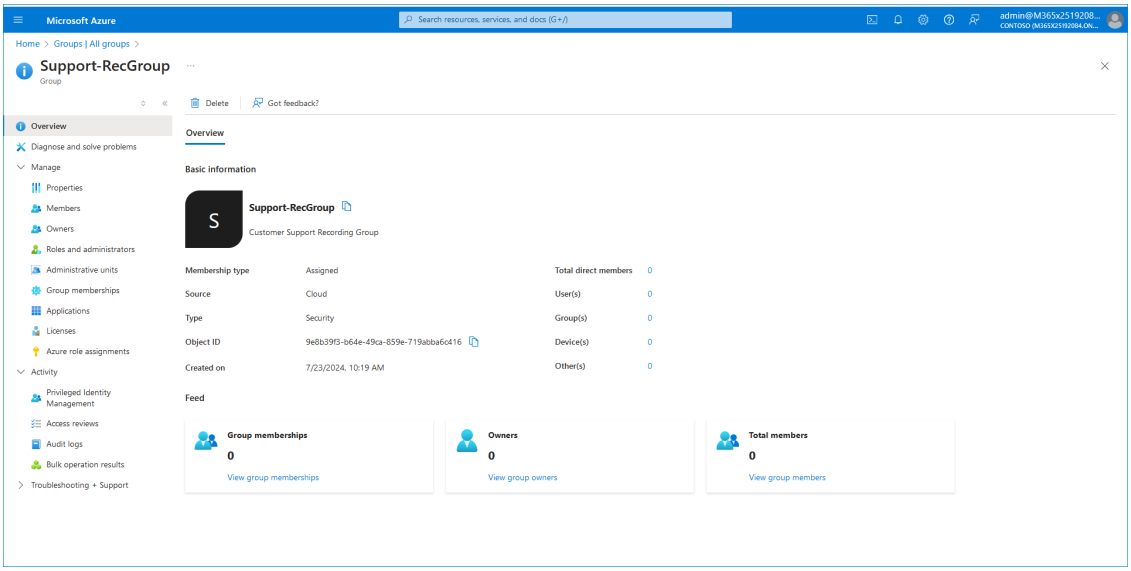


4. Click **Create**.

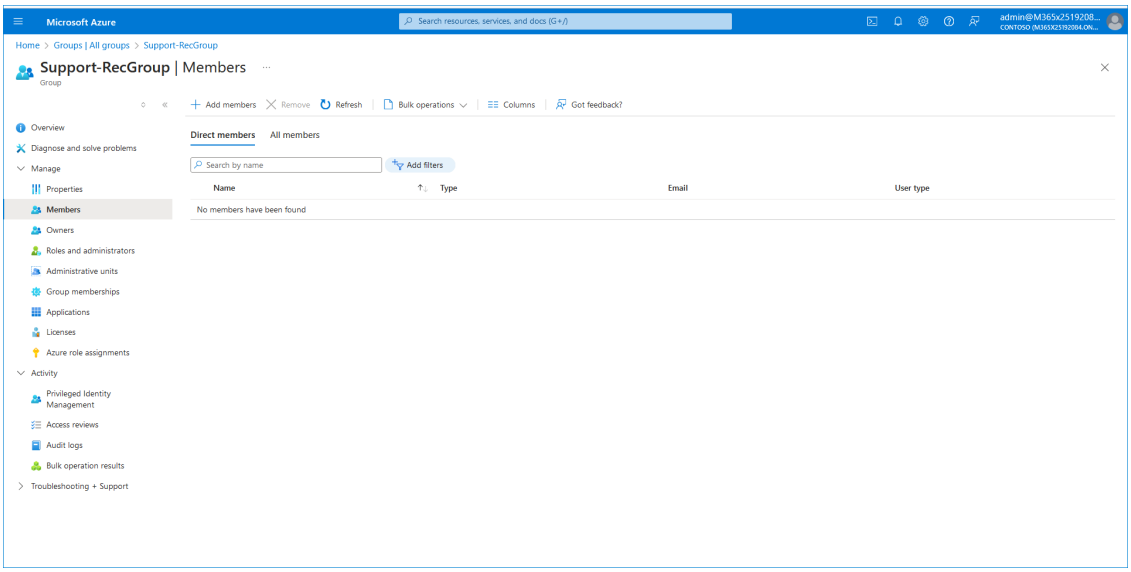
   The new group is created.



5. Select the new group and click to open it.

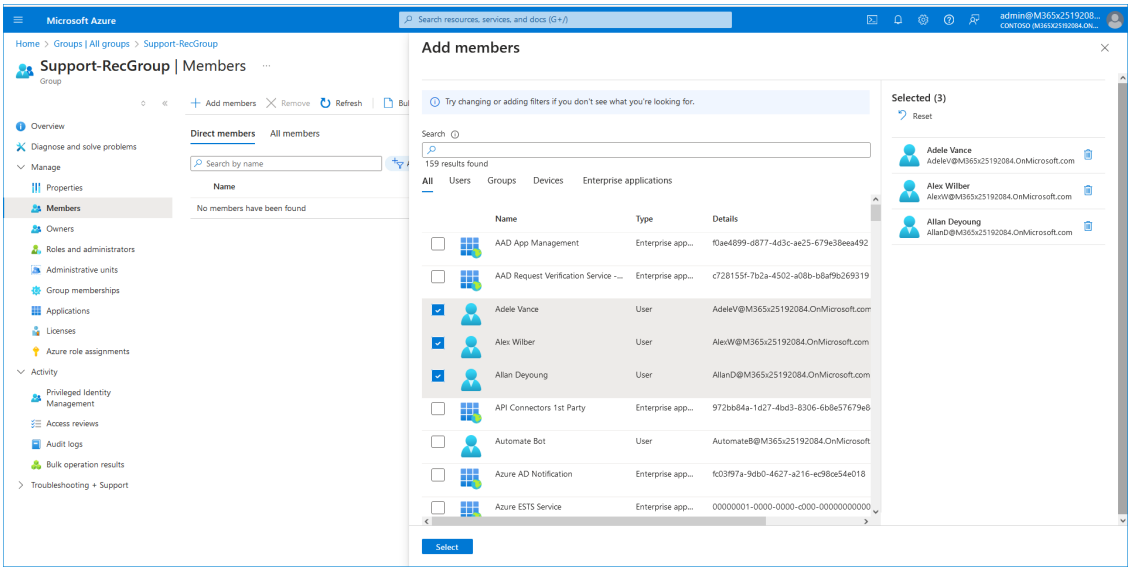


6. In the Navigation pane, select **Manage** > **Members** to add members to the group.

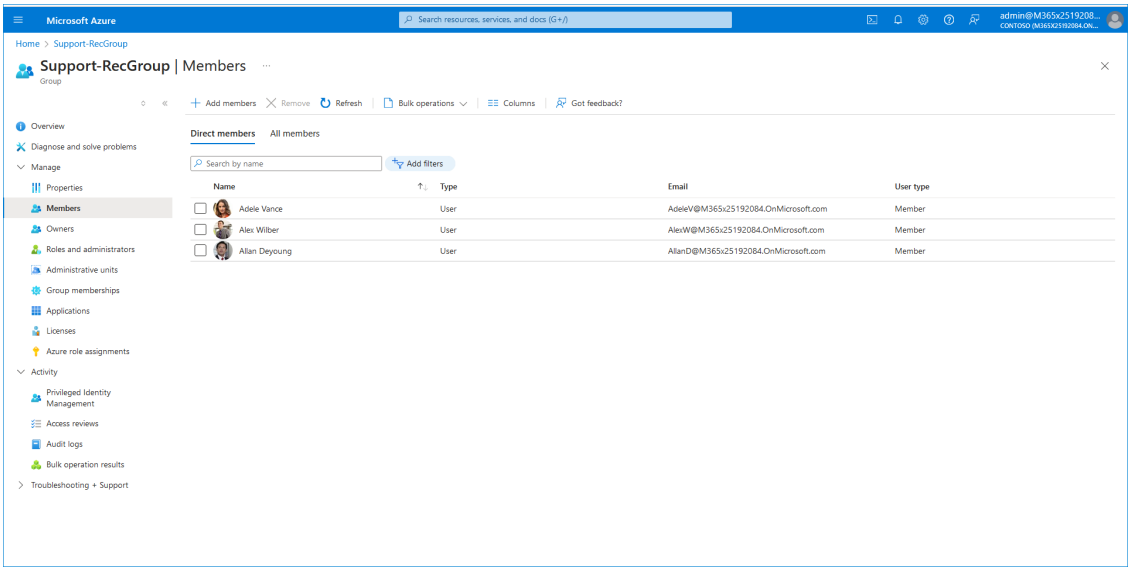


7. Click **Add Members**.

8. Search for the desired user to record, select them, and then click **Select**.



The members are added to the group.



Logging into SmartTAP Interface

Login to the SmartTAP interface for the first time using your M365 tenant operator with 'Global admin' credentials which are required for onboarding your Enterprise service. Once you have successfully deployed the service, you can add additional Enterprise M365 operators. Once the SmartTAP Service has been deployed by your Service Provider, Once you have purchased SmartTAP, you receive a Welcome email including a URL link to the SmartTAP Web interface.

➢ To log in for the first time:

1. Click the URL link sent in the Welcome email shown below.

```
Subject: Welcome! Your SmartTAP Application is Ready
```

Dear <End Customer Name> Team,

Congratulations! Your application deployment is complete and we're thrilled to inform you that you can now start utilizing SmartTAP . To get started, follow these steps.

M365 Administrator permissions are required for each step

1. Create 2 AAD Groups in Azure Active Directory

o Create two security groups in AAD.

1. One group for users that will be targeted to be recorded. Assign associated users to this newly created group. You can start by assigning one user to the group as a test user.

2. One group for users that will access the recording. Assign associated users to this newly created group. (This is an optional step as a default administrator will have access to all of the recordings).

2. Access & Configure Application - Follow 'Quick Start' Wizard

o Access the app at https://qaming.ai-logix.net/.

o Log in with one of the default administrator UPNs provided before the app was deployed: tania@customername.com.

Step 1: Click 'Connect M365' to Grant admin consent by clicking on each 'Grant Admin Consent' option to ensure proper access and operation of the app. Once completed click 'Finish' to return to Quick Start wizard.

Step 2: Click 'Configure Recording' to determine what calls to record, for how long to keep, and the group of the users to record.

1. Under 'Configuration' tab review and if needed change call types to record or retention period.

2. Under the 'Groups Mapping' tab add the AAD security group you created to be recorded.

3. Under the 'MSFT Policy' tab make sure to download MSFT Compliance Policy script and execute the script. Click 'Finish' to finalize the recording profile and return to Quick Start wizard.

Step 3: Click 'Configure Access' to set access permissions for call recordings and the system commonly known as Roles Based Access Control (RBAC). (Optional step, default administrator has full access).

1. Under 'Permissions' set permissions for call recording access and system configuration.

2. Under the 'Groups Mapping' tab add the AAD security group you created to access the recordings.

3. Click 'Finish' to finalize the Access profile. You will receive confirmation that you are ready to start recording.

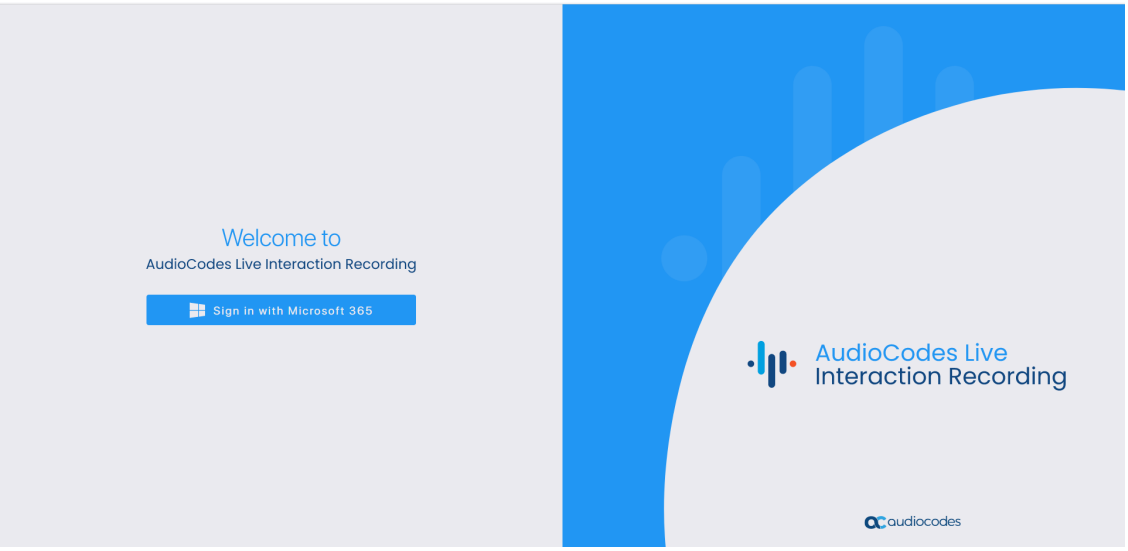
That's it! Your application is now set up for use and recording! See the admin guide here.

Test a Call with a Targeted User:

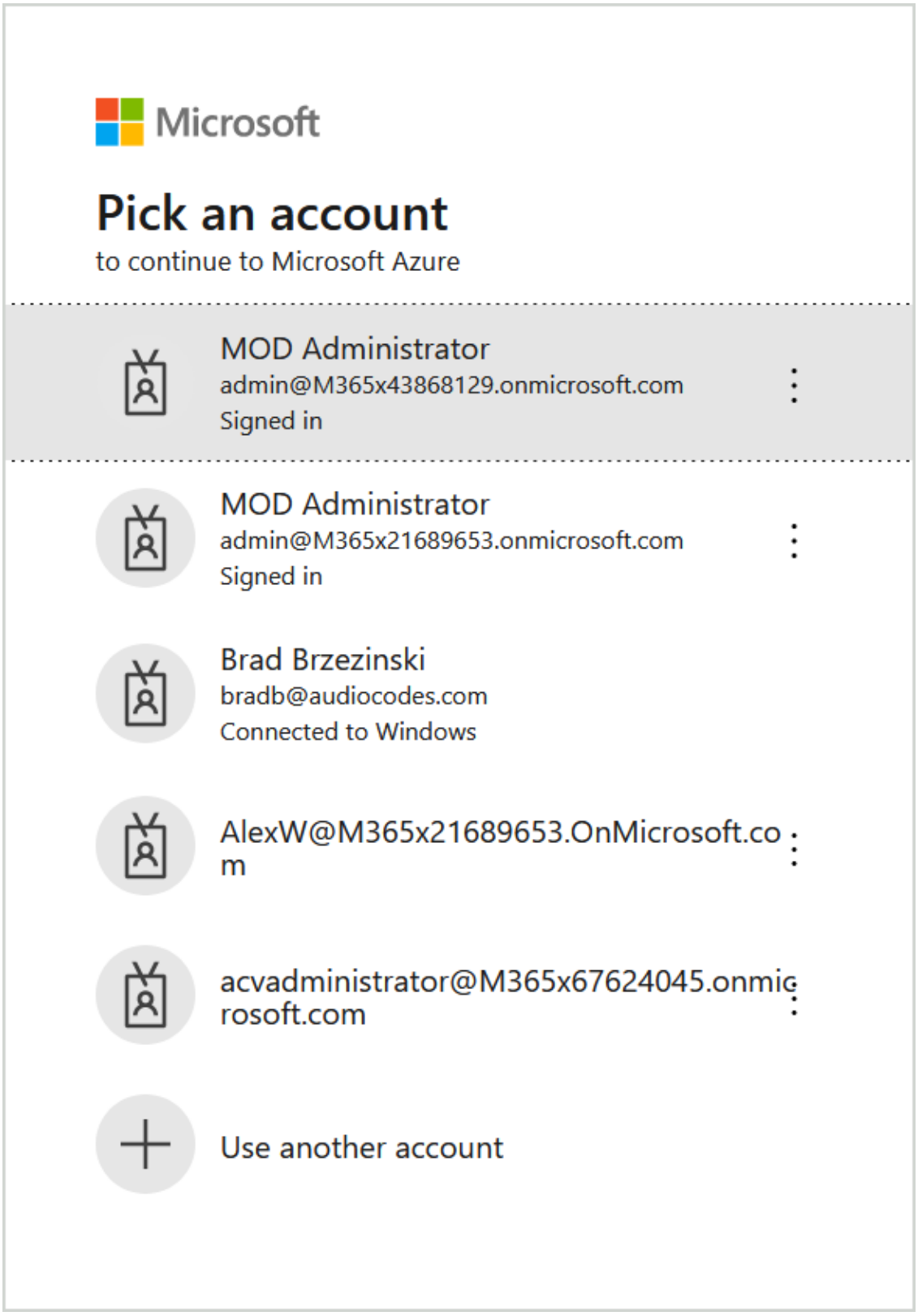
- Try out a test call with a targeted user to be recorded.
- Check you have recording notifications with the recording banner presented in Microsoft Team during the call. End the call so the recording can be played back.

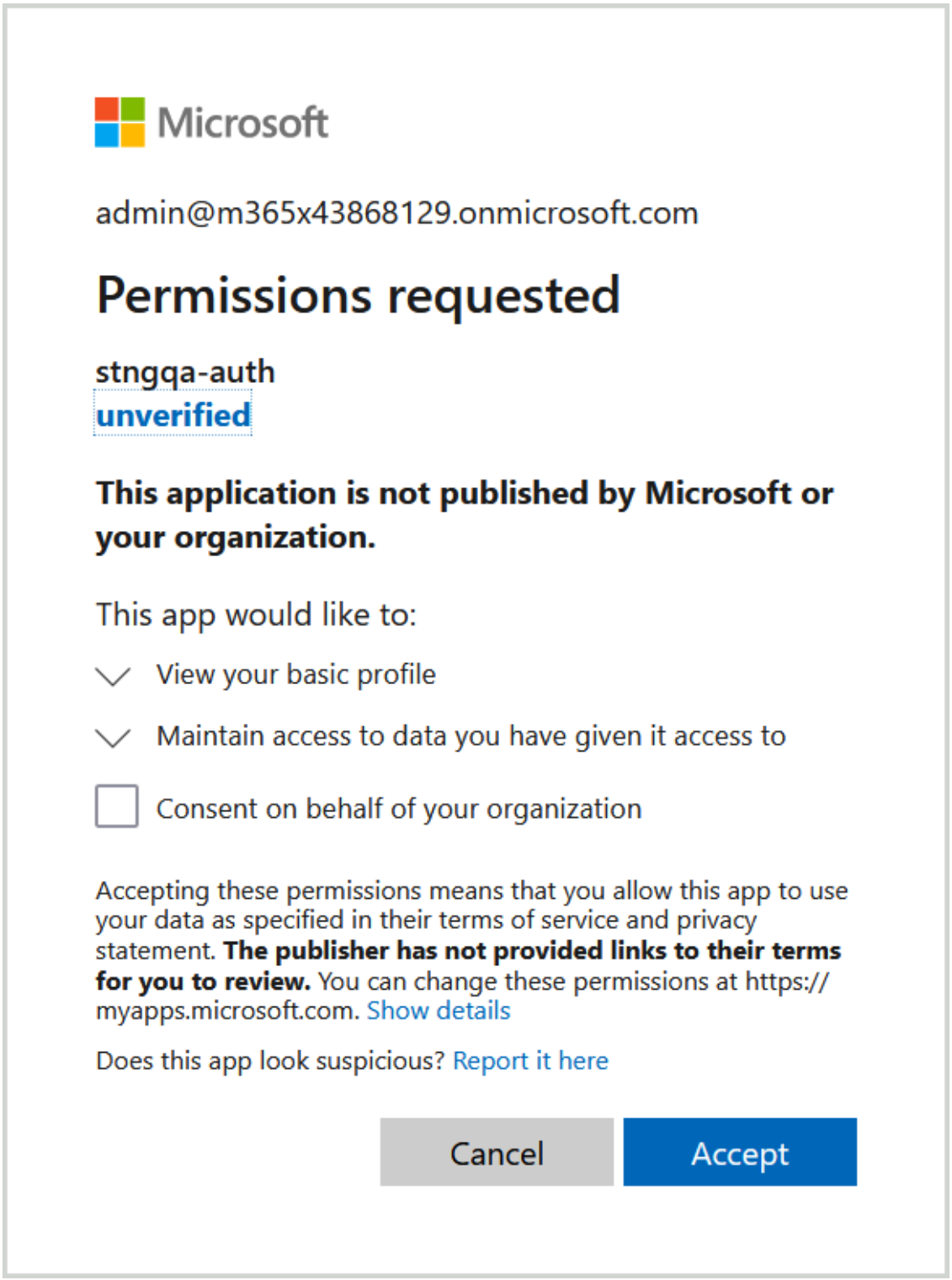
```
•    Navigate and click on the 'Interactions' page in top left corner
navigation panel in your application to see that the call is successfully
recorded and can be played back.

We're excited for you to explore the possibilities of SmartTAP! If you have
any questions or need assistance, feel free to reach out.

Best Regards,

AudioCodes Team
```

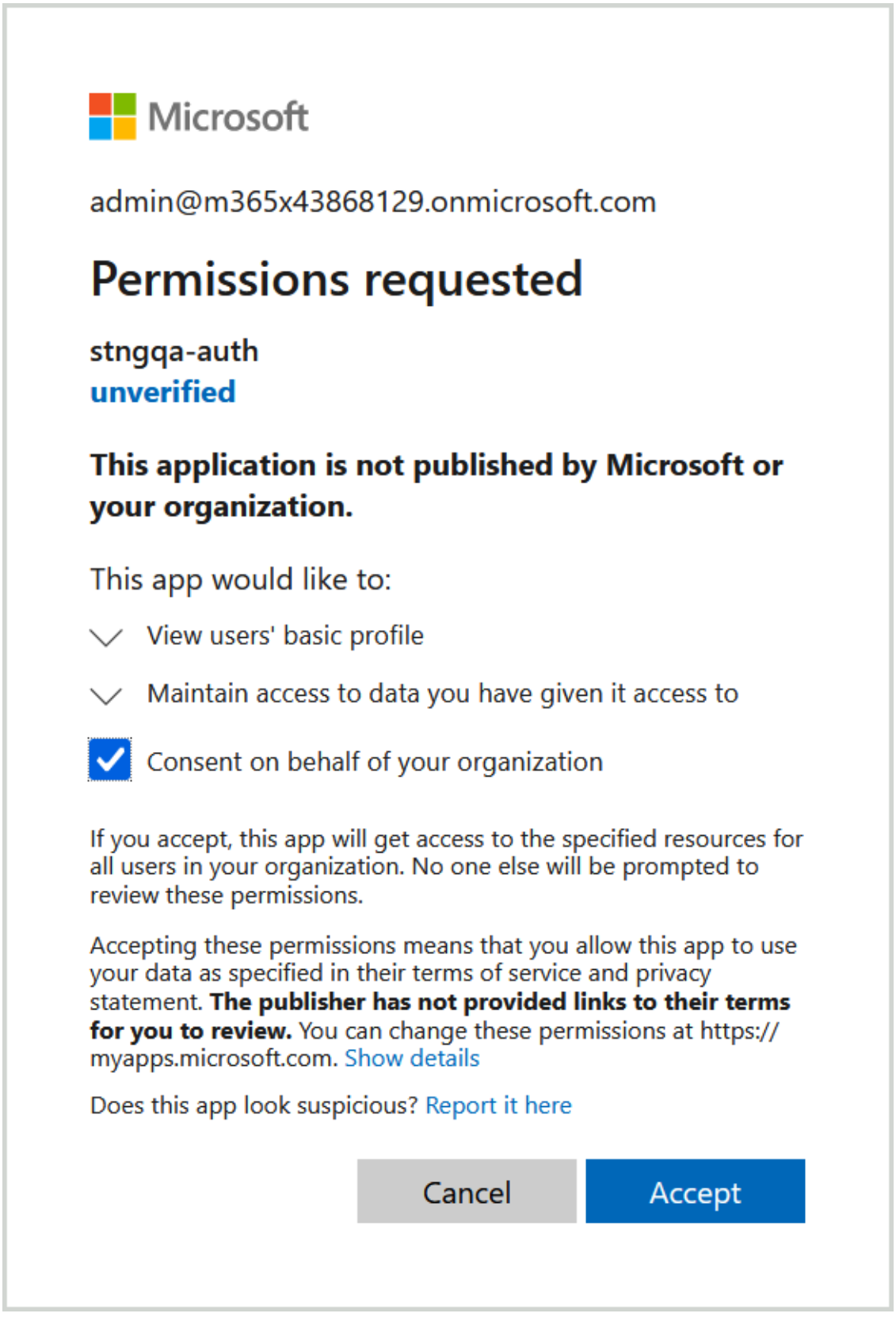
The Welcome page for the InteractionRecording interface is displayed.



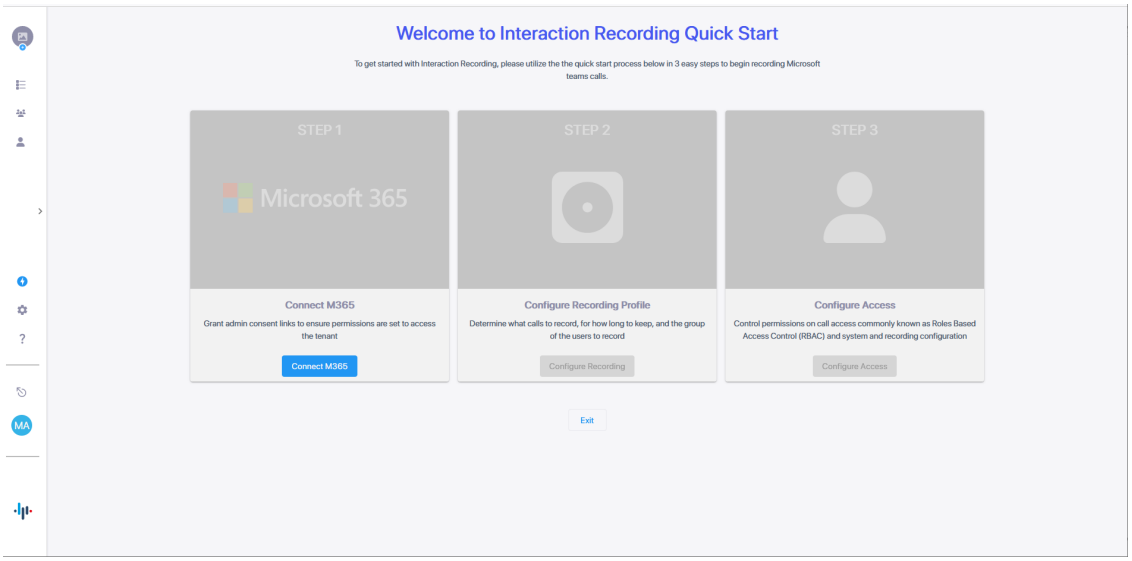
2. Click **Sign in with Microsoft 365**.
3. Choose the Global admin account of your Live Platform tenant.


Microsoft
Pick an account
to continue to Microsoft Azure
MOD Administrator
admin@M365x43868129.onmicrosoft.com
Signed in
MOD Administrator
admin@M365x21689653.onmicrosoft.com
Signed in
Brad Brzezinski
bradb@audiocodes.com
Connected to Windows
AlexW@M365x21689653.OnMicrosoft.com
acvadministrator@M365x67624045.onmicrosoft.com
Use another account


Microsoft
admin@m365x43868129.onmicrosoft.com
Permissions requested
stngqa-auth
unverified
This application is not published by Microsoft or your organization.
This app would like to:
View your basic profile
Maintain access to data you have given it access to
Consent on behalf of your organization
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. The publisher has not provided links to their terms for you to review. You can change these permissions at https://myapps.microsoft.com. Show details
Does this app look suspicious? Report it here
Cancel
Accept



4. Select the **Consent on behalf of your organization** check box, and then click **Accept**. The Quick Start wizard opens.



5. Proceed to Quick Start below.

Quick Start

Once the SmartTAP Service has been deployed by your Service Provider, Once you have purchased SmartTAP, you receive a Welcome email similar to the following including a URL link to the Quick Start wizard. The Quick Start provides a three-step wizard for setting up your SmartTAP service:

- **Step 1:** Establishes consents to secure connection with the customer's M365 platform for all managed Azure and SmartTAP services.
- **Step 2:** Sets up their Recording profiles including which calls may be recorded, retention and storage period, whether to enable call notifications and call filtering. Profiles are then assigned to one or more of the customers' AAD tenant groups, and in the last stage configure additional Microsoft Teams Call policies. Once you have completed the configuration, you must download and run the Recording Profile PowerShell script.
- **Step 3:** Setup Role-based Access Control (RBAC) for determining who can access call recordings, create and modify profiles and configure global settings.

- The Quick Start wizard must be performed by the customer M365 Administrator.
- You can also click in the Icon pane to open this wizard (this icon disappears once you have completed the Onboarding). Click Connect to M365 on page 146 to manage the consents.

➢ **Do the following:**

1. Click **Connect M365** to start the wizard.

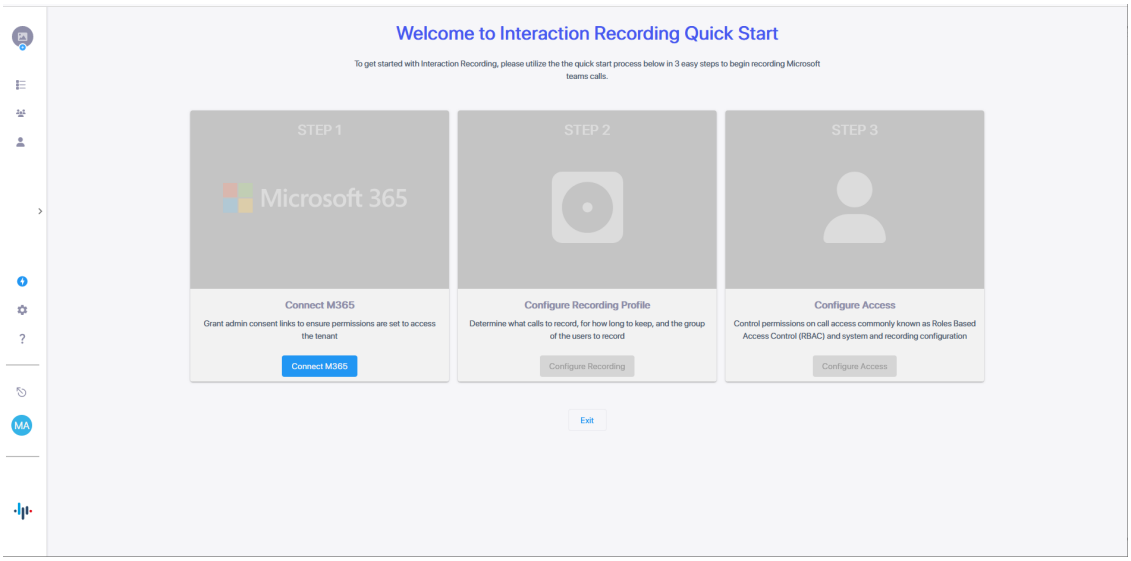
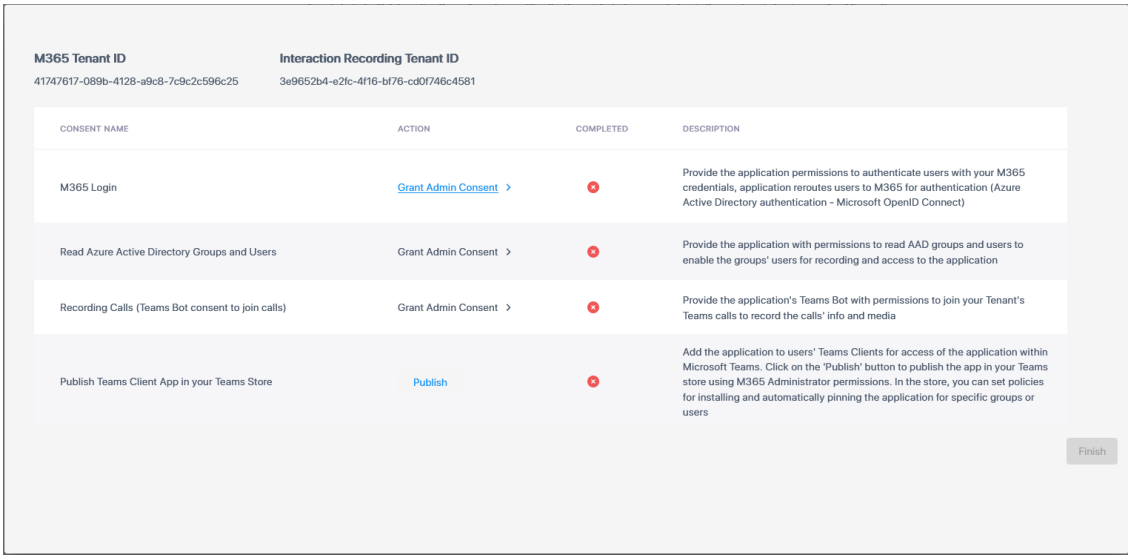


Figure 2-1: Essential Recording Tenant



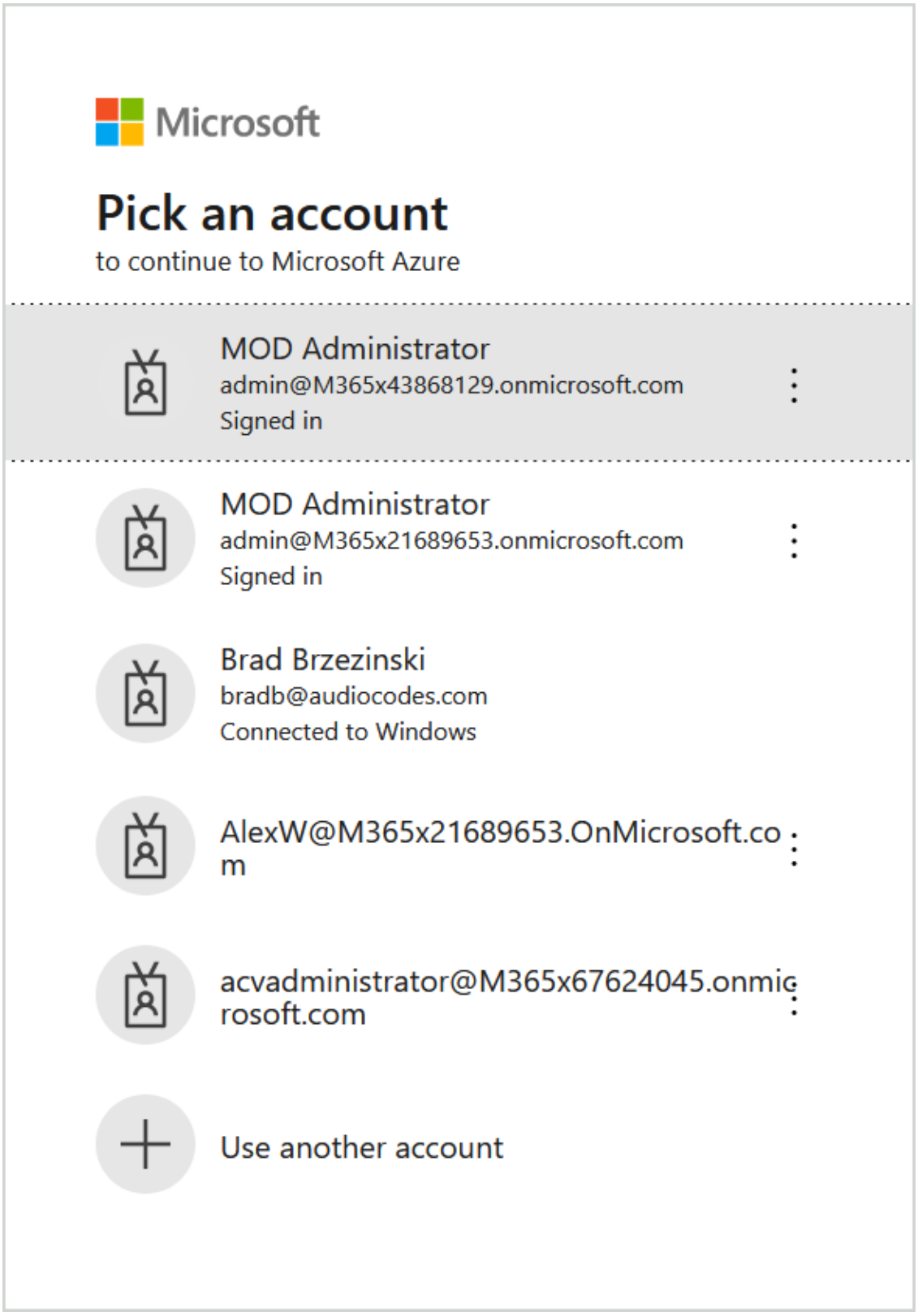
The table below describes the required consents and the Enterprise applications that are created on your M365 tenant.

Consent	Description
M365 Login	Provide the application permissions to authenticate users with your M365 tenant credentials. The application reroutes users to M365 for authentication (Azure Active Directory authentication-Microsoft OpenID Connect-Oauth 2). The permissions are required for the SmarTAP application to authenticate users utilizing your tenant AAD authentication, and Microsoft Open ID Connect (Oauth 2) authentication. The permissions enable AudioCodes Live SmartTAP to reroute users accessing the AudioCodes Live SmartTAP application either from a browser or from the AudioCodes Live SmartTAP Teams application (see row below) to be authenticated according to your

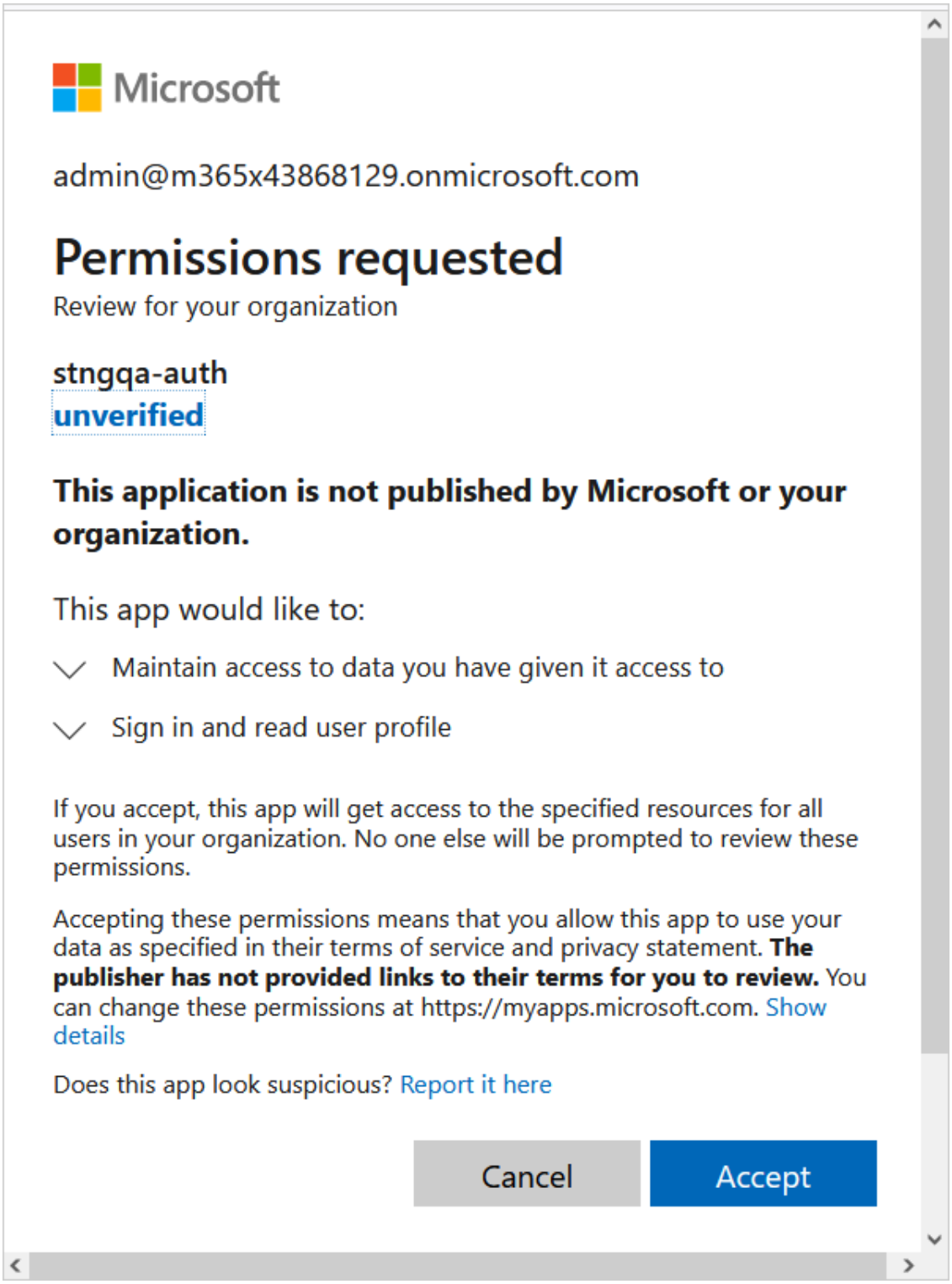
Consent	Description
	organizational M365 policy. The Deployment generates the Enterprise application <LivePlatformSer verName>-auth. Youconsent to the following permissions: ■ email – View users; email address (Delegated) ■ offline_access – Maintain access to data you have given it access to (Delegated) ■ openid – Sign users in (Delegated) ■ profile – View users' basic profile (Delegated) ■ User.Read – Sign in and read user profile (Delegated) ■ If you published the Teams app, the following permissions are added: ✓ AppCatalog.Submit – Submit application packages to the catalog and cancel pending submissions. ✓ AppCatalog.ReadWrite.All – Read and write to all app catalogs
Publish Teams Client App in your Teams Store (Optional)	Add the application to users Teams Clients for access of the application within Microsoft Teams. Click the publish button to access the app within your Teams store using M365 Administrator permissions. In the store, you can set policies for installing and automatically pinning the application for specific groups are users. ⚠ Publishing the app makes it available for users in the tenant organization within Teams store. Each user needs to add the application from their Teams admin center in order to access it from Teams.
Read Azure Active Directory Users and Groups	Provide the application permissions to read AAD groups and users from your M365 tenant to enable the groups' targeted users for recording and access to the application. Deployment of AudioCodes Live SmartTAP generates the Enterprise application <LivePlatformServerName>-aad. Youconsent to the following permissions: ■ User.Read.All – Read all users' full profiles (Application) ■ GroupMember.Read.All – Read all group memberships (Application)
Recording Calls (Teams Bot consent to join calls)	Provide the applications' Teams Bot with permissions to join your Tenant's Teams calls to record the calls' info and media. The calls-app permissions are required for the AudioCodes Live SmartTAP Bot application to join your Teams' tenant calls and to receive the media to be recorded. Deployment of AudioCodes Live SmartTAP generates the Enterprise

Consent	Description
	application <LivePlatformServerName>-hue. Youconsent to the following permissions: ■ Calls.JoinGroupCall.All - Join group calls and meetings as an app (Application) ■ Calls.AccessMedia.All - Access media streams in a call as an app (Application)
Redundant Recording Calls (Second Teams Bot consent to join calls)	Provide the application's Redundant Teams Bot with permissions to join your tenant's Teams calls to record the calls' info and media. The calls-app permissions are required for the AudioCodes Live SmartTAP Bot application to join your Teams' tenant calls and to receive the media to be recorded. Deployment of AudioCodes Live SmartTAP generates the Enterprise application <LivePlatformServerName>-hue-paired. Youconsent to the following permissions: ■ Calls.JoinGroupCall.All - Join group calls and meetings as an app (Application) ■ Calls.AccessMedia.All - Access media streams in a call as an app (Application) ⚠ This consent is required in the event where a Pro User license has been configured for the service.

1. Click the **Grant Admin Consent** link for the M365 login.
2. Choose the Global admin account of your Live Platform tenant.



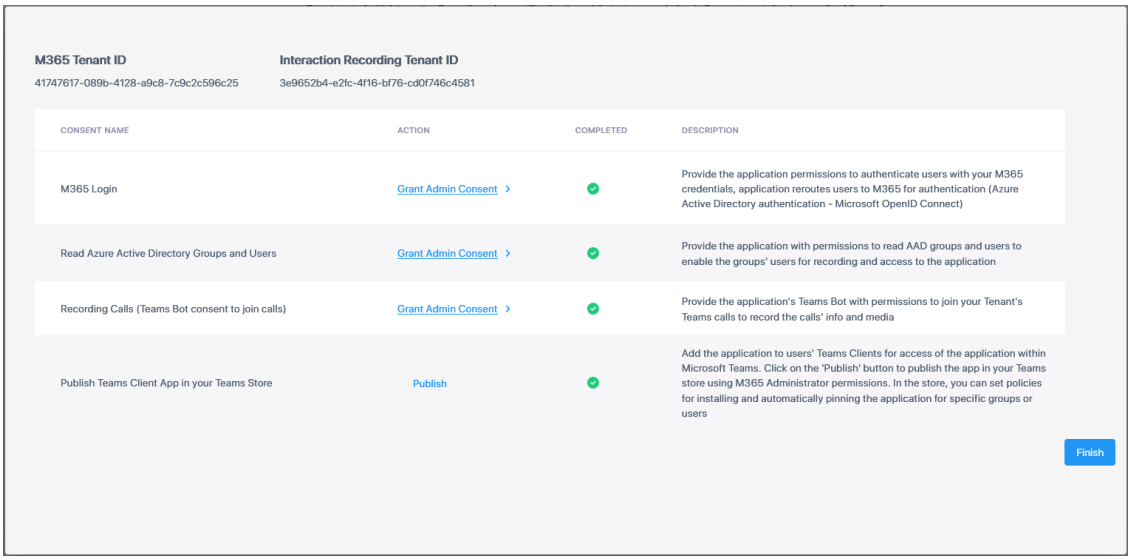
3. Click **Accept**.



4. Repeat the process for each permission.

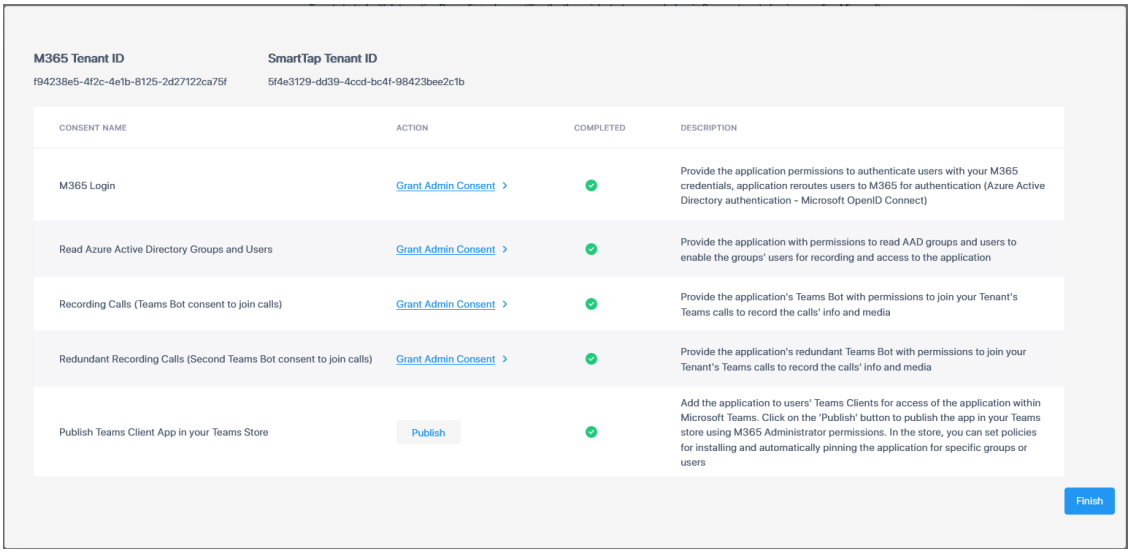
The final action to publish the Teams Client App in your Teams Store is optional.

Figure 2-2: Tenant with Essentials license

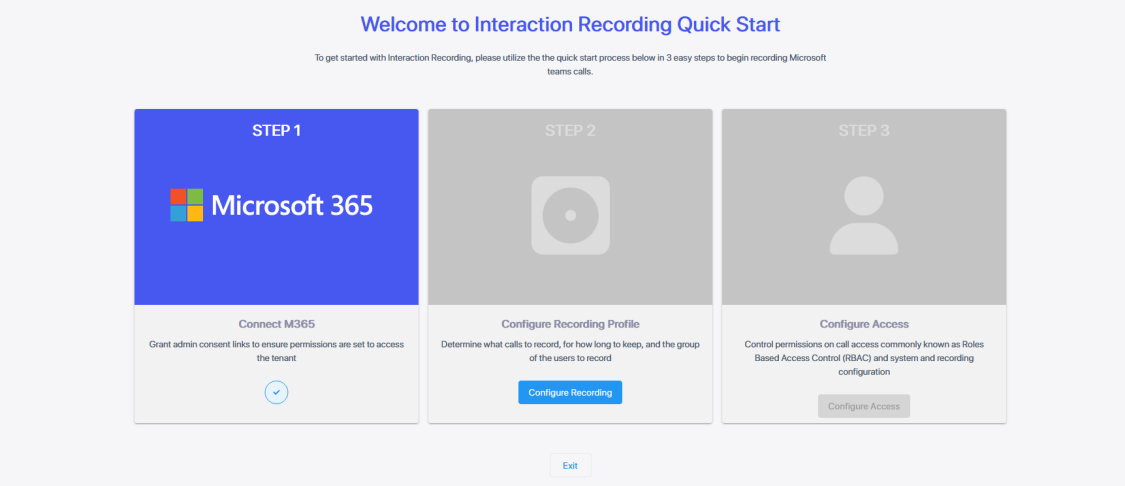


For Pro Users with capabilities for Double Recording with Paired Bot users, an additional consent is required for the Second Teams Bot.

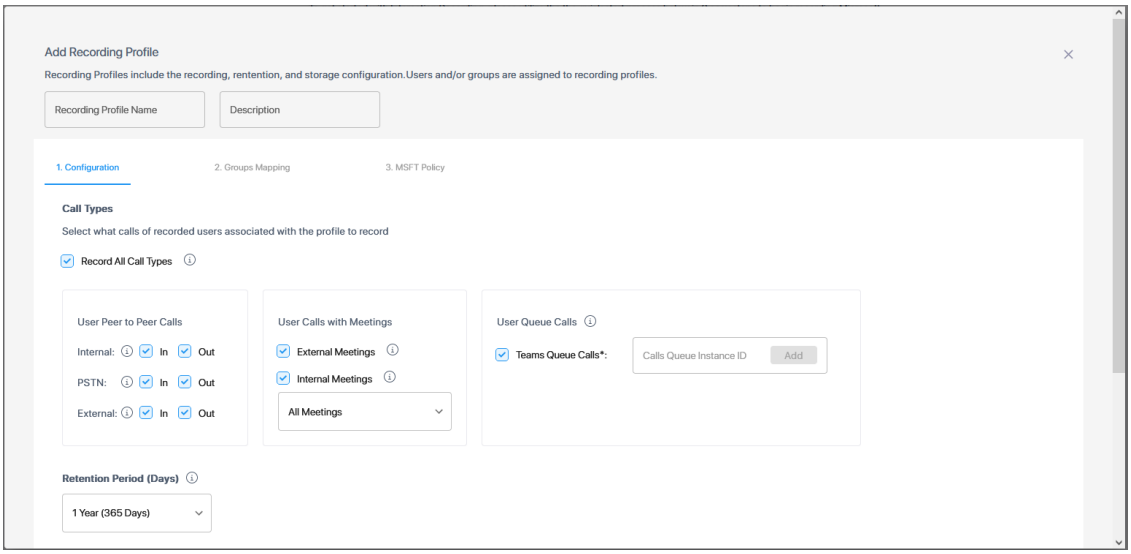
Figure 2-3: Tenant with Pro License

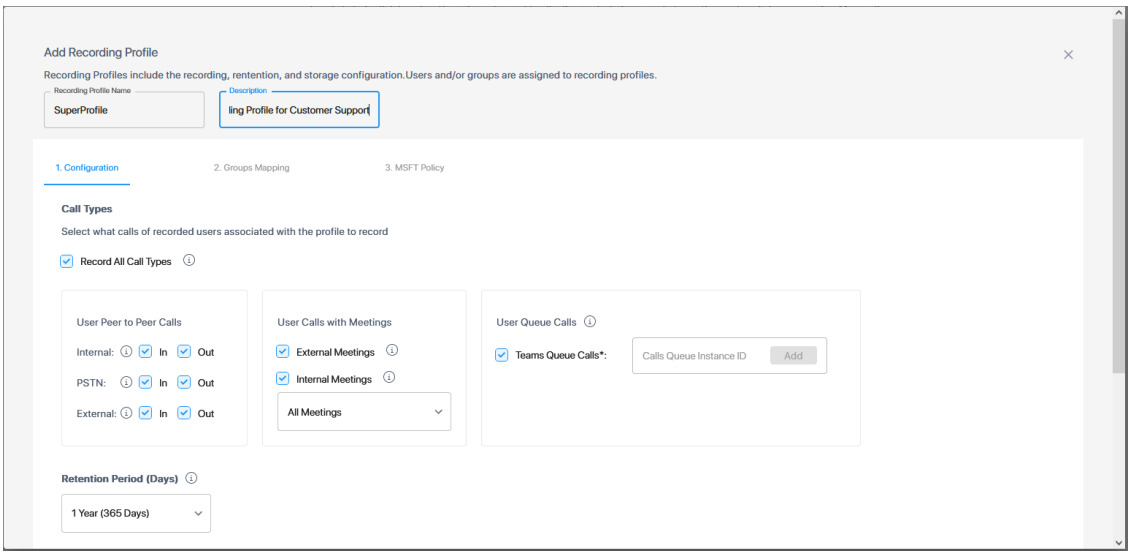


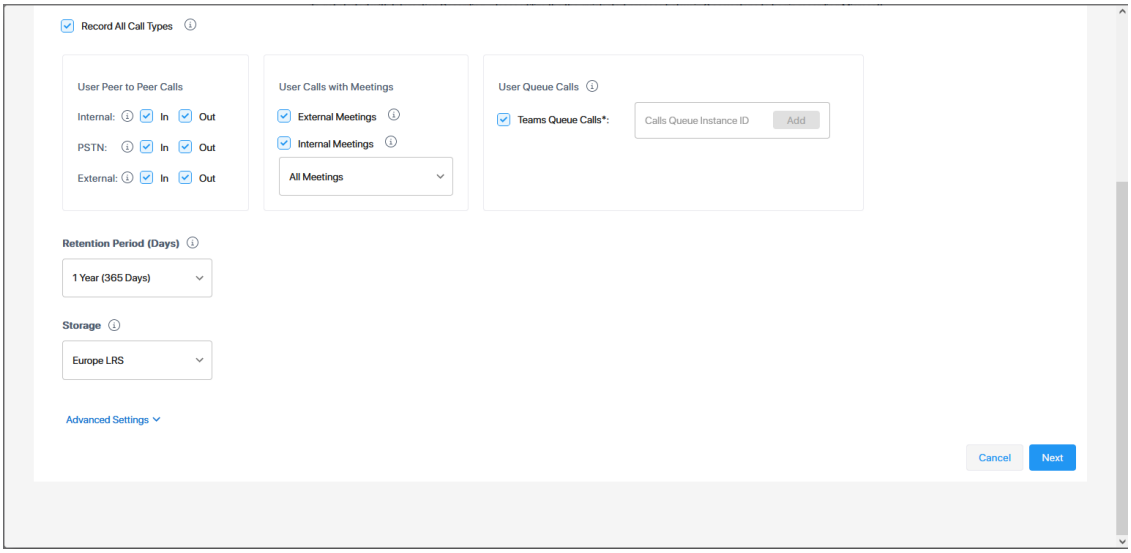
5. Click **Configure Recording Profile**.

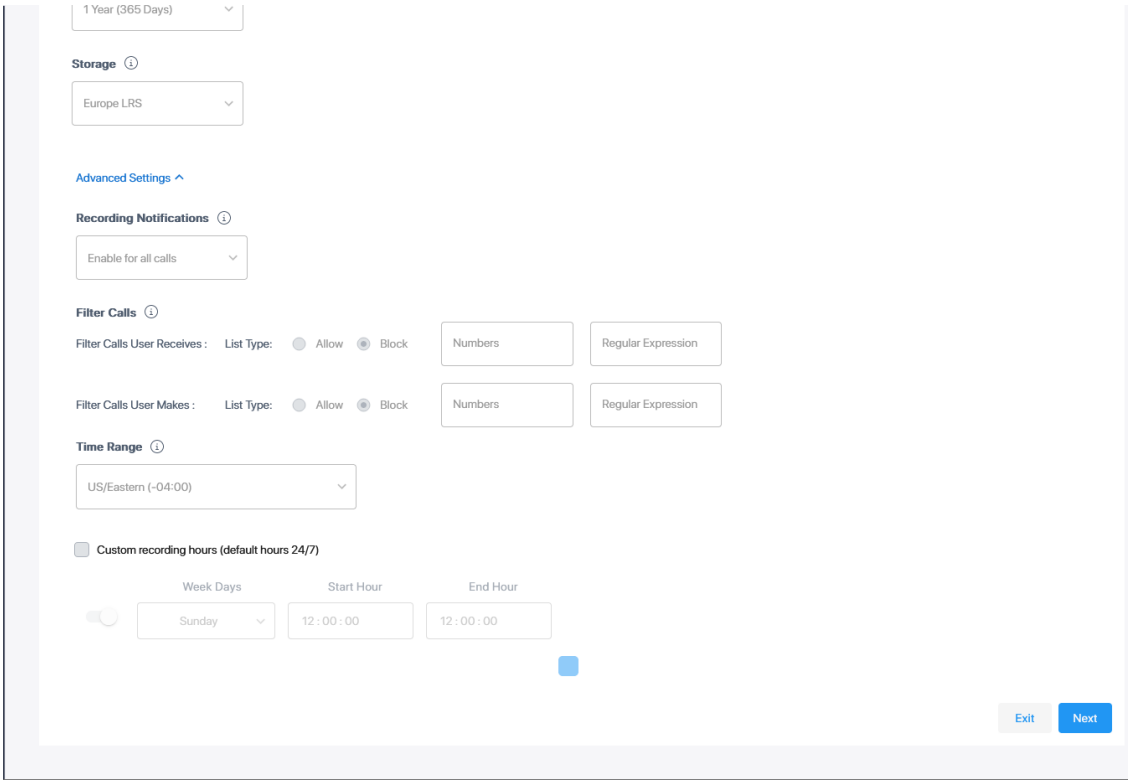


6. Configure Recording Profile (see Adding Recording Profiles on page 48).



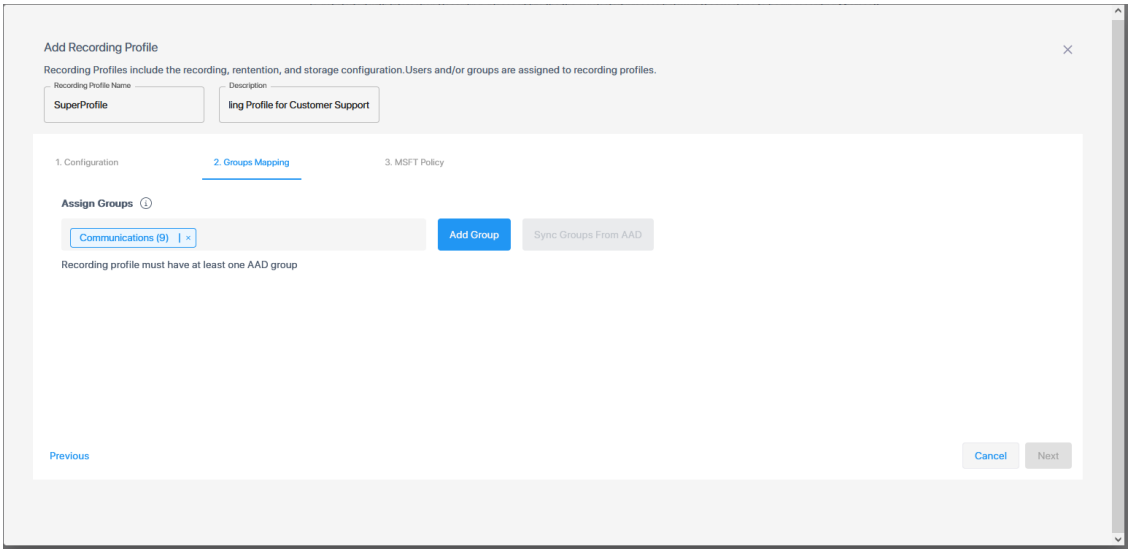


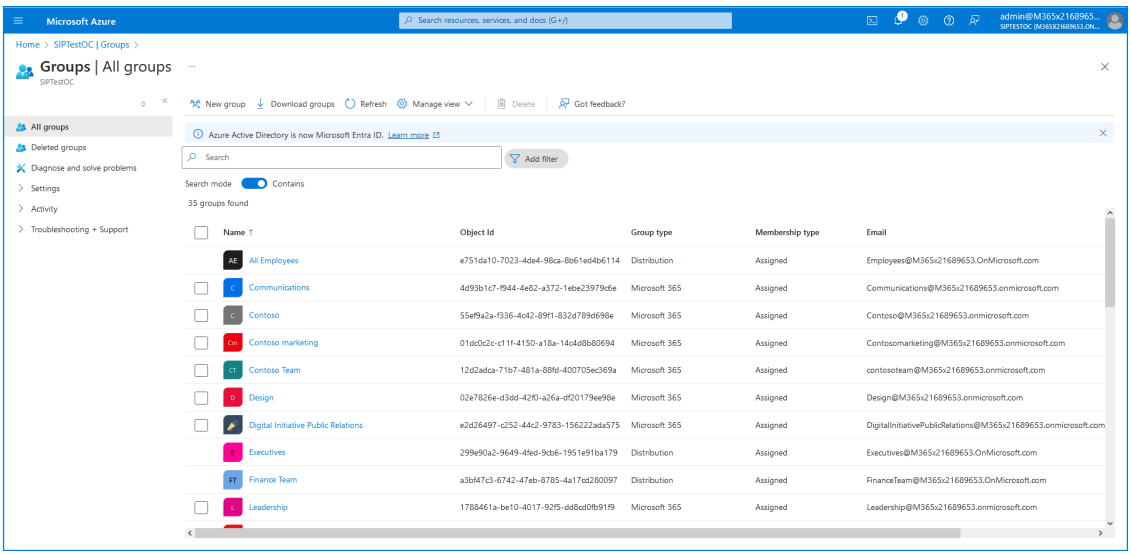




> The Recording Notifications field is only displayed when enabled by the Service Provider when adding the service. In addition, the customer must sign a consent waiver.

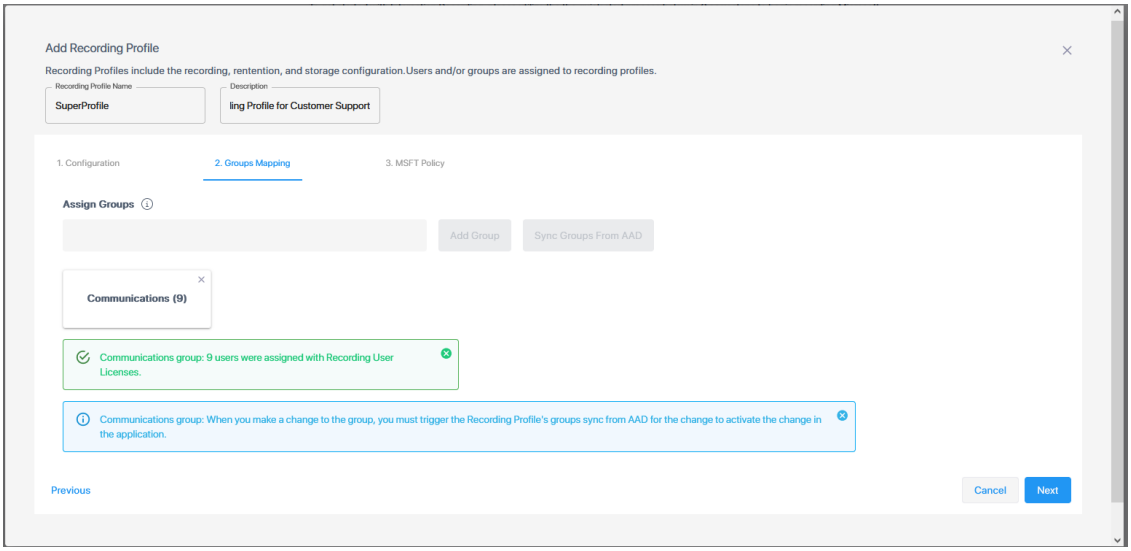
7. Click **Next** to continue.



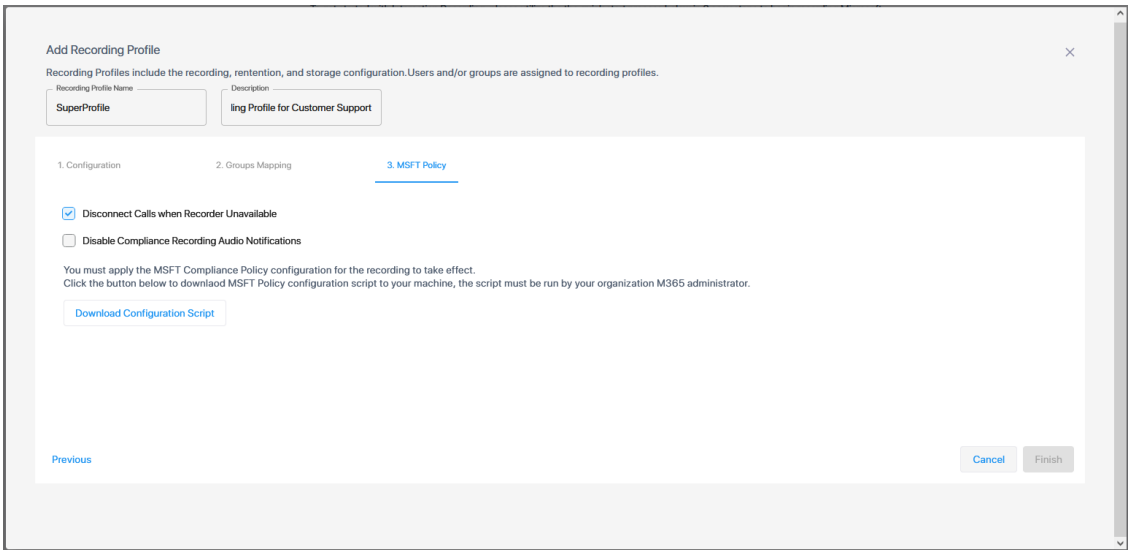


8. Assign Azure group to the profile; log in to the Azure portal for your tenant to confirm which group you wish to associate with the profile. Once assigned, the confirmation message below is displayed.

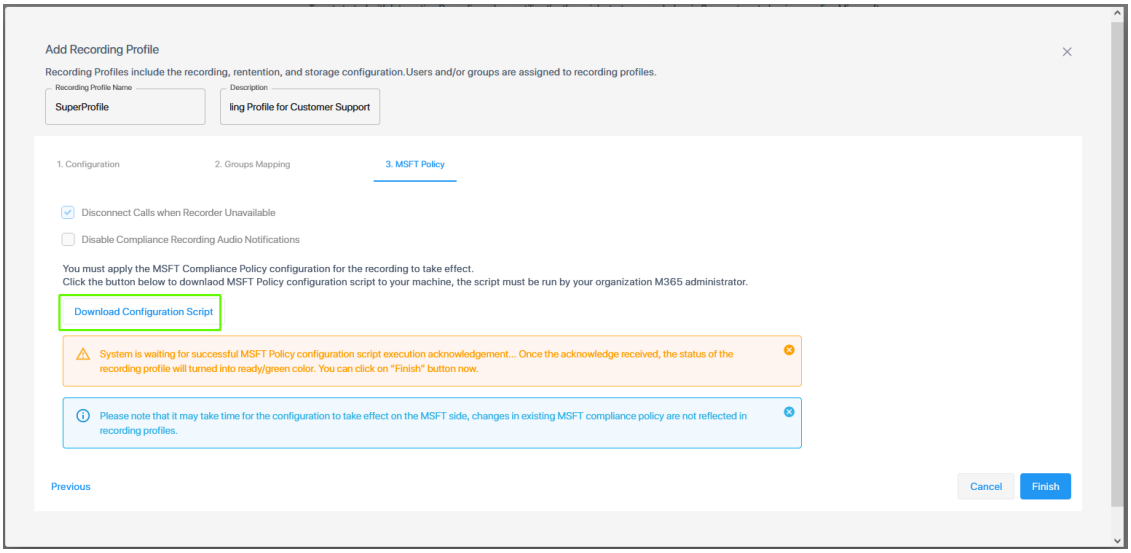
If you later add or remove group members, you must perform synchronization operation (see Synchronizing Recording Profiles on page 71).



9. Click **Next** to continue.



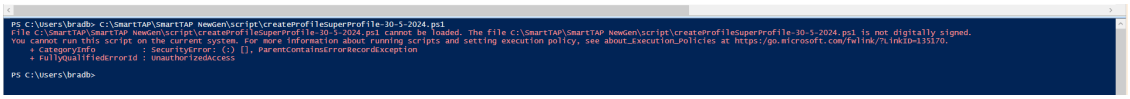
10. Configure the following MSFT Policies:
    - **Disconnect Calls when Recorder Unavailable:** Calls are disconnected when recording functionality is not available.
    - **Disable Compliance Recording Audio Notifications:** Disable Microsoft Teams Recording banner notifications.
11. Click the **Download Configuration Script** link to download the Recording Profile script.



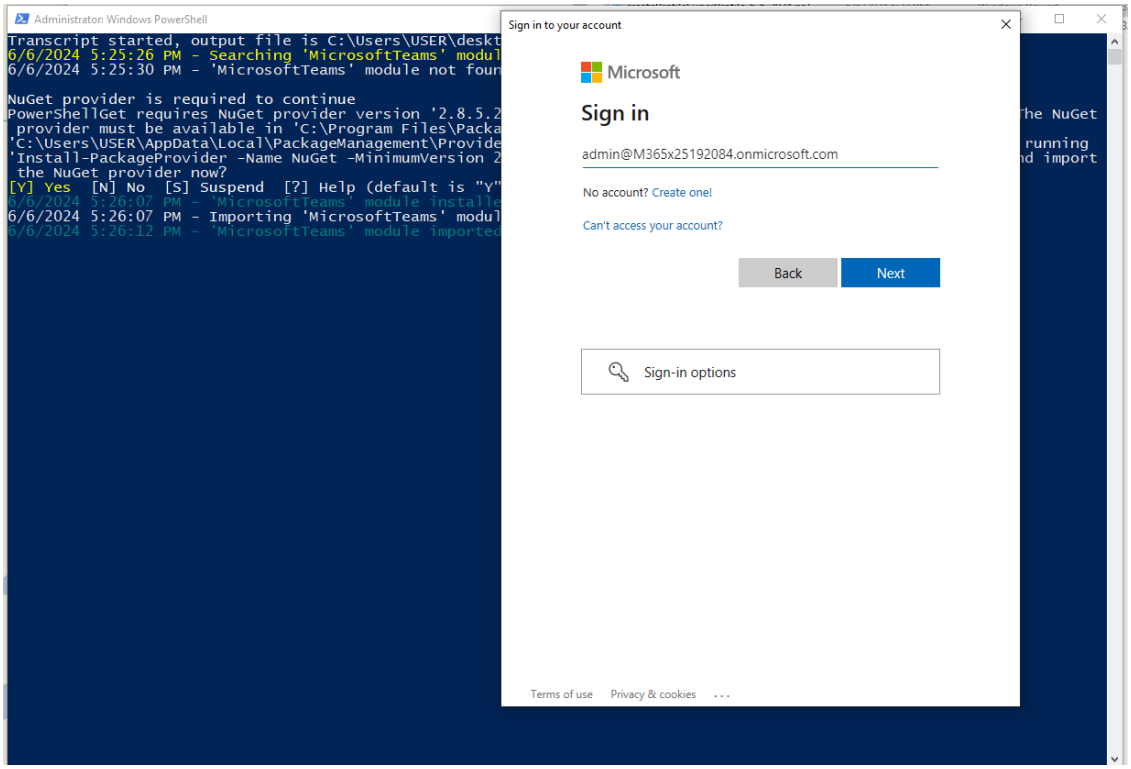
12. Open PowerShell console and run the following policy:

```
Set-ExecutionPolicy -ExecutionPolicy
Bypass
```

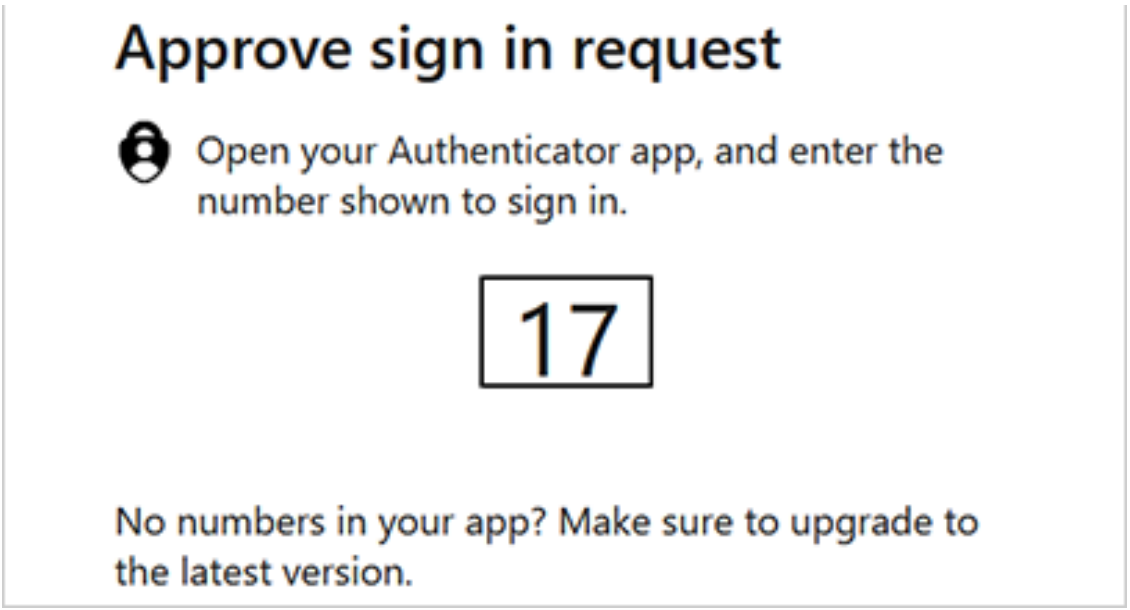
The following message may appear in the console if the above command is not run.



13. Run the script createProfileSuperProfile-dd-m-yyyy.ps1 as Administrator. Once running, you are prompted to enter the credentials of the Azure customer tenant account.

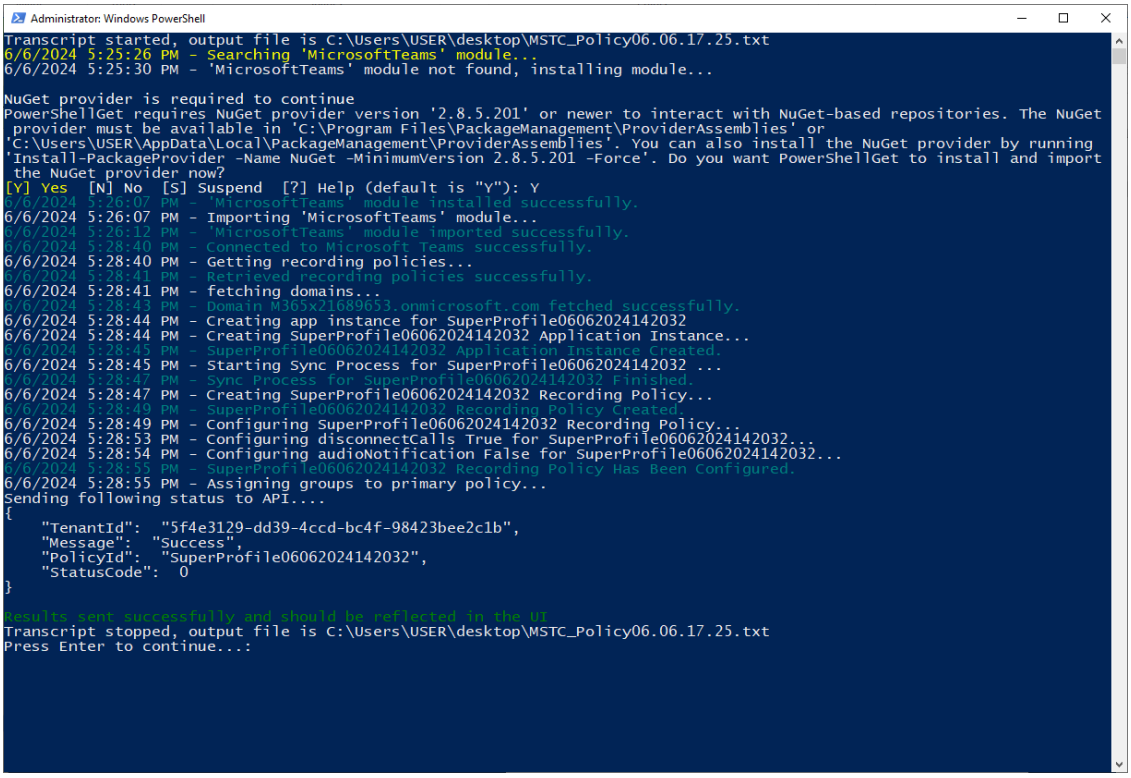


14. Enter Admin credentials of your customer tenant and authenticate the tenant using the Microsoft Authenticator when prompted.

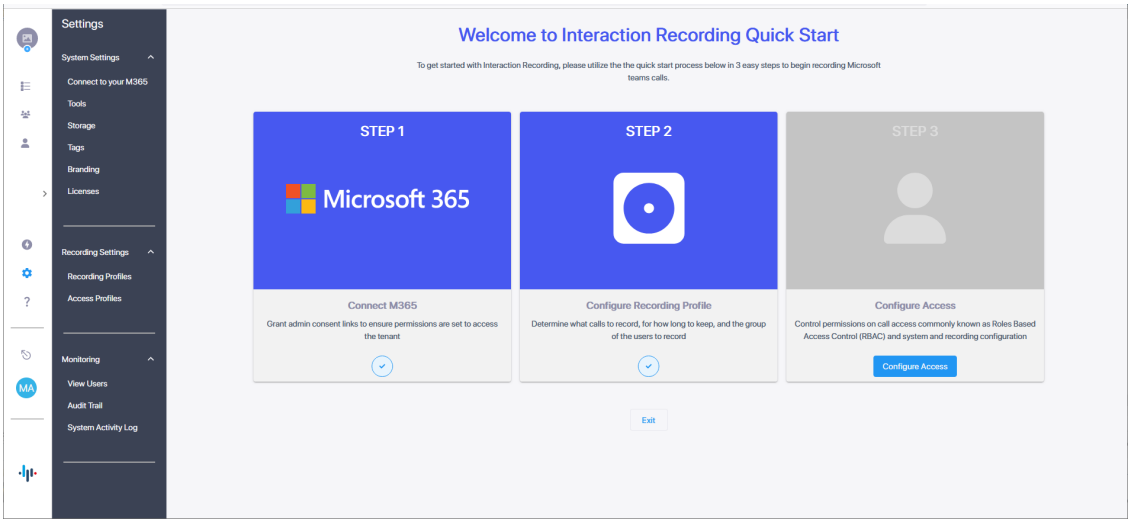


The script supports Multifactor authentication.

Once the script has successfully completed, a confirmation message is displayed in the PowerShell console as shown below.

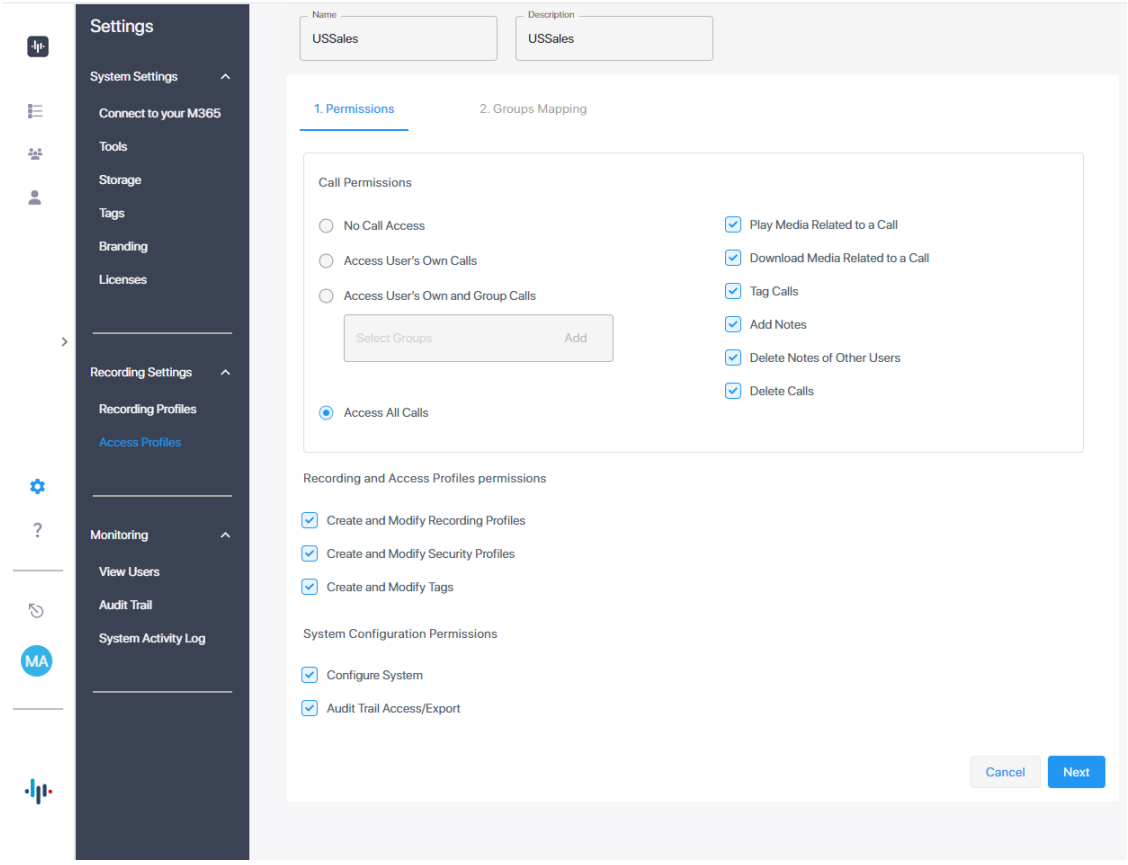


15. Return to the wizard. Notice that Step 1 and Step 2 have completed. Proceed to Step 3.



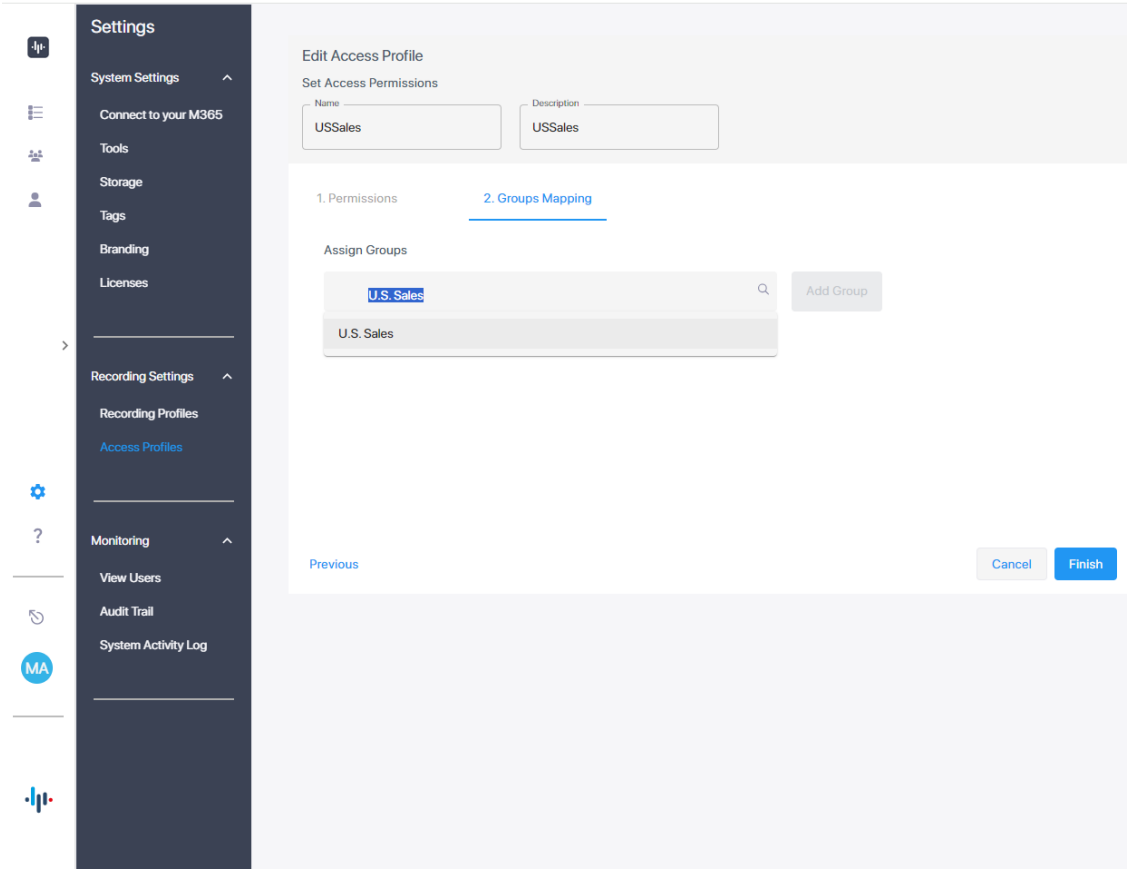
16. Click **Configure Access**.

17. Configure the Access Profile (see Adding an Access Profile on page 83).

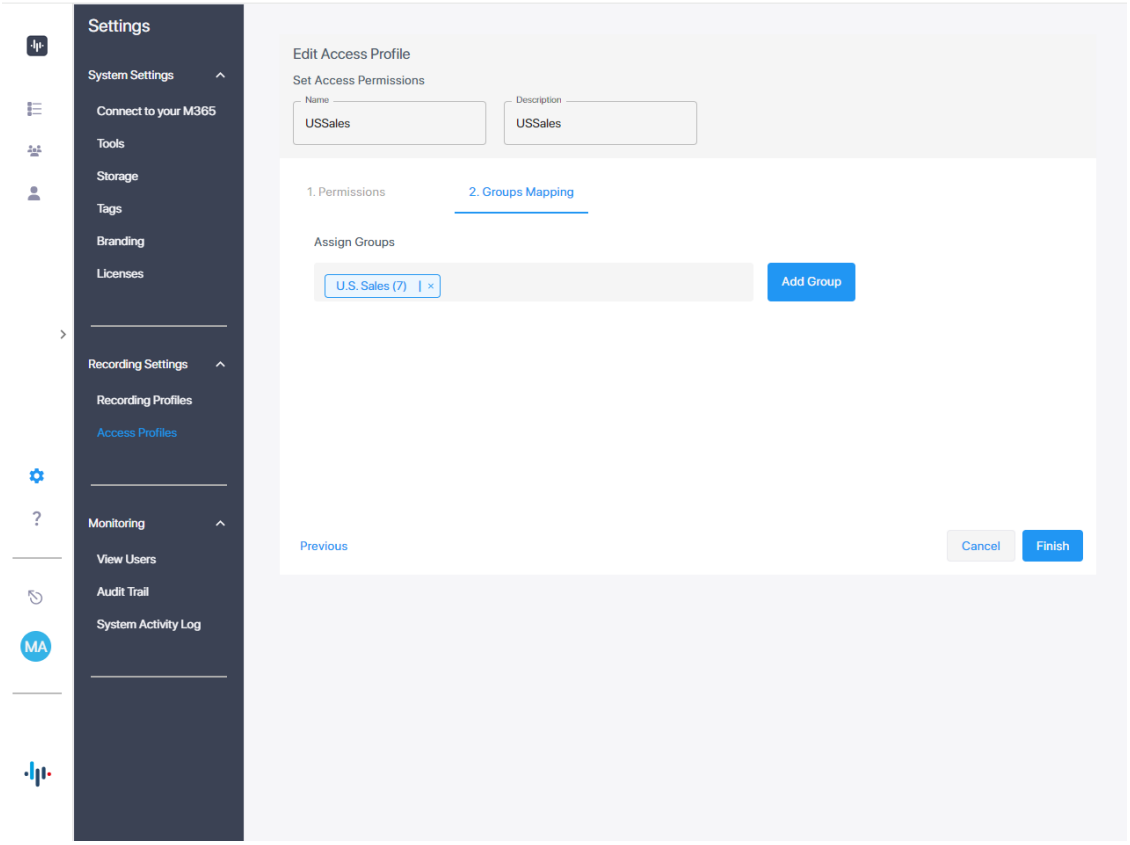


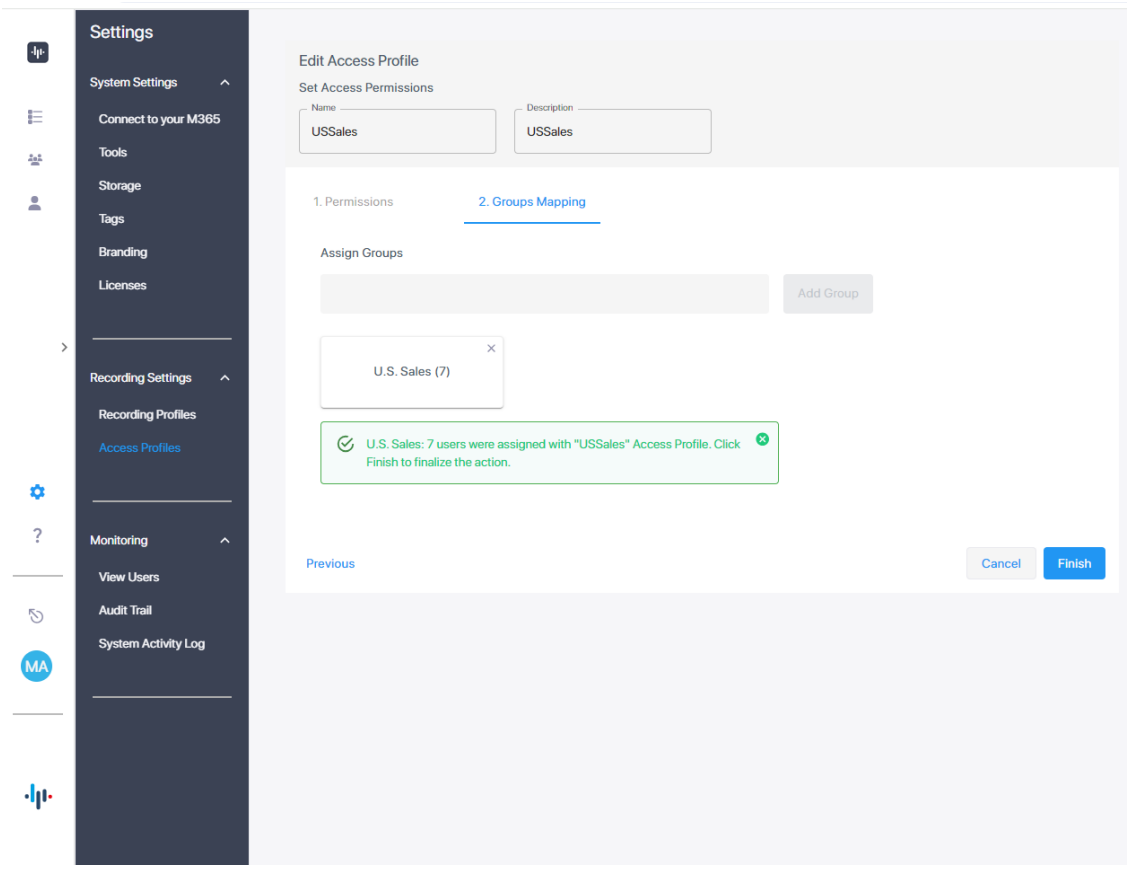
In the example above, an access profile has been assigned with maximum permissions to access all calls and perform all available configuration actions in the Web interface.

1. Click **Next**.



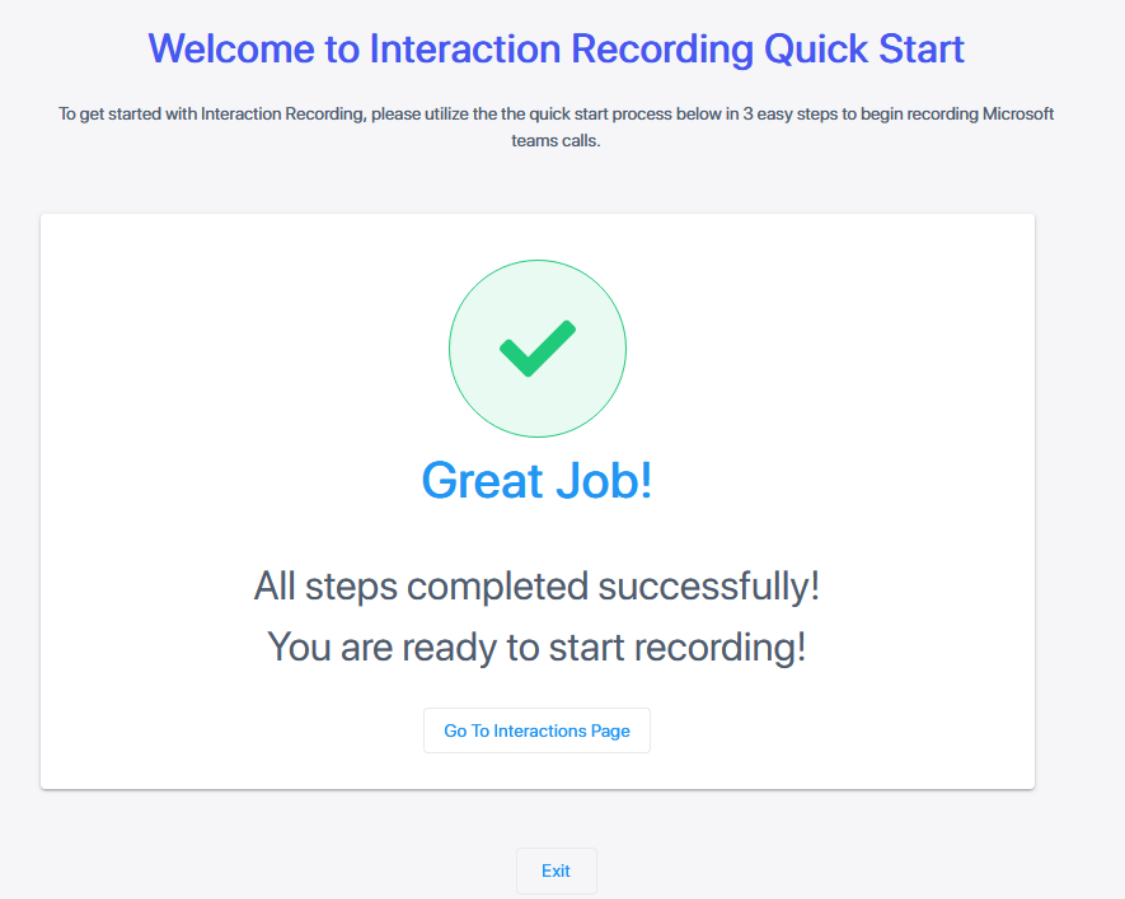
2. Assign Groups: Start typing the name of the AAD group to assign, the group name is validated and then displayed; click **Add Group**.





The Access Profile group assignments are synchronized automatically with your M365 platform.

3. Click **Finish**; the following confirmation message is displayed indicating successful completion of the wizard.



Web Interface Elements

Once you have successfully onboarded your service, you can start using the AudioCodes Live SmartTAP for managing SmartTAP recordings. See the following overview of interface elements:

- Settings Navigation Pane below
- Toolbar on the next page

Settings Navigation Pane

The navigation pane includes the options described in the table below

Option	Description
System Settings	
Connect to your M365	Connect to M365 on page 146
Tools	Tools on page 148
Storage	Bring-Your-Own-Storage on page 153
Tags	Manage Tags on page 159

Option	Description
Branding	Branding on page 161
Licenses	Licenses on page 163
Recording Settings	
Recording Profiles	Managing Recording Profiles on page 47
Access Profiles	Managing Access Profiles on page 82
Monitoring	
View Users	Managing Users on page 166
Audit Trail	Viewing and Searching an Audit Trail on page 172
System Activity Log	System Activity Log on page 175

Toolbar

The toolbar includes the options described in the table below.

Icon	Item	Description
	Branding on page 161	Lets you upload your corporate logo to the Web interface toolbar.
	Interactions on page 94	Displays all recorded interactions of targeted users.
	Managing Active Calls on page 132	Displays the list of active recorded calls for all targeted users attached to recording profile groups of the customer tenant.
	My Active Call on page 143	Displays the details of the Active call of the logged in Admin user.
	Quick Start on page 15	Opens the Onboarding setup wizard which lets you do the following: ■ Consent to all required M365 permissions. ■ Configure Recording profiles

Icon	Item	Description
		■ Configure Access profiles
	System Settings on page 146	Opens the System Settings menu.
	Help	Opens a link to the Online Help.
	Logout	Closes the active session.
	Logged in user	Details of the logged in user.

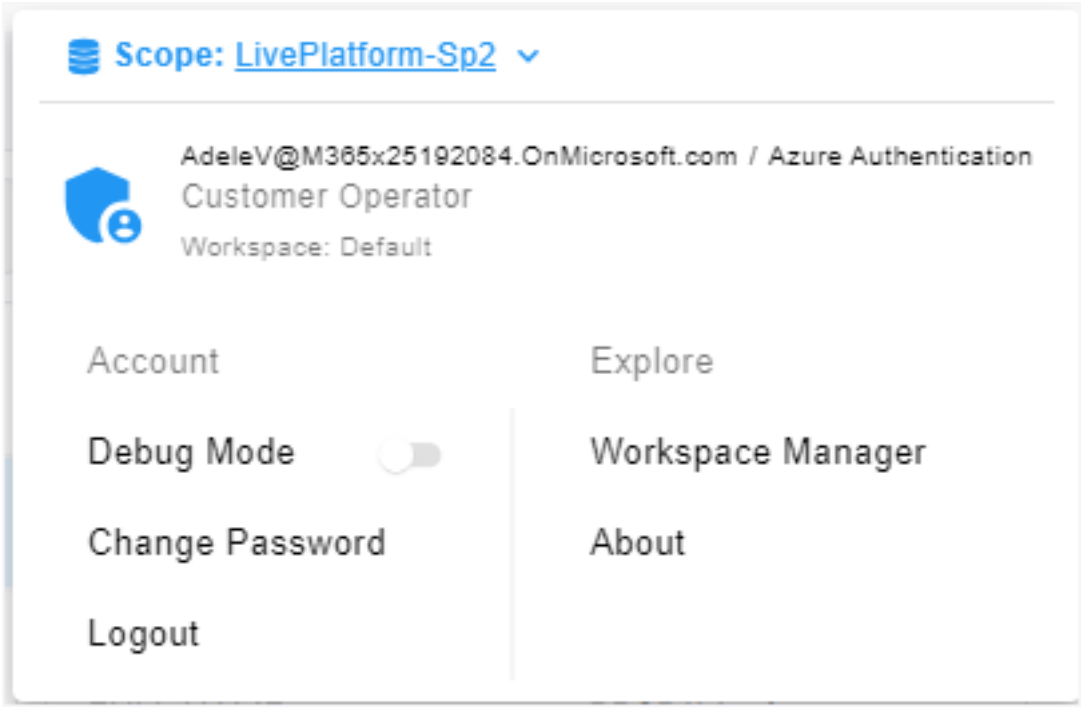
Monitor Onboarding Process in Live Platform

Once you have completed the Quick Start, you can login to the Live Platform and monitor the progress of the deployment of your new service. Initially a Warning alarm is raised for the service pending the completion of the Quick Start wizard including the granting of all consents by the customer Global Admin. Once the consents have been provided and a secure connection with the customer's M365 platform established, the alarm is cleared.

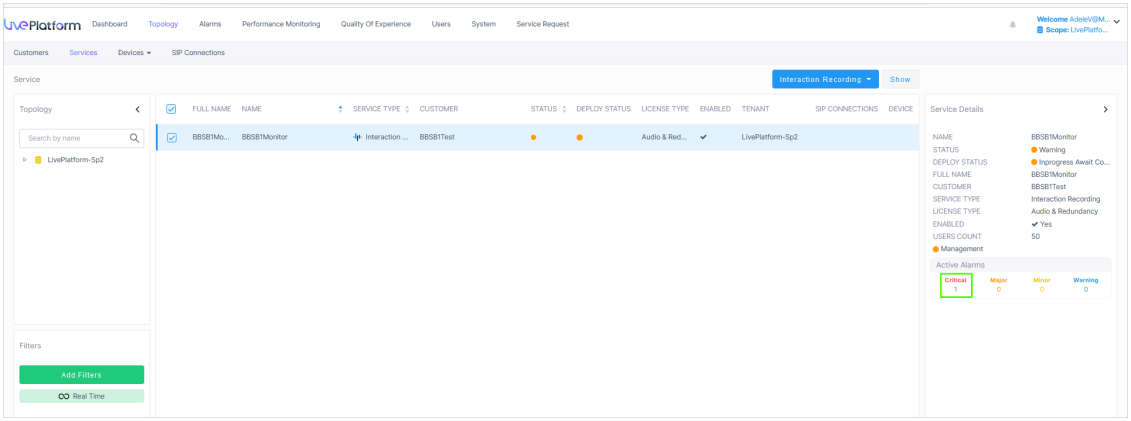
It may take a few minutes for the statuses to update following the successful completion of the Quick Start.

➢ **To login to AudioCodes Live SmartTAP:**

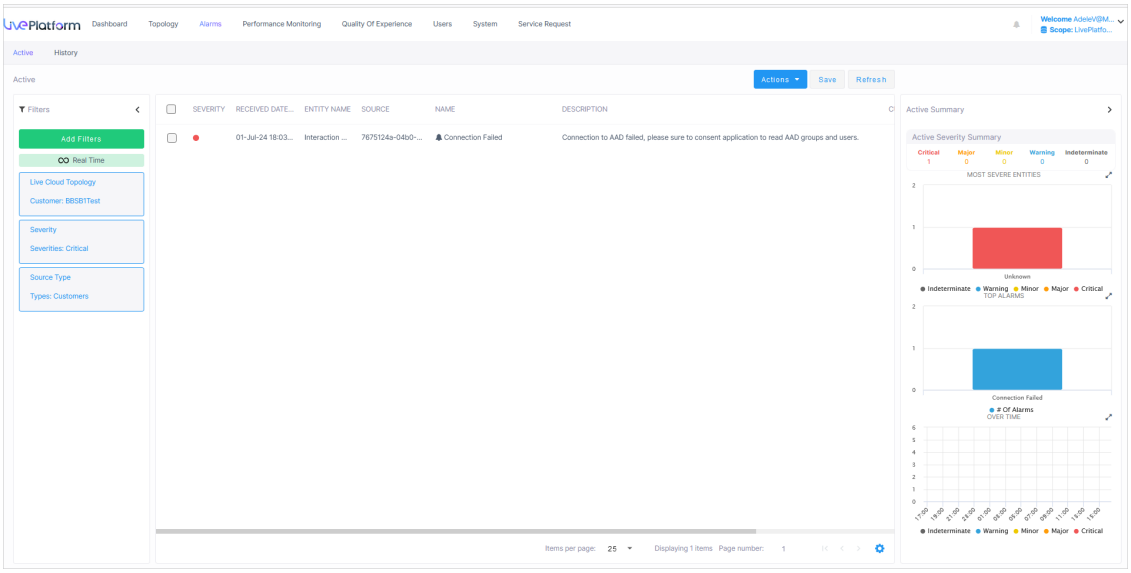
1. Login to the Live Platform with your Live Platform Global admin or customer operator (see Add Live Platform Operators on page 36 and Logging In).



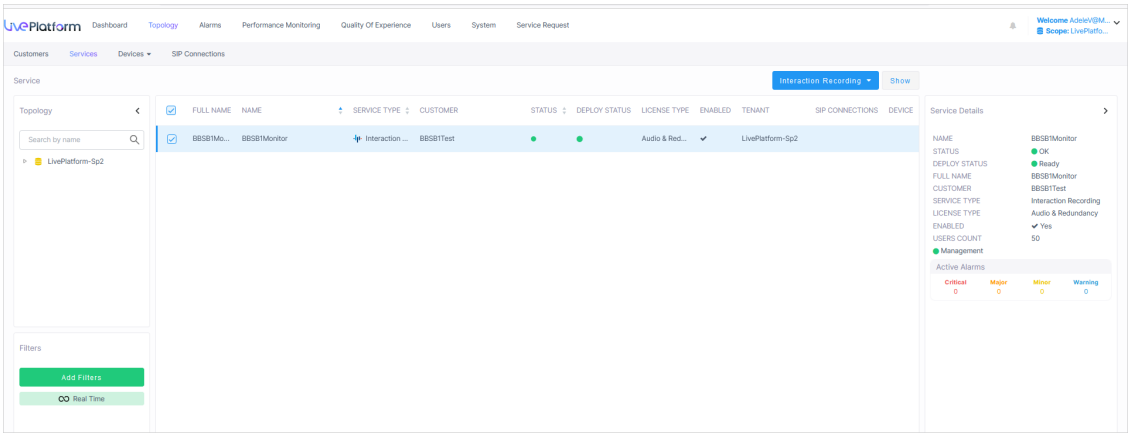
2. In the Menu bar, choose **Topology** and then click the **Services** tab.



3. In the Service Details pane, click the Active Critical alarm to open the Alarms page to display the details of the alarm. The alarm indicates that consent to read AAD Groups and Users is required.



Once consent is provided and the alarm is cleared, the OK and Ready statuses are displayed.



Add Live Platform Operators

When the customer Global admin logged in to the Live Platform portal for first time connection, a connection is established with Azure and the Enterprise Application Registration added under the customer tenant. You must then login to the Azure portal, navigate to this Enterprise application, add the desired customer operators and assign them Live Platform roles.

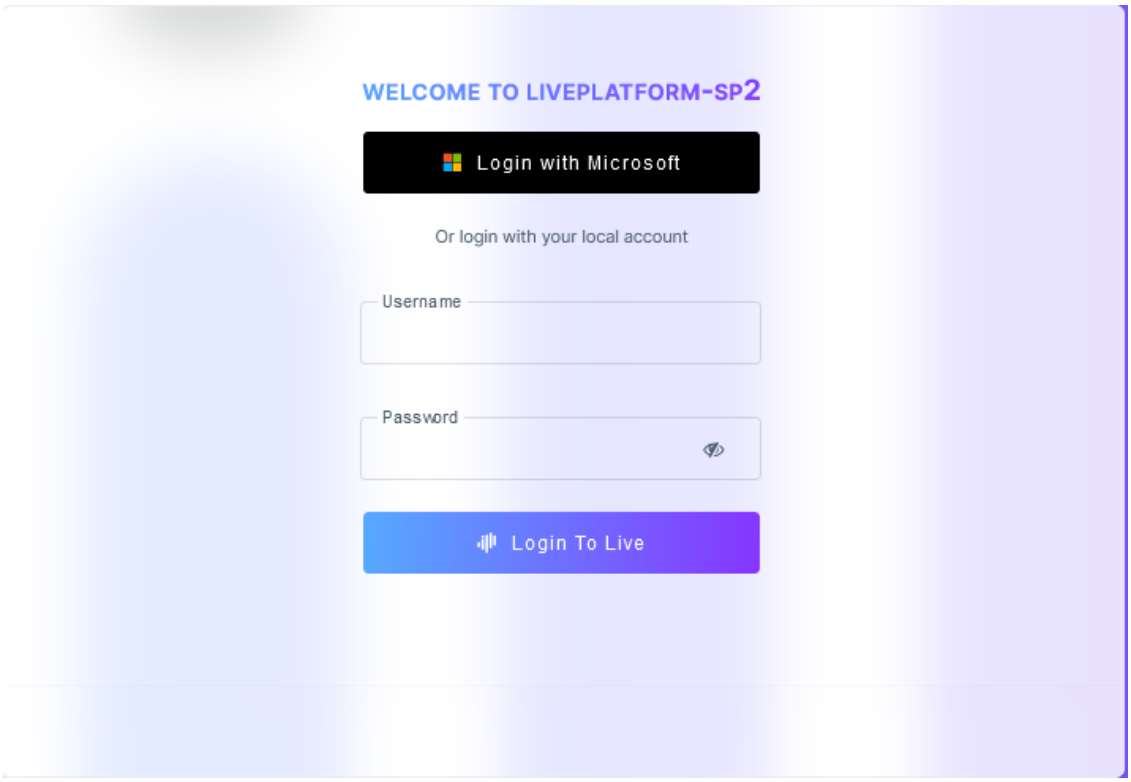
> Perform this procedure with 'Global Admin' permissions for the Azure customer tenant.

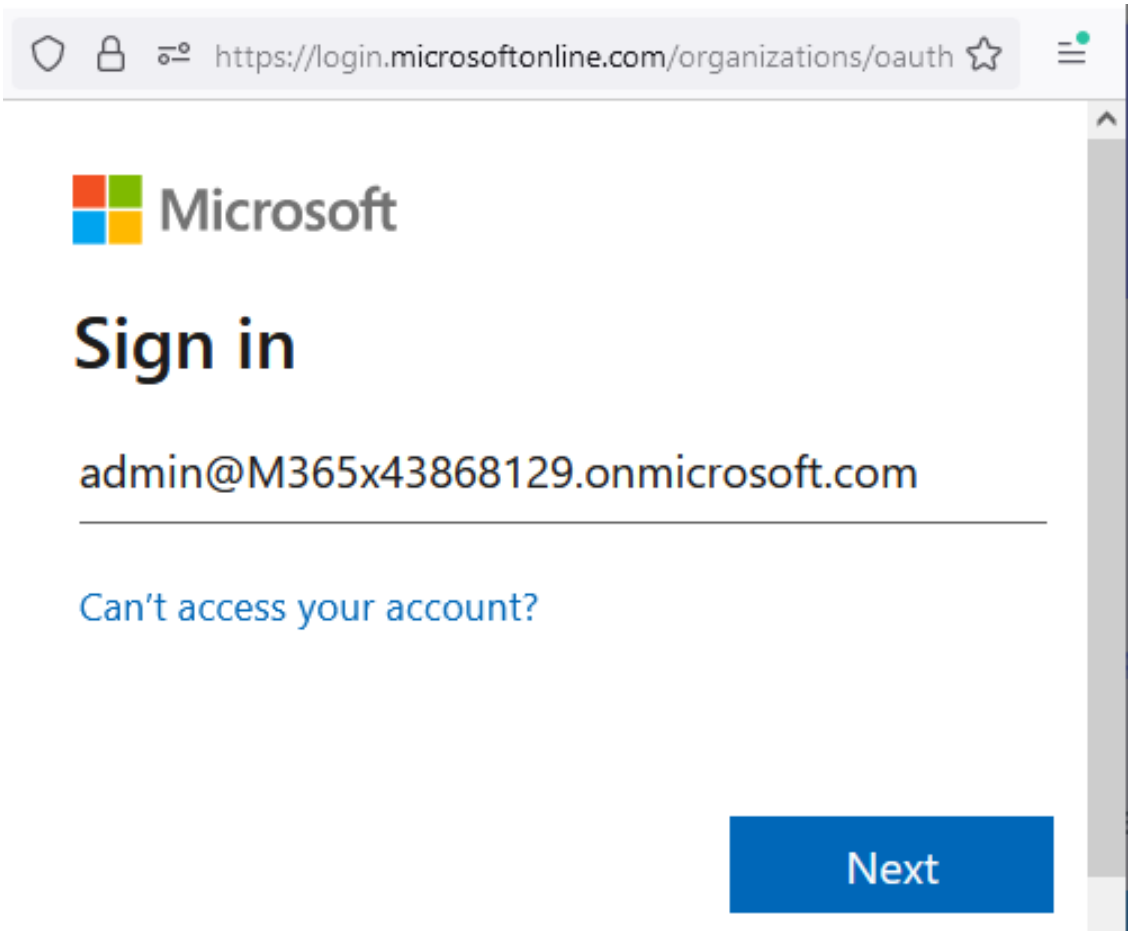
The following roles can be assigned to the AudioCodes Live SmartTAP portal operators:

- Operator
- Monitor
- Lite Operator

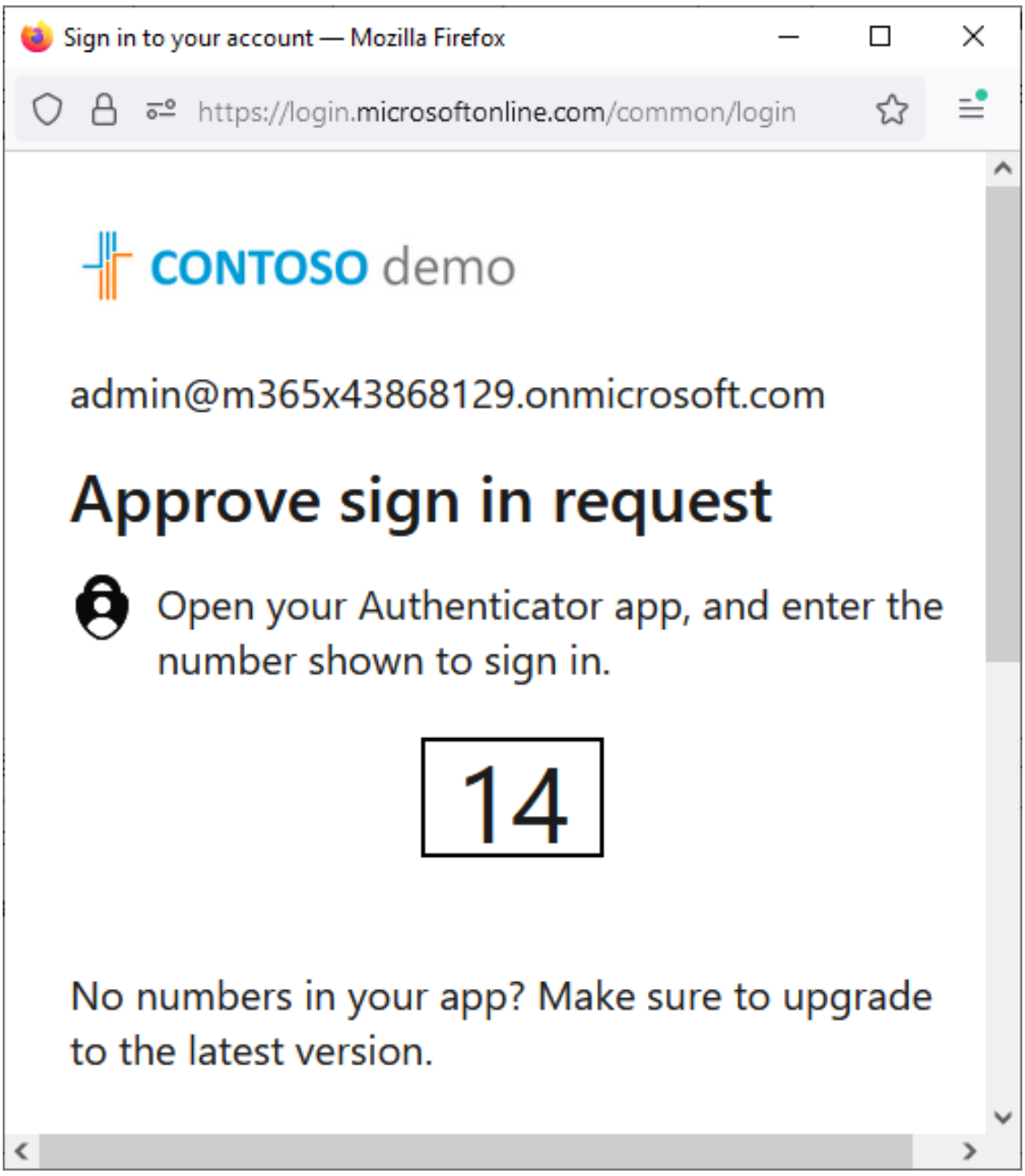
➢ **Do the following:**

1. Login to the Live Platform portal with the Global admin credentials of the customer tenant.

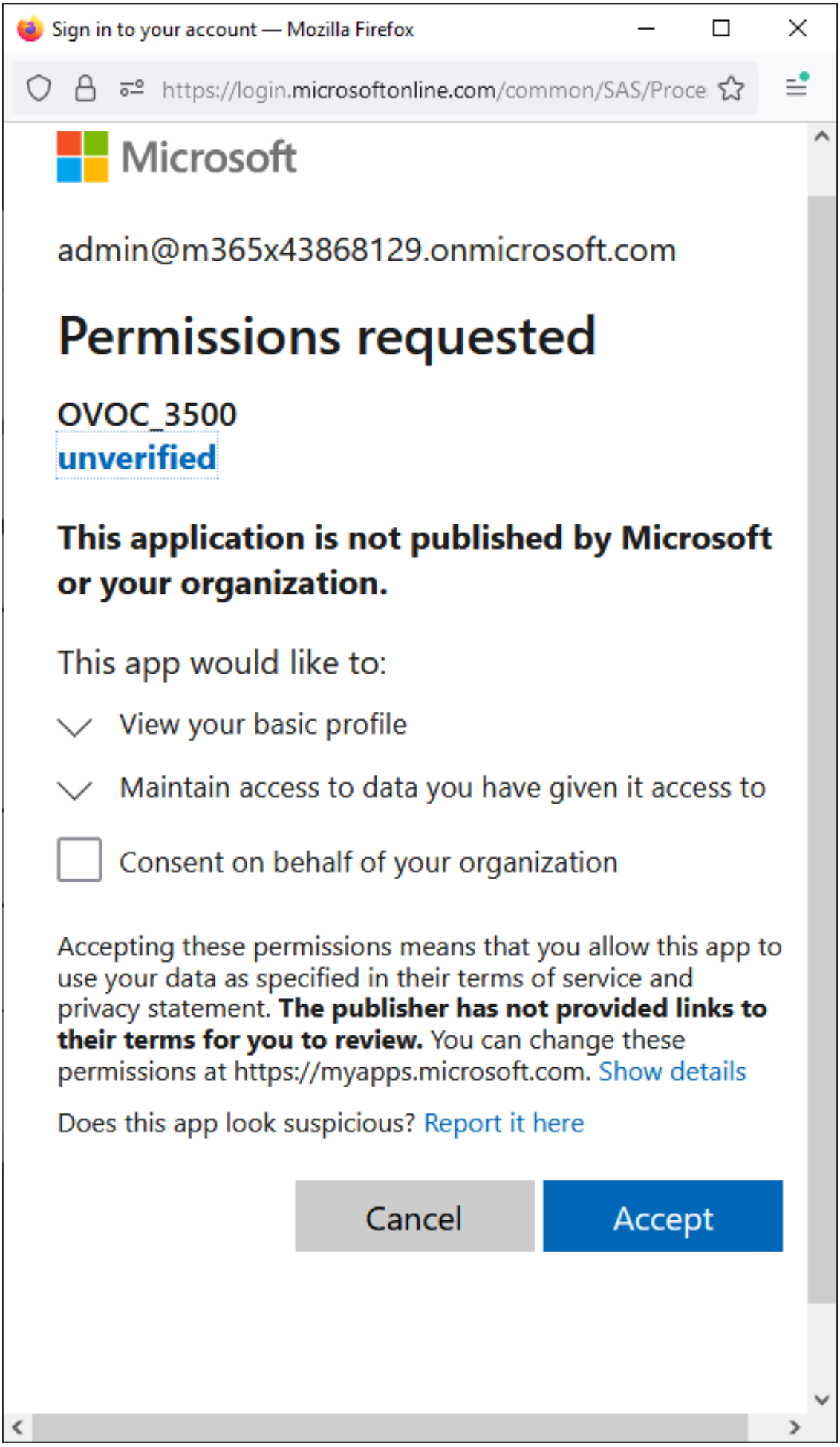


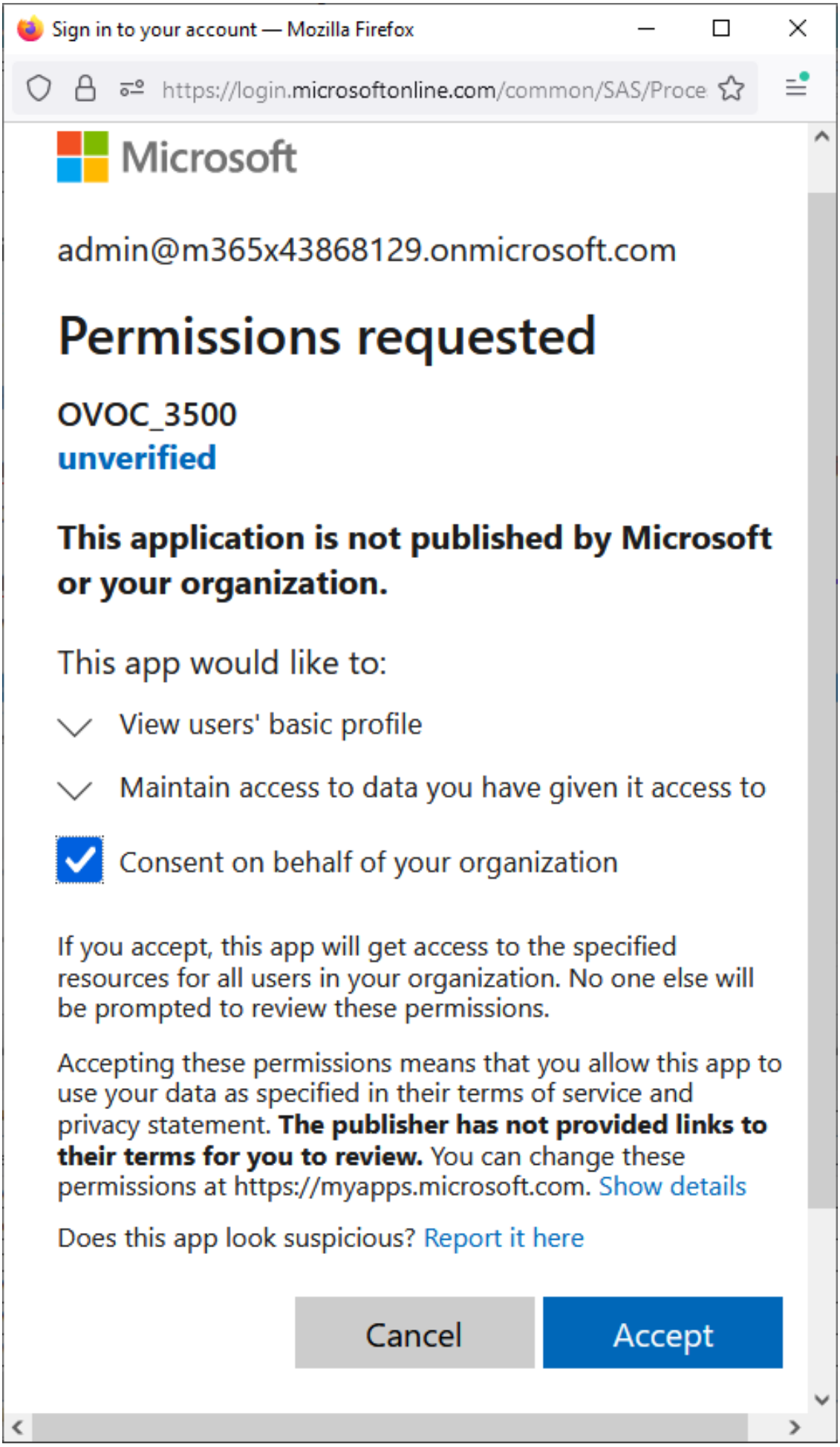


2. Add the tenant account to the Microsoft Authenticator and approve the Sign-in request.



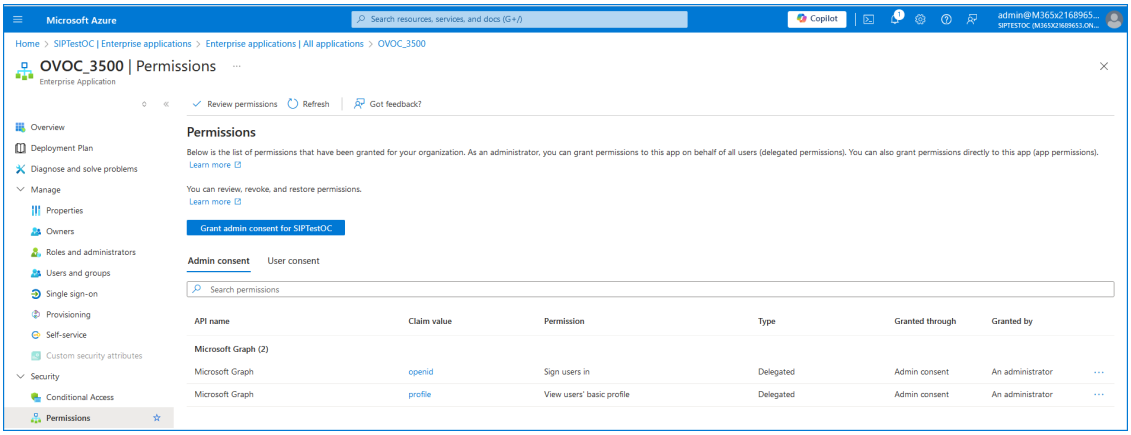
3. Select the **Consent on behalf of your organization** check box, and then click **Accept**.


Sign in to your account — Mozilla Firefox
https://login.microsoftonline.com/common/SAS/Proce
Microsoft
admin@m365x43868129.onmicrosoft.com
Permissions requested
OVOC_3500
unverified
This application is not published by Microsoft or your organization.
This app would like to:
View your basic profile
Maintain access to data you have given it access to
Consent on behalf of your organization
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. The publisher has not provided links to their terms for you to review. You can change these permissions at https://myapps.microsoft.com. Show details
Does this app look suspicious? Report it here
Cancel
Accept

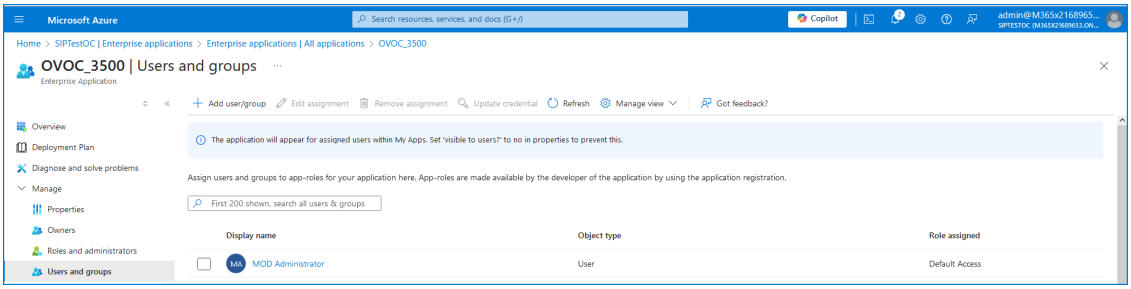

Sign in to your account — Mozilla Firefox
https://login.microsoftonline.com/common/SAS/Proce
Microsoft
admin@m365x43868129.onmicrosoft.com
Permissions requested
OVOC_3500
unverified
This application is not published by Microsoft or your organization.
This app would like to:
View users' basic profile
Maintain access to data you have given it access to
Consent on behalf of your organization
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. Login to the Azure portal with Tenant 'Admin' permissions and navigate to the newly created Enterprise application.

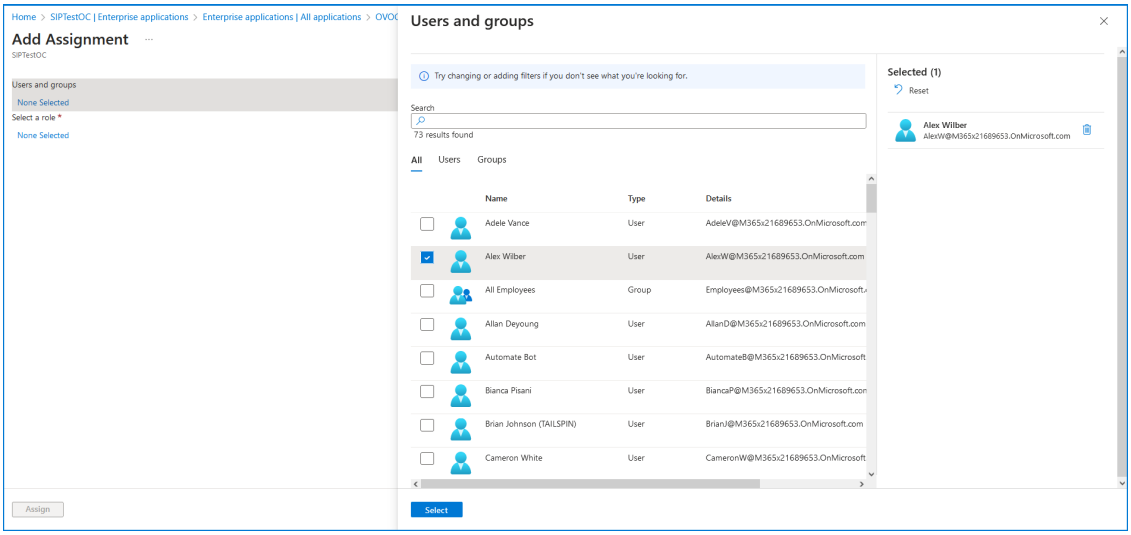
5. In the Navigation pane, select **Permissions**. Note the permissions that were granted to the customer Global Admin.



6. In the Navigation pane, select **Users and groups**.



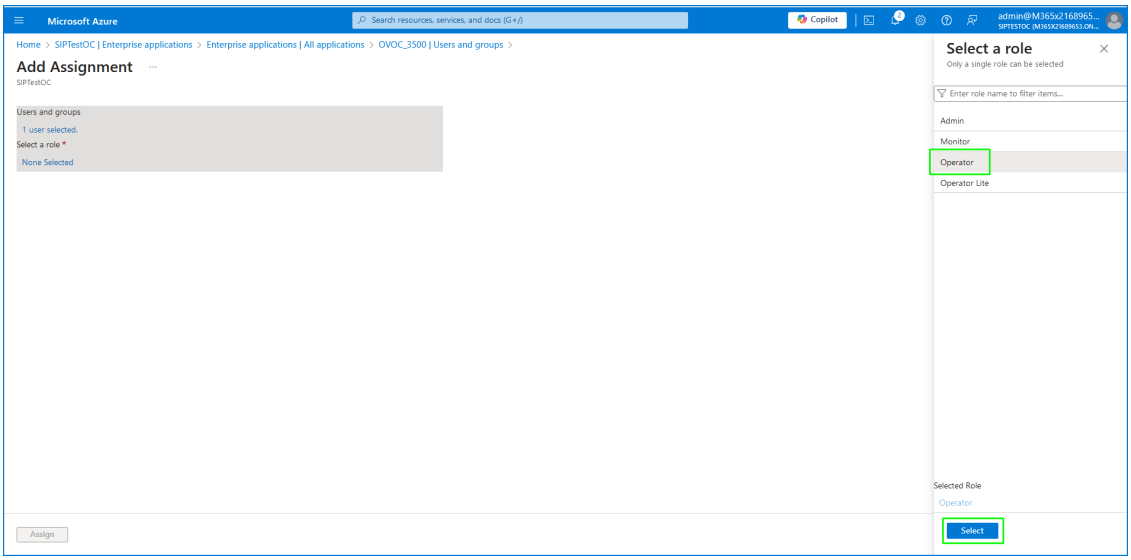
7. Click **Add user/group**.



8. In the left pane, select **Users**, in the right pane, select the user for which you wish to add an assignment and then click **Select**.

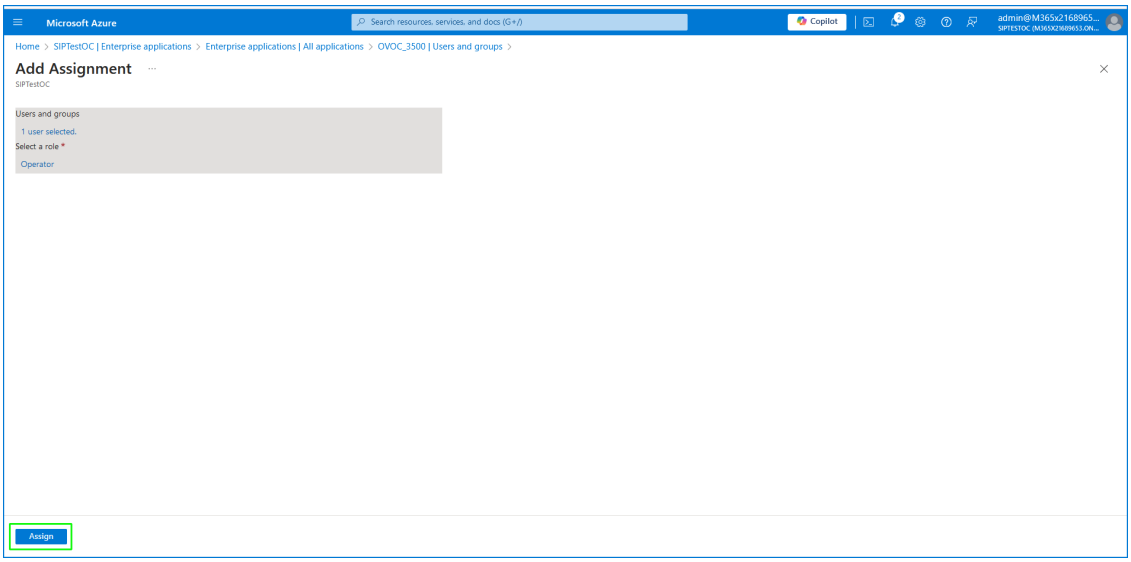
9. In the left pane, click the **None Selected** link to select a role, and then in the right pane, assign one of the following permissions:

- Monitor
- Operator
- Operator Lite

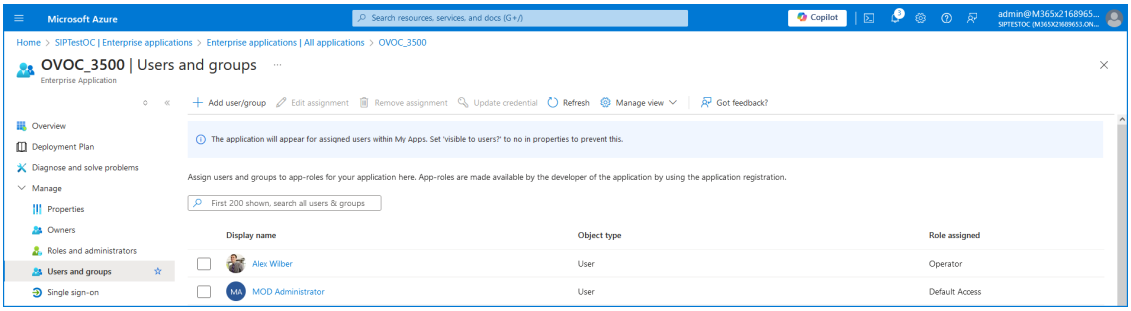


10. Click **Select** to confirm selection.

11. Click **Assign**. The new user with assigned role “admin” is displayed in the screen below.



The user Alex Wilber is added a customer operator.

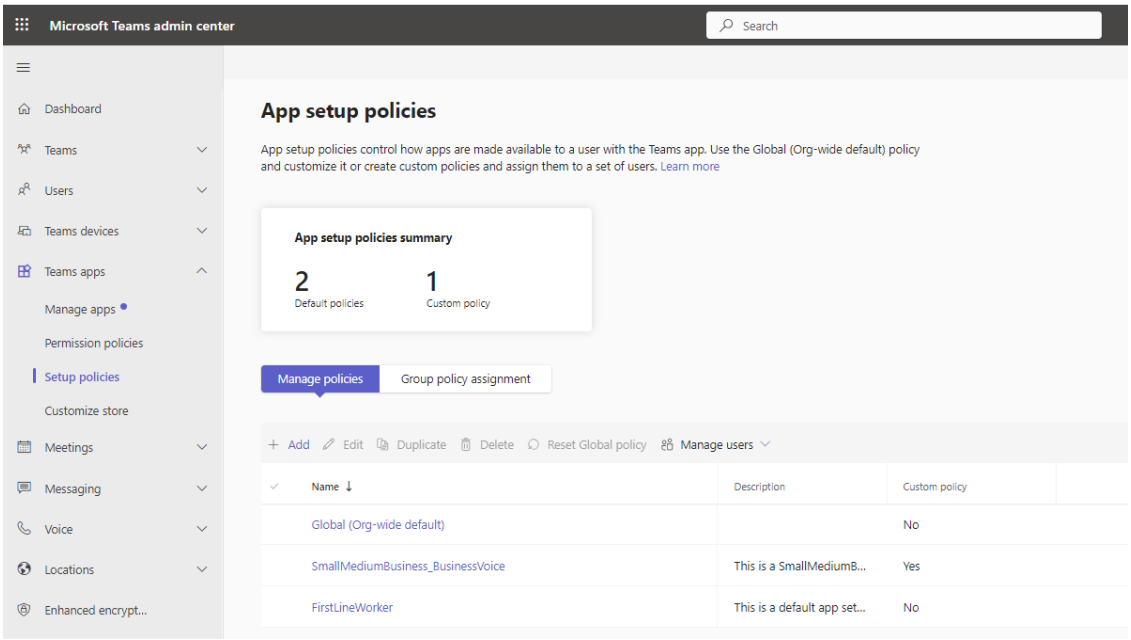


Add and Pin SmartTAP Teams App

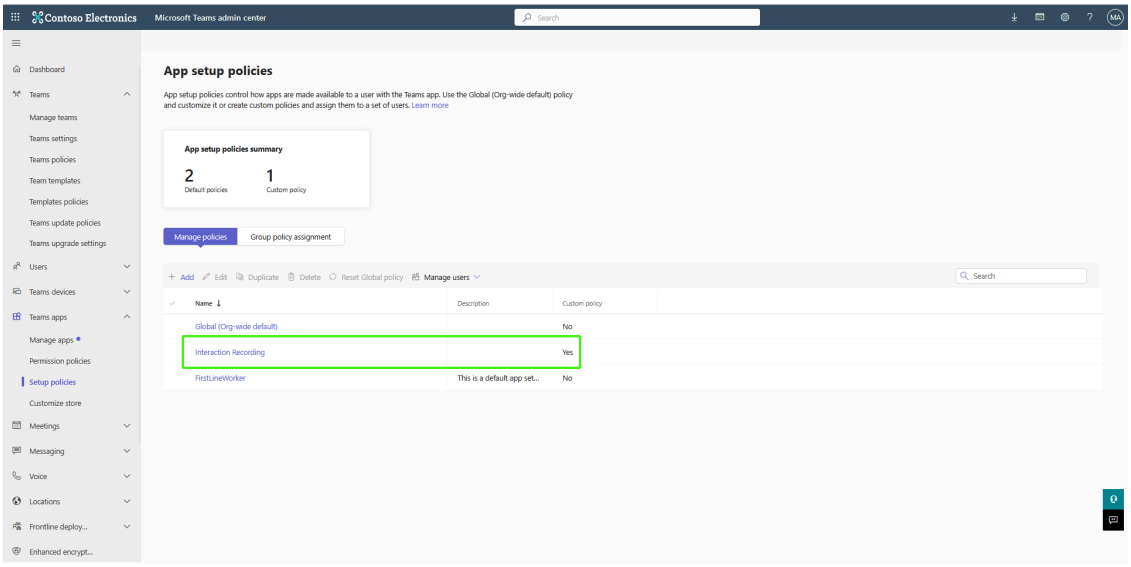
Admins are recommended to add and pin the AudioCodes Live SmartTAP Teams app to the whole organization or to Recording groups that will be using the app.

➢ To add and pin the Teams app:

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

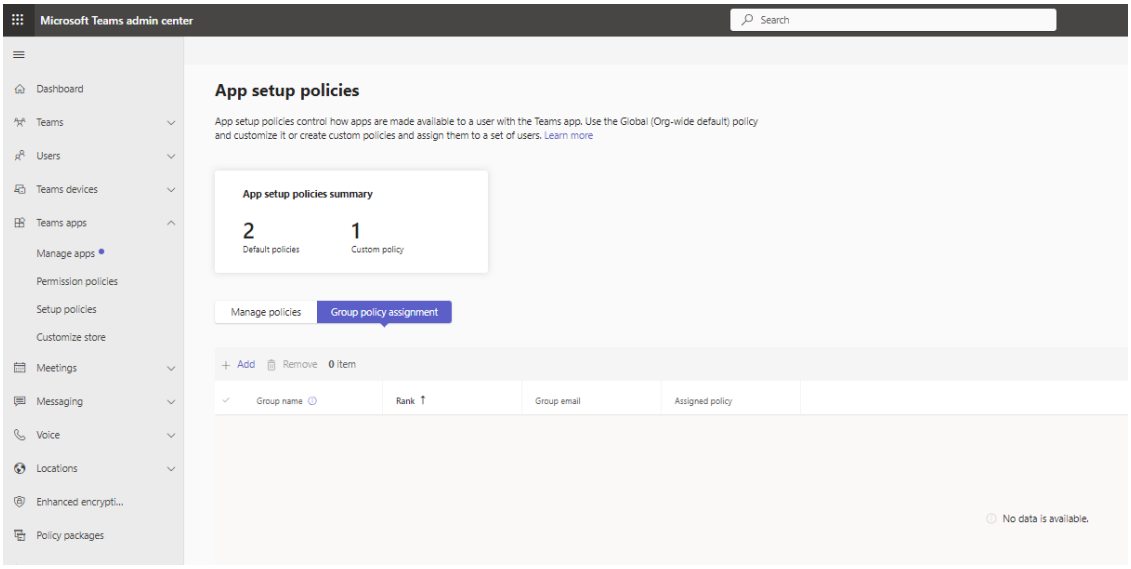


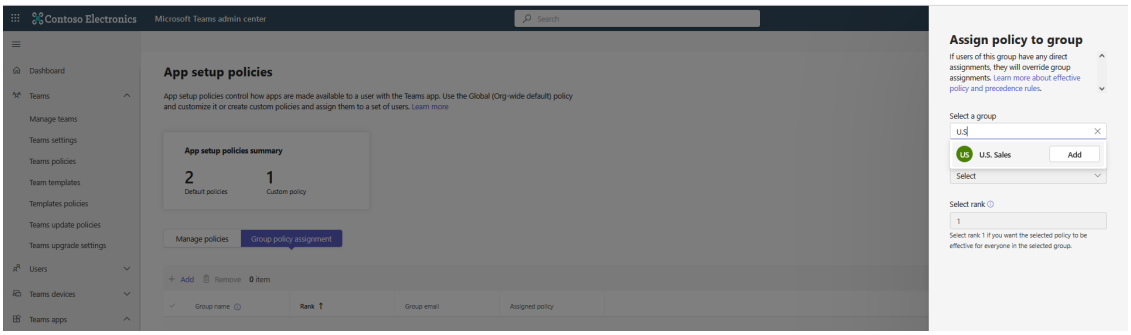
2. Add SmartTAP app to the installed apps and to the pinned apps (recommended) so that it'll be displayed for users by default.



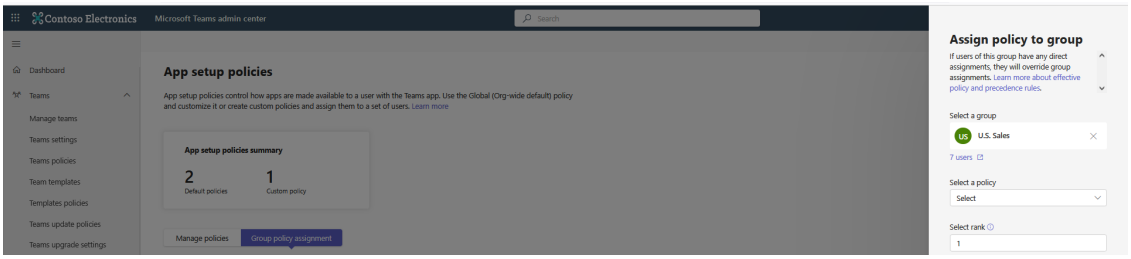
3. To apply to a group, create a separate policy, add the SmartTAP Teams app to the installed and pinned apps, and then assign group(s) as shown below.

4. To assign to a group, click **Group policy assignment** under the setup policy option.

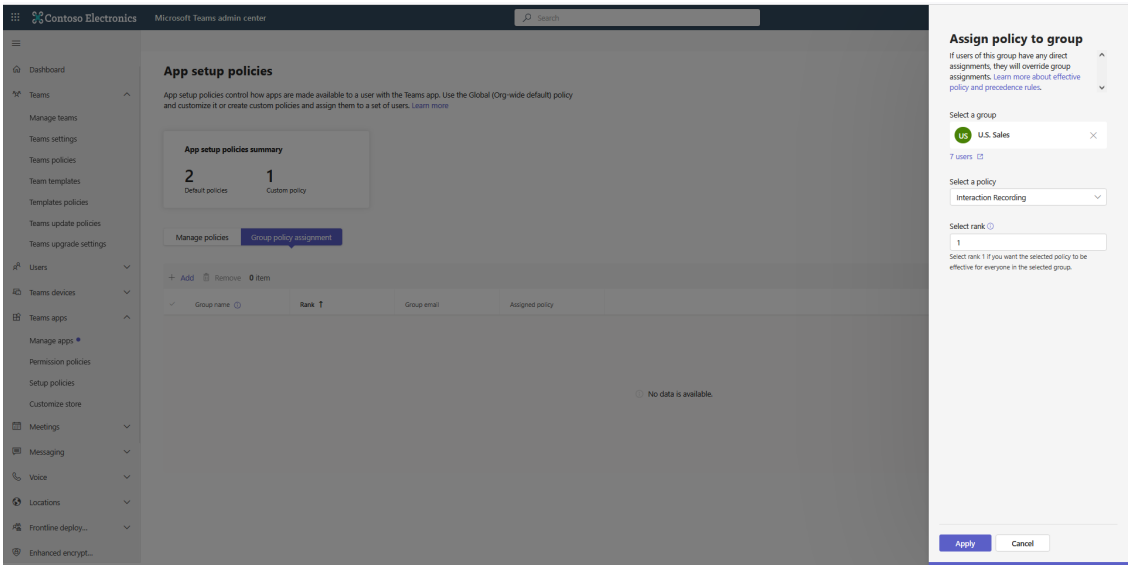




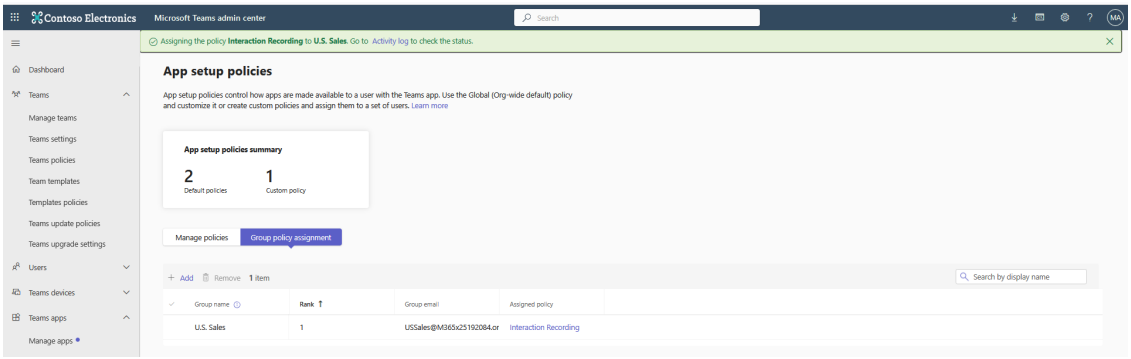
5. Select the Recording group to which to assign the policy, and then click **Add**.



6. Select a policy (SmartTAP in the example shown below) and then click **Apply**.



The new policy is assigned.



3 Day Two Management using the SmartTAP User Interface

This interface includes the following configuration and monitoring features:

- Recording Settings on page 47
- Interactions on page 94
- Managing Active Calls on page 132
- My Active Call on page 143
- System Settings on page 146
- Monitoring on page 166

Recording Settings

- Managing Recording Profiles below
- Managing Access Profiles on page 82

Managing Recording Profiles

Recording profiles configures the recording capabilities of AAD groups of targeted users. A profile may be assigned to one or more groups. In the Quick Start wizard, you created an initial Recording profile. You can modify this profile and create additional profiles. The Recording profile includes the following capabilities:

- Determines which call types may be recorded.
- Sets Data Retention policies.
- Configures Azure Blob Storage region location to store calls.
- Attaches AAD groups including Targeted users to recording profiles.
- Blocks recording of calls according to specific numbers.
- Determines the time of day you wish to record or to prevent recording of targeted users.
- Configures Microsoft Teams Calling Policies.

To comply with Microsoft Bot Grouping API for meeting recording, storage optimization and avoiding redundancy, SmartTAP implements the following policy for recording large meetings:

- **Recording:** SmartTAP stores only one copy of a meeting recording for the organizer, regardless of the number of targeted participants. For example, in a 300-person call with 300 targeted users for recording, SmartTAP stores one copy of the call for the organizer and another recording for the rest of the 299 users. This ensures efficient use of storage space.

When users belong to different recording policies, the result is one recording for all users of the same recording policy.

- **Playback:** Playback of a user recording of a meeting starts from the point the user joins the meeting and ends when user leaves the meeting.
- **Retention Period**: The retention period for these recordings is based on the recording profile retention period of the targeted users. The longest retention period among the recording user groups (organizer vs. the rest of the targeted users) will apply.

Download of meeting is not supported.

See also:

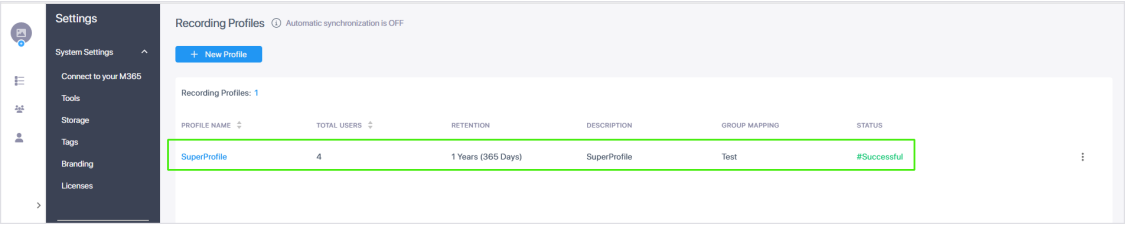
- Adding Recording Profiles on the next page

- Modifying Recording Profiles on page 66
- Synchronizing Recording Profiles on page 71
- Recording Profile-Call Type Configuration Examples on page 81
- Disabling Recording Profile on page 79
- Deleting Recording Profile on page 80

➢ **Do the following:**

1. In the Icon pane, click , and then in the Navigation pane, select **Recording Settings** > **Recording Profiles**.

   The Recording profile configured in the Wizard is displayed as "Successful".



   The table below describes the parameters in this table.

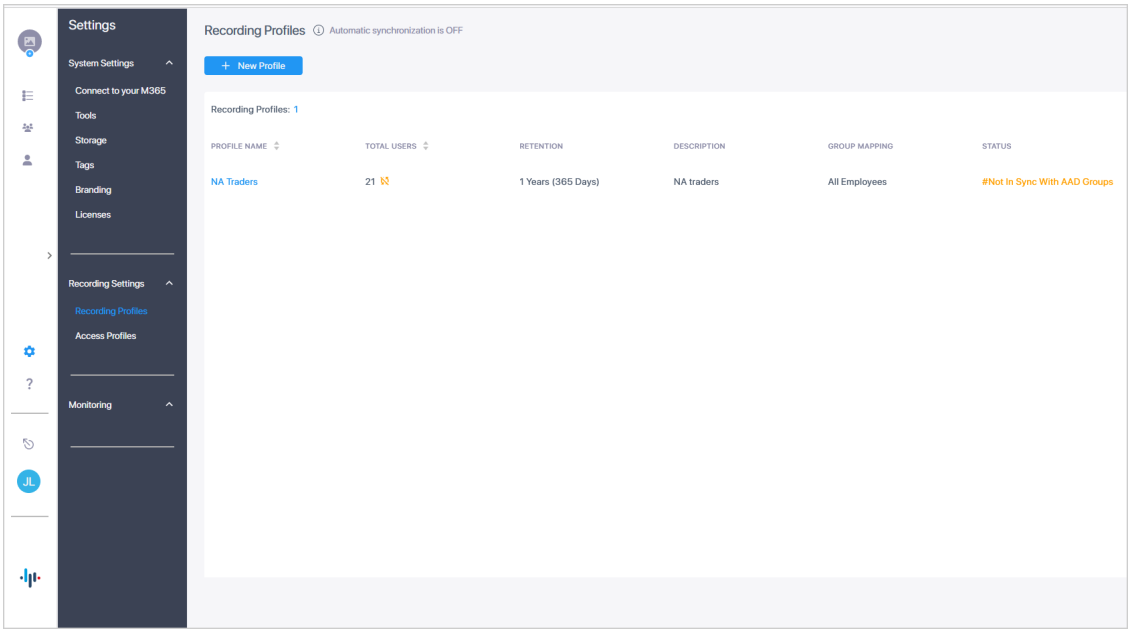
Field	Description
Profile Name	Enter a name for the new recording profile.
Total Users	The total number of users with Targeted user recording licenses.
Retention	Retention time period for calls associated with the profile. Default: One year.
Description	Description of the recording profile.
Group Mapping	Azure tenant Security group that is mapped to this profile.
Status	Indicates the status of the synchronization with Azure tenant: ■ Not in Sync with AAD Groups ■ Successful

Adding Recording Profiles

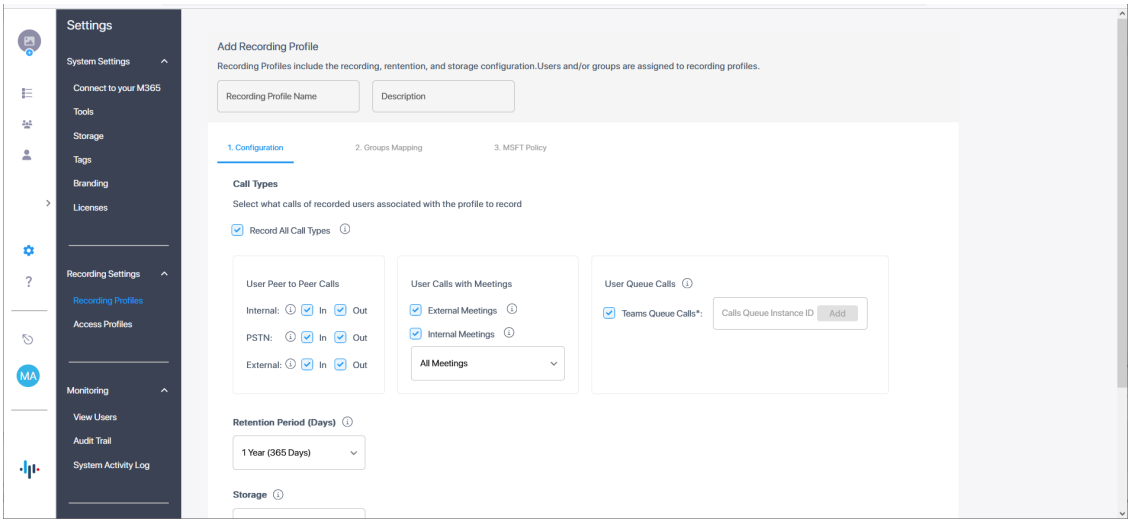
The Quick Start wizard process created an initial Recording profile for your tenant. You can then add additional recording profiles for targeted users.

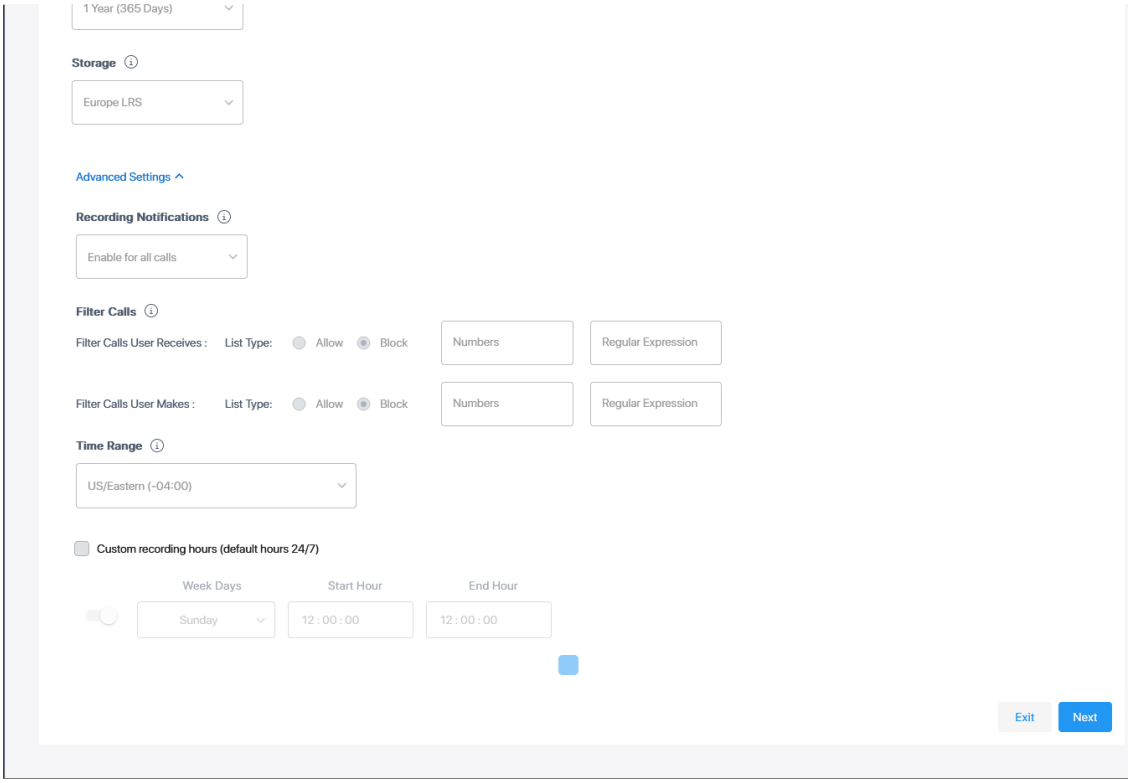
➢ Do the following:

1. In the Icon pane, click , and then in the Navigation pane, select **Recording Settings** > **Recording Profiles**.



2. Click **New Profile**.





3. Configure profile according to the tables below.

Field	Description
Profile Name	Enter a name for the new recording profile.
Profile Description	Enter a description of the new recording profile.
All	Record all calls that the recording profile user participates in as calling party. This option is enabled by default or when a new recording profile is created.
User Peer-to-Peer Calls When Call Types 'PSTN', 'Internal' or 'External' are enabled, and then the call is escalated to a Conference call (when additional parties are added to the call), the escalated Conference part of the call will be recorded as part of the original peer-to-peer call recording leg.	
Internal	Refers to Peer-to-Peer calls between the targeted recording profile user and other users within the same domain. One of the following values: ■ In: Records Internal calls that the Targeted user receives. ■ Out: Records Internal calls that the Targeted user makes.

Field	Description
PSTN	Refers to Peer-to-Peer calls between the Targeted recording profile user and parties outside of the organization's network on PSTN. One of the following values: ■ In: Records PSTN calls that the user receives. ■ Out: Records PSTN calls that the user makes.
External	Refers to Peer-to-Peer calls between the Targeted recording profile user and parties with Federated domain or any public Microsoft Teams domain. ■ In: Records External calls received by the Targeted recording profile user from Federated Domain users. ■ Out: Records External calls made by the Targeted recording profile user to Federated Domain users.
User Calls with Meetings	
External Meetings	Refers to Targeted user calls with meetings that are scheduled by External users and belong to an External organization. ⚠ This option is supported by Microsoft Teams Integration and with “Full Time” Recording Type only.
Internal Meetings	Refers to Targeted user calls with meetings that are scheduled by Internal users from the same domain as the Targeted user. This option records Teams calls with an Internal conference bridge in the Enterprise domain. An Internal Conference is a scheduled, ad-hoc meeting that occurs on a bridge belonging to the targeted user organization. When enabled, all user calls with internal meetings are recorded according to the below options. When disabled, none of the user calls with internal conferences are recorded. One of the following options: ■ **All Meetings:** Records meetings with both internal and external participants. ■ **External Participants:** Records only meetings with External participants. External participants are those participants who either don’t have an Azure object id or don't belong to the recording organization. For example, participants joined from PSTN, guests from Web or from Federated organization or

Field	Description
	from a Teams home client. The application starts recording the targeted user call leg to the meeting when an external participant joins the meeting and continues recording until the targeted user disconnects or the meeting bridge disconnects the call.
Teams Queue Calls (transfer mode)	Record Microsoft Teams calls that have been retrieved from a queue by a call agent. The recording is triggered as soon as the call is connected to an agent. Recording by IDs is only supported when routing method is set to 'Transfer'.
Call Queues Instance ids	Comma separated list of the call queue instance ids which should be recorded (see Retrieving Recording Queue Instances on page 62). Relevant when Teams Queue Calls (Transfer mode) is configured and "All" is not selected. When “All” is selected, all user calls will be recording including calls from any call queue. The maximum length of the field is 2048 characters.
Retention Period (Days)	Call retention is the number of days to keep recordings in storage. Default: One Year. Use the default with caution since eventually the storage location will be completely consumed. To meet business requirements, it's highly recommended to set the retention value to a positive number. AudioCodes Live SmartTAP deletes calls that exceed the retention period once a day. A network administrator with appropriate security profile credentials has the option to add / modify retention policies. Configure one of the following Retention period time frames: ■ Week (7 Days) ■ Month (30 Days) ■ 3 Months (90 Days) ■ 6 Months (180 Days) ■ 1 year (365 Days) (Default) ■ 2 years (730 Days) ■ Custom

Field	Description
Storage	Azure Blob Storage account location according to region.

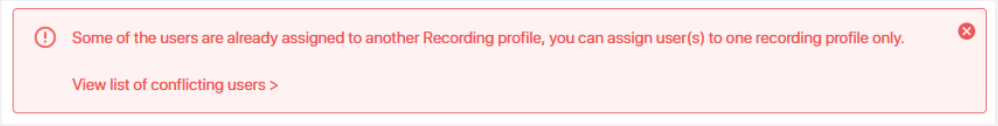
Advanced Settings

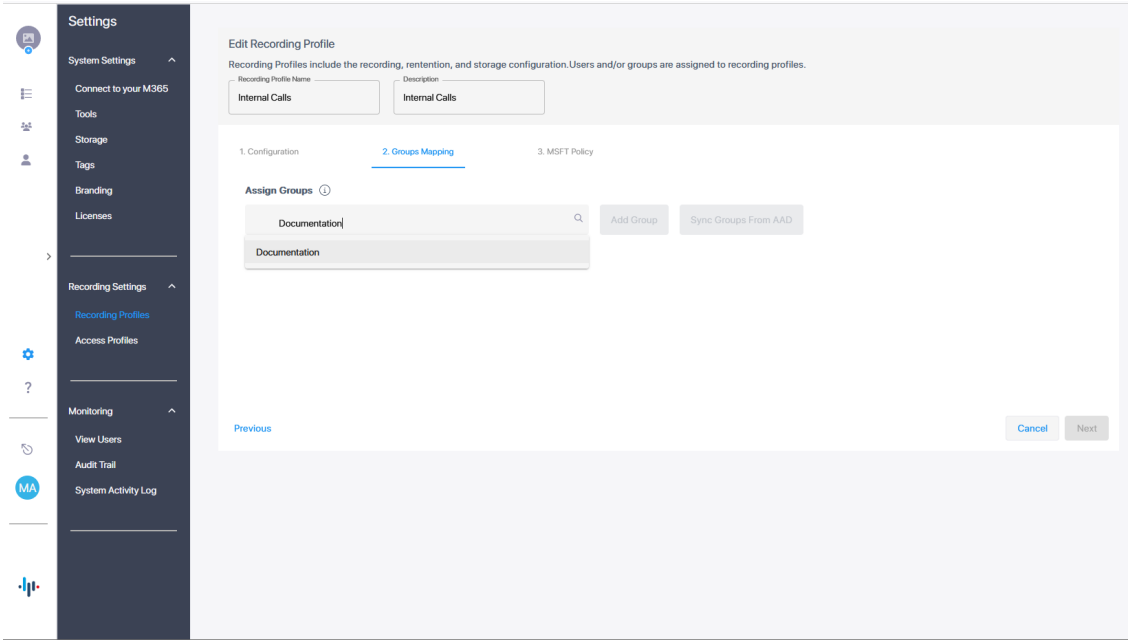
Field	Description
Recording Notification	Controls whether Microsoft Teams banner recording notifications are displayed: ■ **Enable for all calls:** Recording notification are enabled for all calls (Default). ■ **Disable for all calls** Recording notifications are disabled on all calls (visual and audio notifications). ■ **Disable for PSTN calls:** Audio Recording notifications are disabled on PSTN calls. This parameter is only displayed when enabled by the Service Provider in the AudioCodes Live SmartTAP SmartTAP service. In addition, you must sign a waiver to enable this feature.
Filter Calls User Receives Filter Calls User Makes	To filter calls that the user receives or makes, choose the type of the filter. To record the user calls with specific numbers, choose **Allow** in the List Type. To record calls of the user except with specific numbers, choose **Block**: in the List Type. The Filter is applied on the calls with the comma-separated phone numbers defined in the Numbers field. For example: “17326524689, 17326524690” regular expression can be entered when the phone number ranges need to be filtered. For example, to filter calls with phone numbers that starts with area code 732 or 609, enter the following in the regular expression field:^(1{1}|\1{1})?(732|609)\d*$. When both the numbers and regular expressions are provided, the system first checks against the regular expression and if a match is not found, continues with the numbers. The maximum length of the numbers and the regular expression field is 2048 characters. Filtering is applicable to Skype for Business integrations and to Microsoft Teams (PSTN calls only).

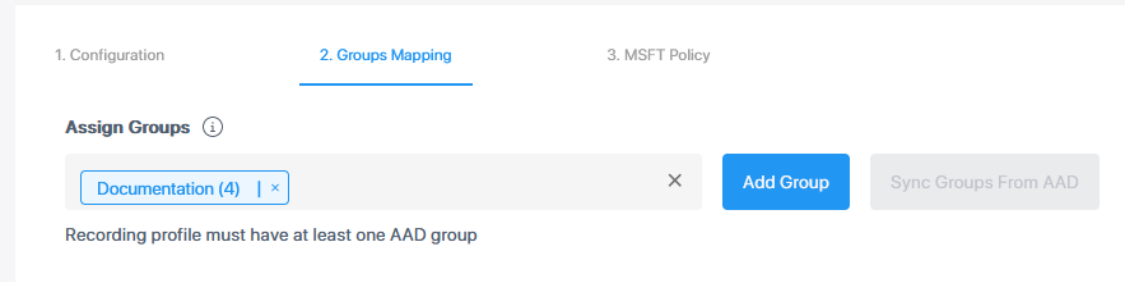
Field	Description
	The **+** sign should **not** be added in **Numbers** and **Regular Expression** fields as its not recognized by AudioCodes Live SmartTAP.
Time Range	Specify a time range for call recording, which includes the option to choose specific days of the week and time ranges based on the location of the server for the (product name) region.
Custom Recording Hours	Custom Recording Hours (default 24/7): ■ Week Days ■ Start Hour ■ End Hour

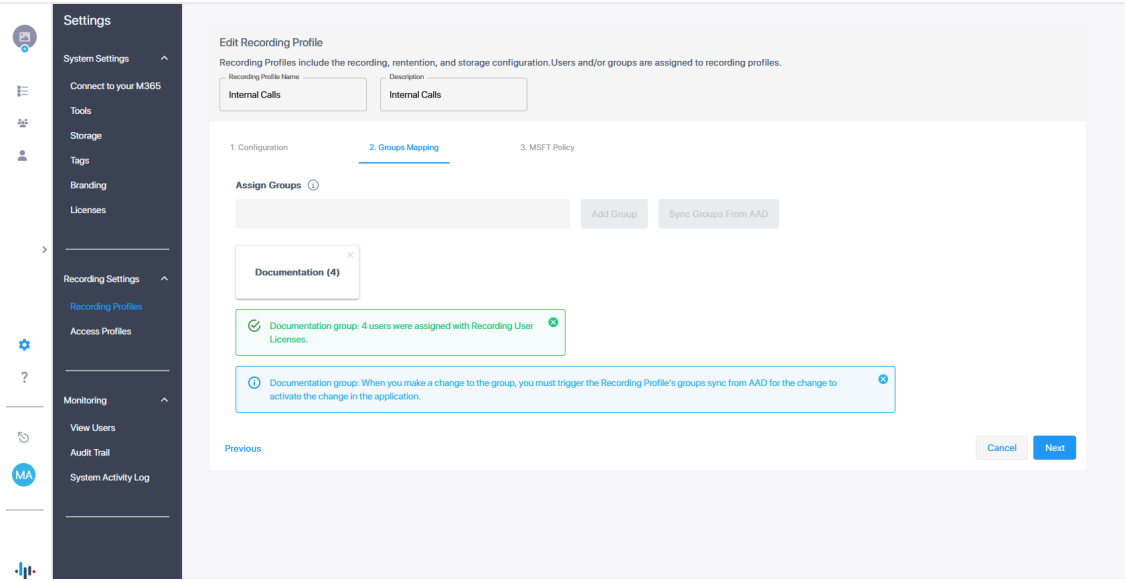
1. Click **Next** to add groups.

Users can only be mapped to one Recording Profile; however, can be assigned to multiple groups that are mapped to the same profile. In this case, the following message is displayed:

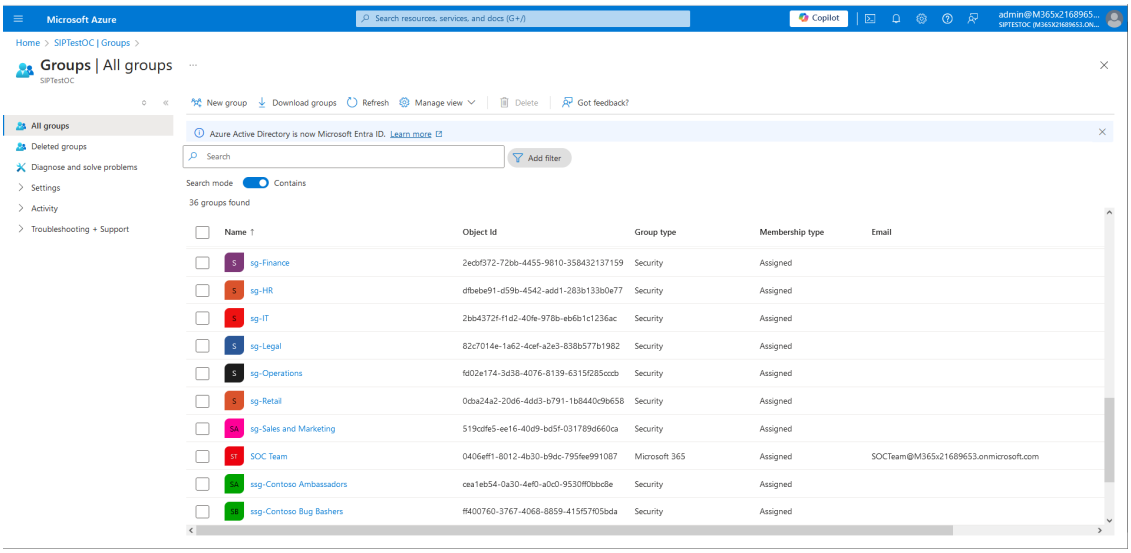




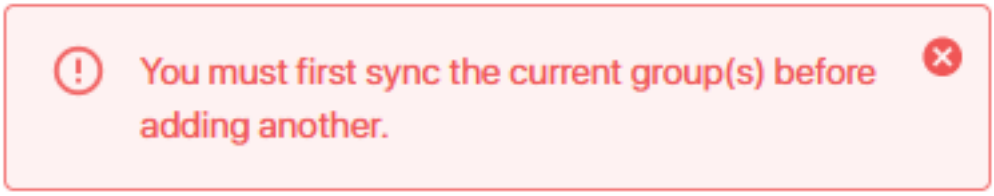




2. Open the Azure portal of your tenant to verify which groups you wish to add.

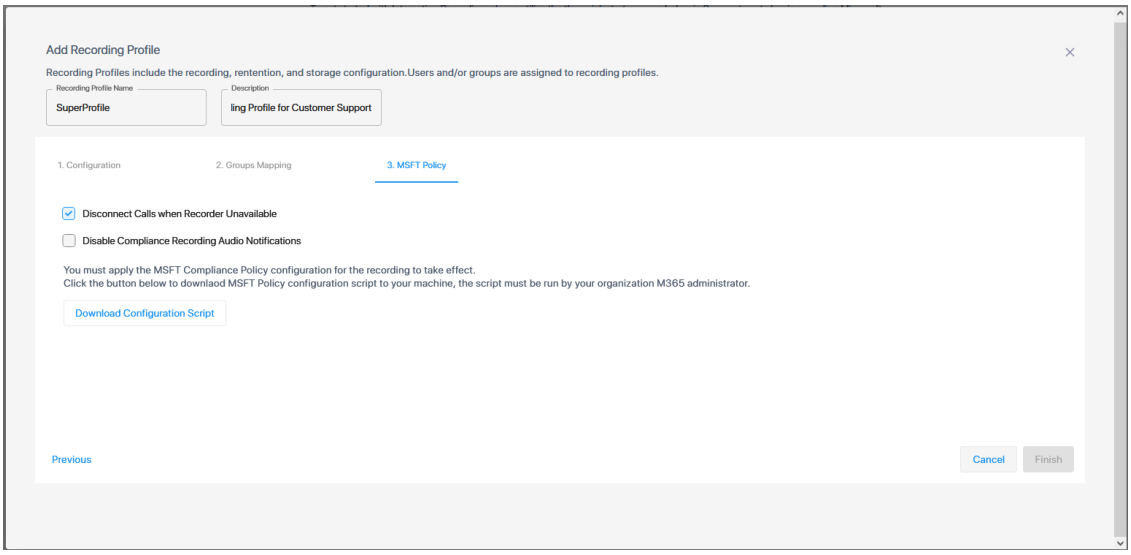


The following message is displayed if you have not yet synced groups with your M365 platform.



3. Perform the Sync; a confirmation message is displayed.

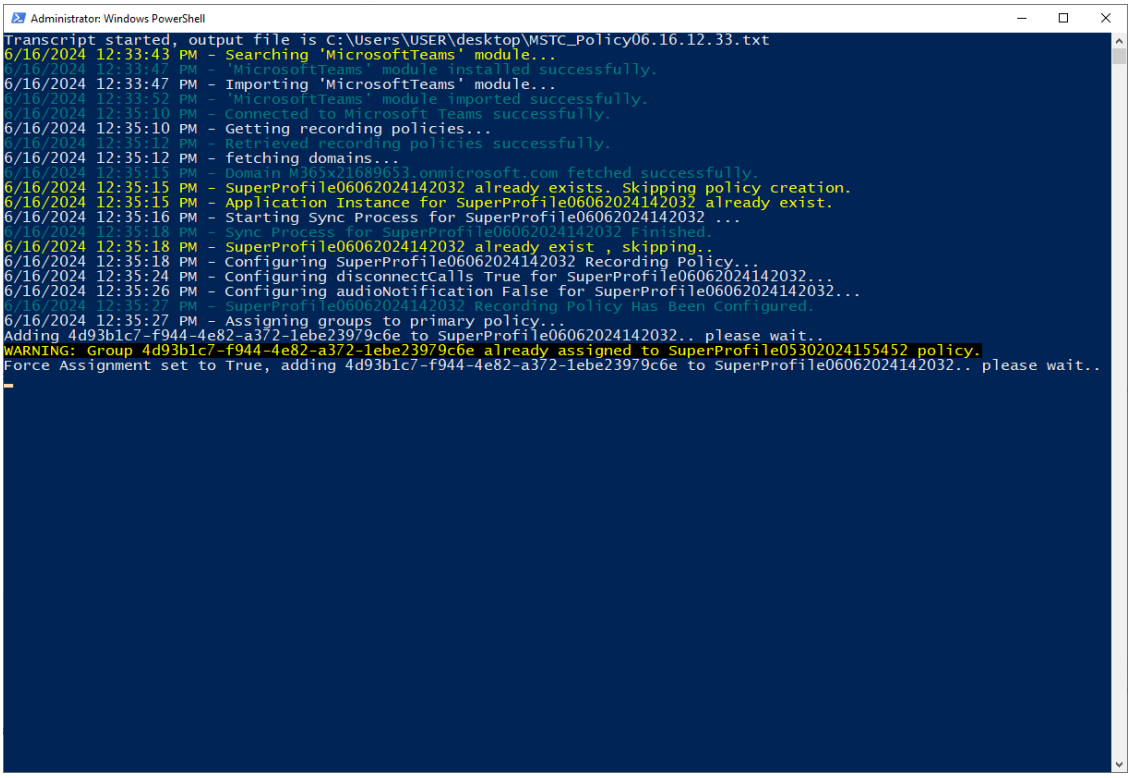
4. Click **Next** to continue.



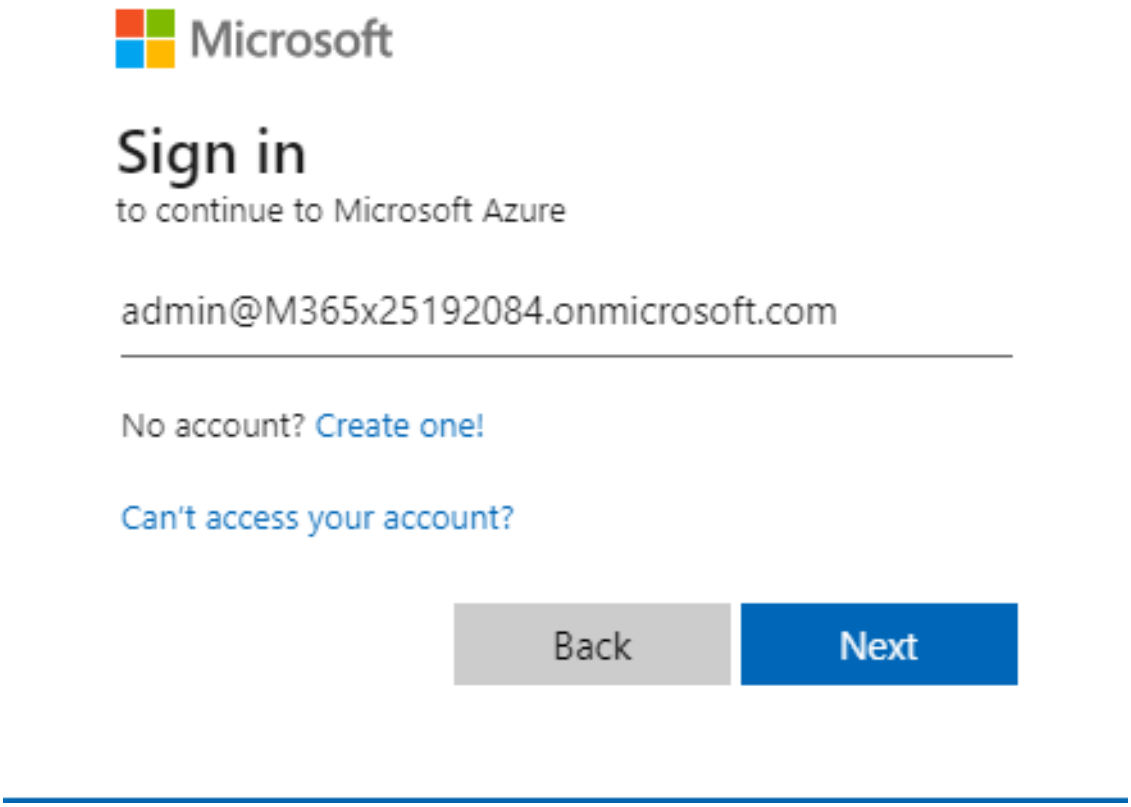
5. Configure the following Microsoft Teams Calling Policies:
   - **Disconnect Calls when Recorder Unavailable:** Calls are disconnected when recording functionality is not available.
   - **Disable Compliance Recording Audio Notifications:** Disable Microsoft Teams Audio Recording notifications that are played to calls participants from PSTN or other UC platforms.
6. Click the **Download Configuration Script** link to download the PowerShell script to your PC.

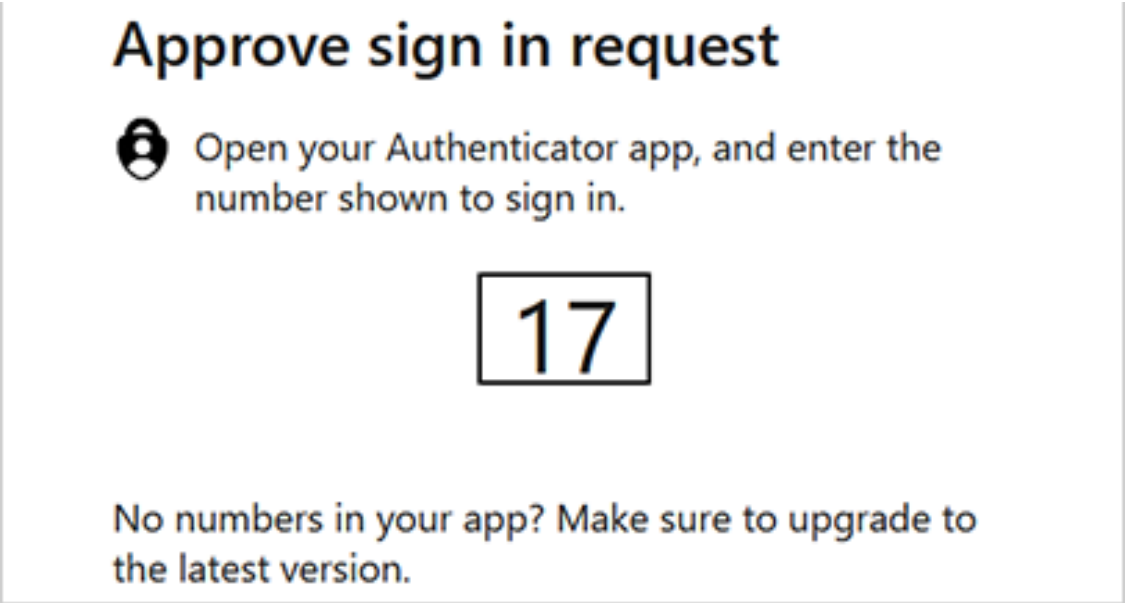
> You can also run the script at a later time using the right-click menu option **MSFT Scripts** (see Download and Run Microsoft Script on page 73).

7. Run the script createProfileSuperProfile-dd-m-yyyy.ps1 as Administrator.

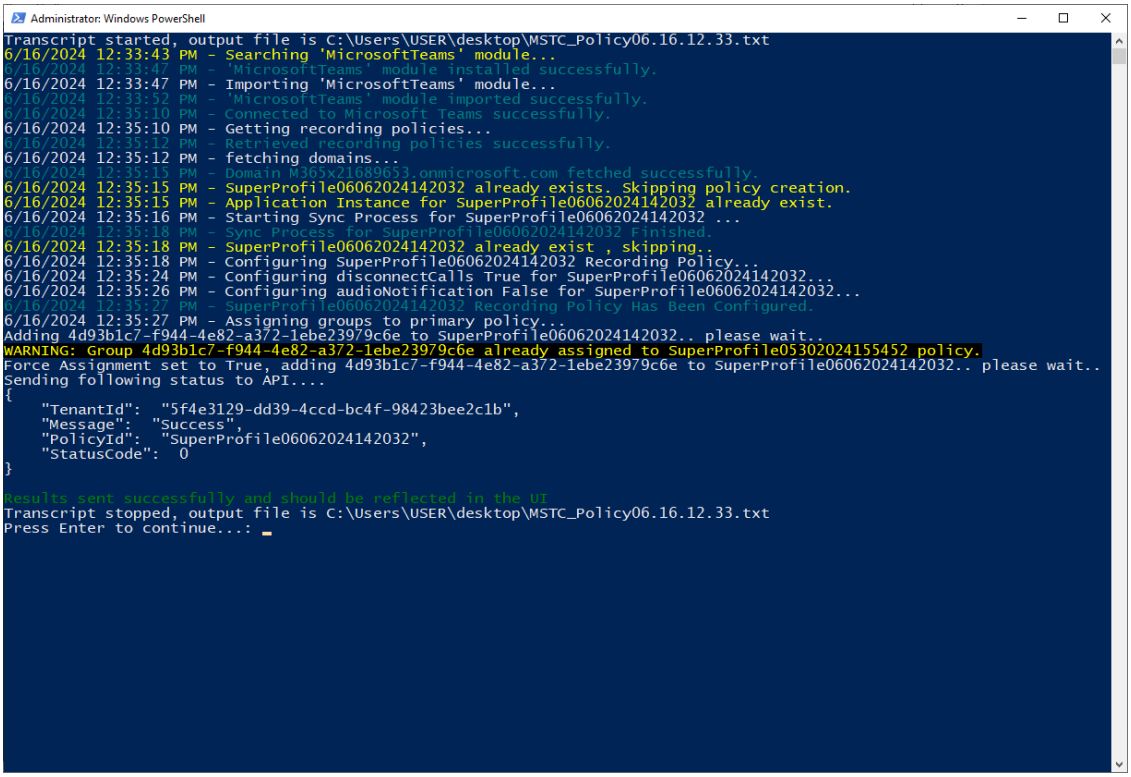


8. Enter the credentials of the Azure customer tenant account and authenticate using the Microsoft Authenticator when prompted.





The script supports Multifactor authentication.



See example log file below (saved to Desktop on the PC where you run the script).

```
**********************
```

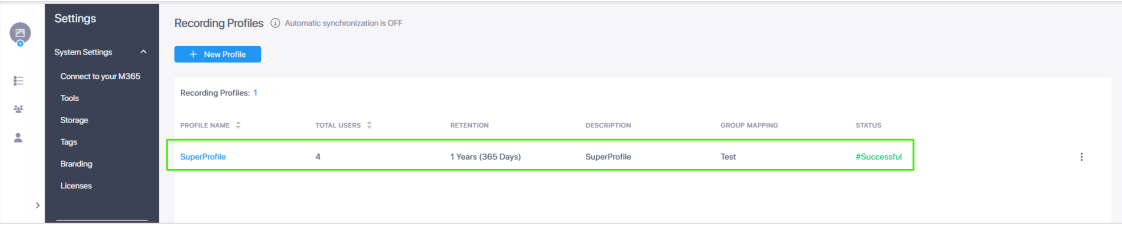
```
Windows PowerShell transcript start

Start time: 20240616123342

Username: LAPTOP-M8LNK8BQ\USER

RunAs User: LAPTOP-M8LNK8BQ\USER

Configuration Name:

Machine: LAPTOP-M8LNK8BQ (Microsoft Windows NT 10.0.19045.0)

Host Application: C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe
-NoProfile -ExecutionPolicy Bypass -File
C:\Users\USER\Desktop\Powershell\editProfileSuperProfile-16-6-2024.ps1

Process ID: 19148

PSVersion: 5.1.19041.4522

PSEdition: Desktop

PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.19041.4522

BuildVersion: 10.0.19041.4522

CLRVersion: 4.0.30319.42000

WSManStackVersion: 3.0

PSRemotingProtocolVersion: 2.3

SerializationVersion: 1.1.0.1

**********************

Transcript started, output file is C:\Users\USER\desktop\MSTC_
Policy06.16.12.33.txt

PS>TerminatingError(Invoke-RestMethod): "
{"type":"https://tools.ietf.org/html/rfc7231#section-
```

```
6.5.13","title":"Unsupported Media Type","status":415,"traceId":"00-
1fa6a9561e39115c5b5258f162c5540d-a5c8015bfcd9c025-00"}"

6/16/2024 12:33:43 PM - Searching 'MicrosoftTeams' module...

6/16/2024 12:33:47 PM - 'MicrosoftTeams' module installed successfully.

6/16/2024 12:33:47 PM - Importing 'MicrosoftTeams' module...

INFO: Loaded Module 'Microsoft.Teams.ConfigAPI.Cmdlets'

6/16/2024 12:33:52 PM - 'MicrosoftTeams' module imported successfully.

6/16/2024 12:35:10 PM - Connected to Microsoft Teams successfully.

6/16/2024 12:35:10 PM - Getting recording policies...

6/16/2024 12:35:12 PM - Retrieved recording policies successfully.

6/16/2024 12:35:12 PM - fetching domains...

6/16/2024 12:35:15 PM - Domain M365x21689653.onmicrosoft.com fetched
successfully.

6/16/2024 12:35:15 PM - SuperProfile06062024142032 already exists. Skipping
policy creation.

6/16/2024 12:35:15 PM - Application Instance for SuperProfile06062024142032
already exist.

6/16/2024 12:35:16 PM - Starting Sync Process for SuperProfile06062024142032
...

6/16/2024 12:35:18 PM - Sync Process for SuperProfile06062024142032
Finished.

6/16/2024 12:35:18 PM - SuperProfile06062024142032 already exist ,
skipping..

6/16/2024 12:35:18 PM - Configuring SuperProfile06062024142032 Recording
Policy...
```

```
6/16/2024 12:35:24 PM - Configuring disconnectCalls True for
SuperProfile06062024142032...

6/16/2024 12:35:26 PM - Configuring audioNotification False for
SuperProfile06062024142032...

6/16/2024 12:35:27 PM - SuperProfile06062024142032 Recording Policy Has Been
Configured.

6/16/2024 12:35:27 PM - Assigning groups to primary policy...

Adding 4d93b1c7-f944-4e82-a372-1ebe23979c6e to SuperProfile06062024142032..
please wait..

WARNING: Group 4d93b1c7-f944-4e82-a372-1ebe23979c6e already assigned to
SuperProfile05302024155452 policy.

Force Assignment set to True, adding 4d93b1c7-f944-4e82-a372-1ebe23979c6e to
SuperProfile06062024142032.. please wait..

Sending following status to API....

{

    "TenantId":  "5f4e3129-dd39-4ccd-bc4f-98423bee2c1b",

    "Message":  "Success",

    "PolicyId":  "SuperProfile06062024142032",

    "StatusCode":  0

}



Results sent successfully and should be reflected in the UI

**********************

Windows PowerShell transcript end
```

```
End time: 20240616123533

**********
```

9. Once you have successfully run the script, verify that the Recording Profile status is 'Successful'.



Retrieving Recording Queue Instances

Configuration of Teams call queues recordings (Transfer mode) in the recording profile requires the retrieval of the application instance of each call queue that is designated for recording. Each call queue is represented by a single Application Instance ID.

➢ To retrieve call queue application instances using PowerShell:

1. Enter the following PS command:

```
PS C:\Users\Admin> Get-CsCallQueue

WARNING:  All the agents added to callqueue have opted out. There are no
agents to call.

TenantId                                        : ad41d6c3-67f0-47cc-9de3-
e07fd185c1c7

Name                                            : CallQueue1

Identity                                        : 361635e9-1159-43be-bdc2-
62efe4db5c16

RoutingMethod                                   : Attendant
```

```
DistributionLists                                :
Users                                            : 9f7309ea-a318-4ac5-92a0-
2f4134736e42
DistributionListsLastExpanded                    : 11/21/2021 08:12:49 +00:00
Agents                                           : 9f7309ea-a318-4ac5-92a0-
2f4134736e42, OptOut
AllowOptOut                                      : True
ConferenceMode                                   : False
PresenceBasedRouting                             : True
AgentsCapped                                     : False
AgentsInSyncWithDistributionLists                : True
AgentAlertTime                                   : 60
LanguageId                                       : en-US
OverflowThreshold                                : 200
OverflowAction                                   : DisconnectWithBusy
OverflowActionTarget                             :
OverflowSharedVoicemailTextToSpeechPrompt        :
OverflowSharedVoicemailAudioFilePrompt           :
OverflowSharedVoicemailAudioFilePromptFileName   :
EnableOverflowSharedVoicemailTranscription       : False
TimeoutThreshold                                 : 1200
```

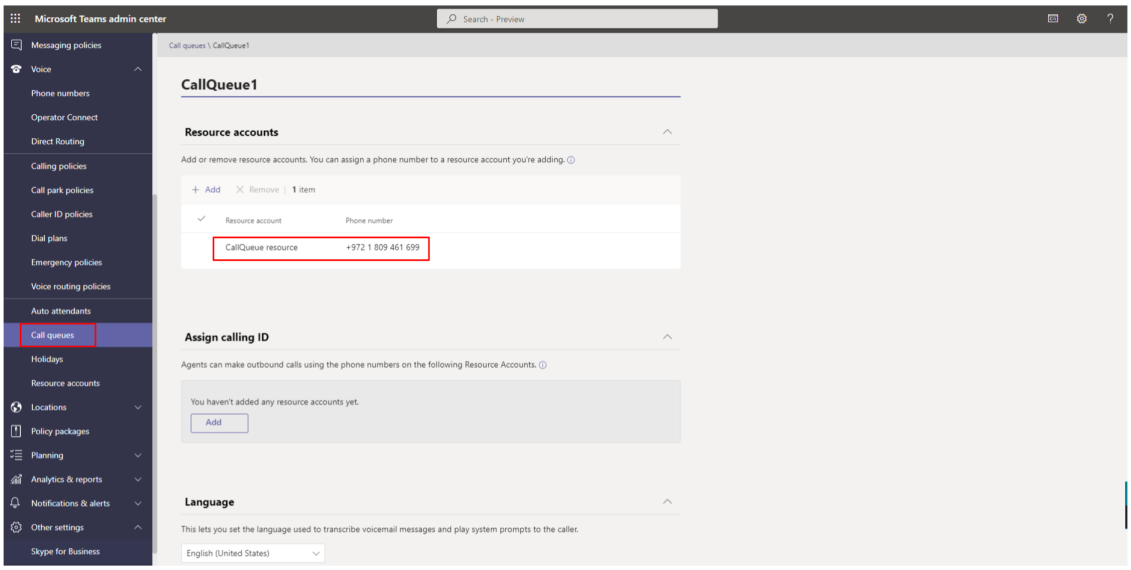
```
TimeoutAction                                : Disconnect
TimeoutActionTarget                          :
TimeoutSharedVoicemailTextToSpeechPrompt     :
TimeoutSharedVoicemailAudioFilePrompt        :
TimeoutSharedVoicemailAudioFilePromptFileName :
EnableTimeoutSharedVoicemailTranscription    : False
WelcomeMusicFileName                         : caal_queue_greeting.mp3
UseDefaultMusicOnHold                        : True
MusicOnHoldFileName                          :
Statistics                                   : Current queue size = 0
ApplicationInstances                         : f17e8e19-1669-4a4c-bf13-
e9e31420edaf
ChannelId                                    :
OboResourceAccounts                          :
```

2. Copy the Application Instance to notepad.

➢ **To retrieve call queue application instances using Teams Administration:**

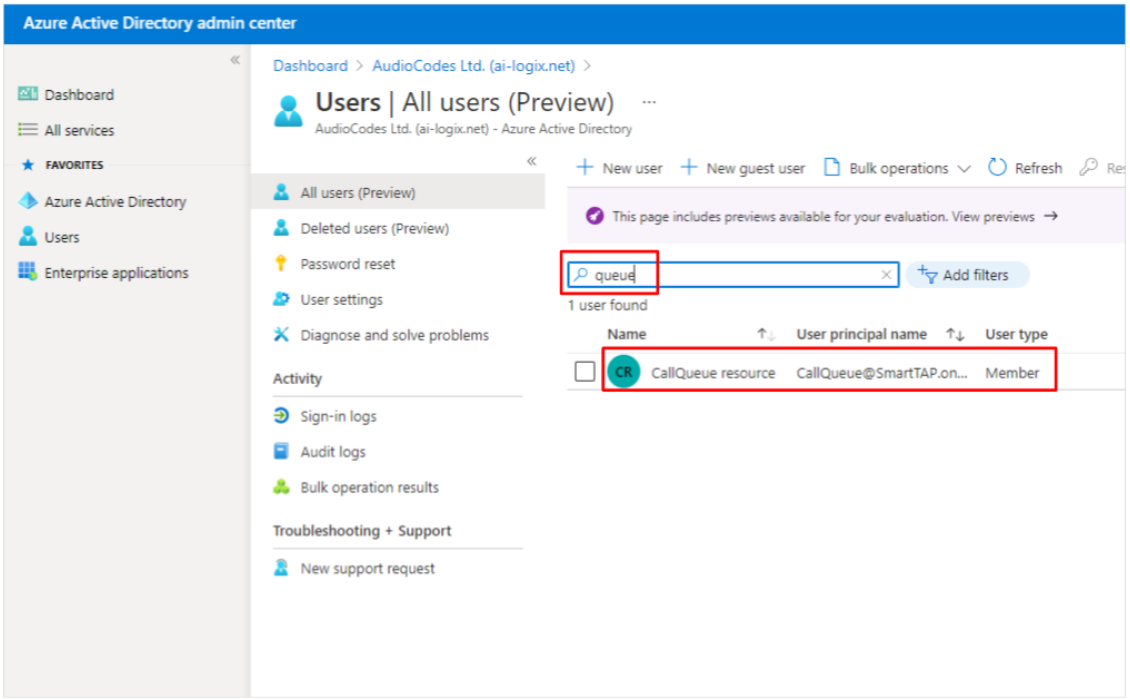
1. Open the Teams Administration portal.
2. Select the Queue.
3. Find Resource details.

Figure 4-1: Call Queues



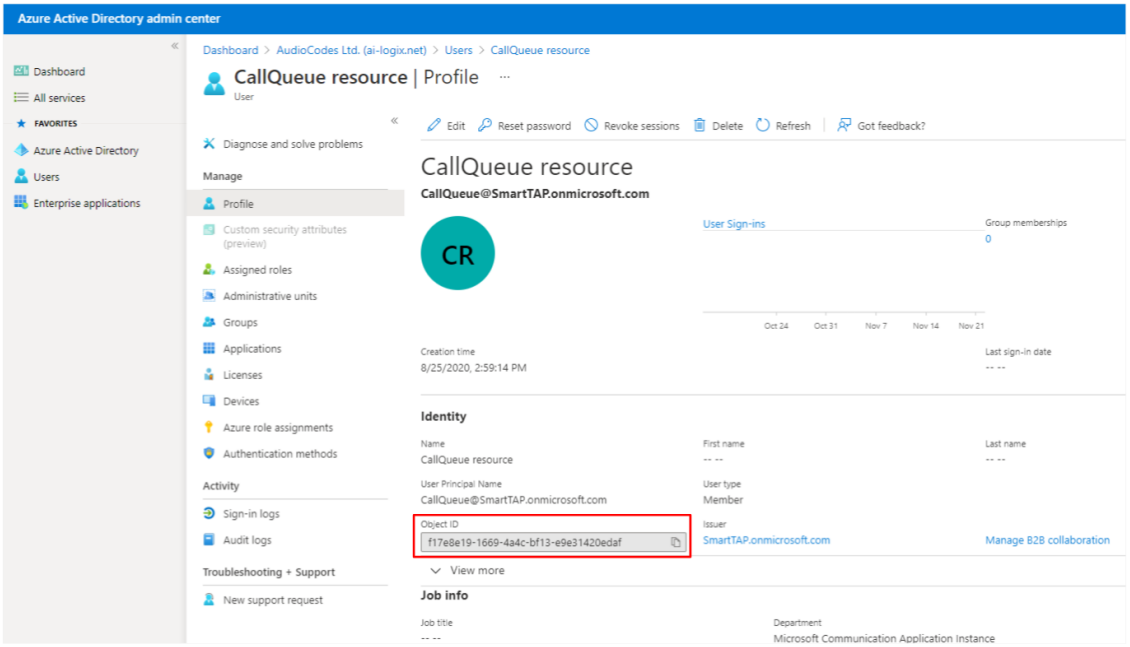
4. In the Azure Active directory find the queue Resource.

Figure 4-2: Resources



5. Copy the Object ID (application instance) to notepad.

Figure 4-3: Call Queue Resource



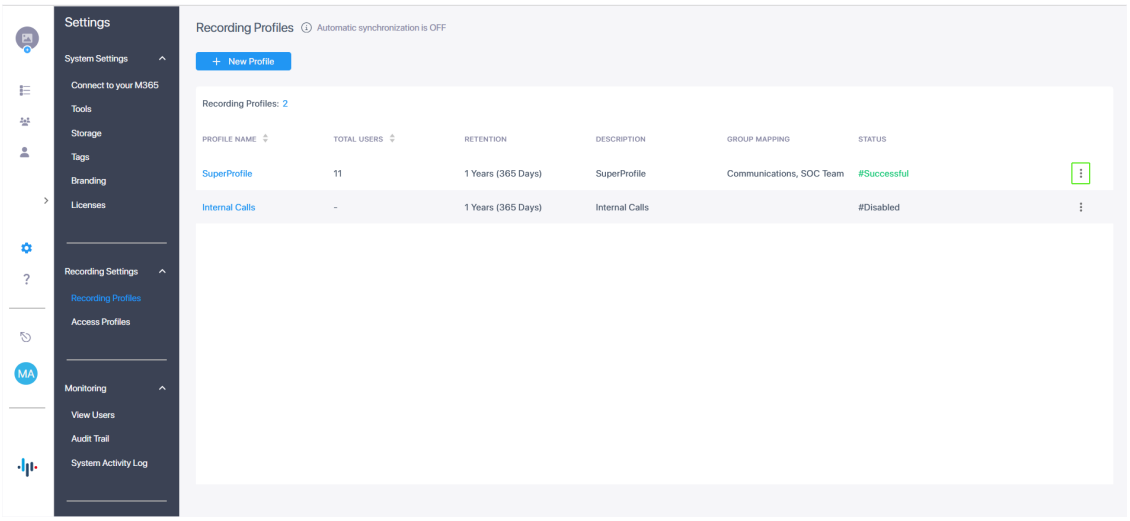
Modifying Recording Profiles

This option lets you modify existing recording profiles. For example, you may add a new site location and wish to associate the new user groups for this location to a recording profile and to configure the Blob storage location.

> Whenever you update Group Mapping and MSFT Policy, you must download and run the Microsoft Configuration script to synchronize with your M365 tenant platform (see Download and Run Microsoft Script on page 73).

➢ Do the following:

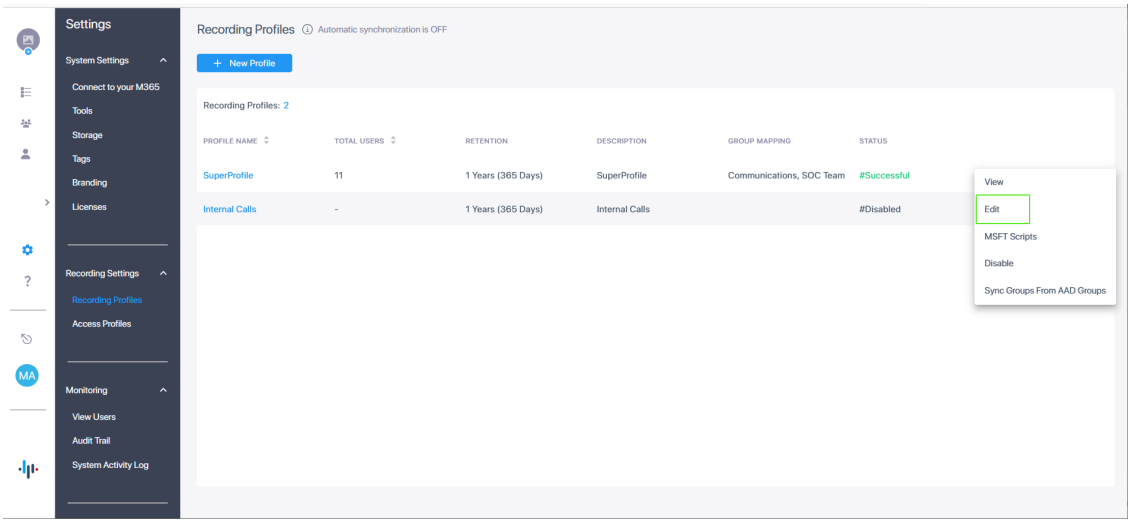
1. In the Icon pane, click , and then in the Navigation pane, select **Recording Settings** > **Recording Profiles**.

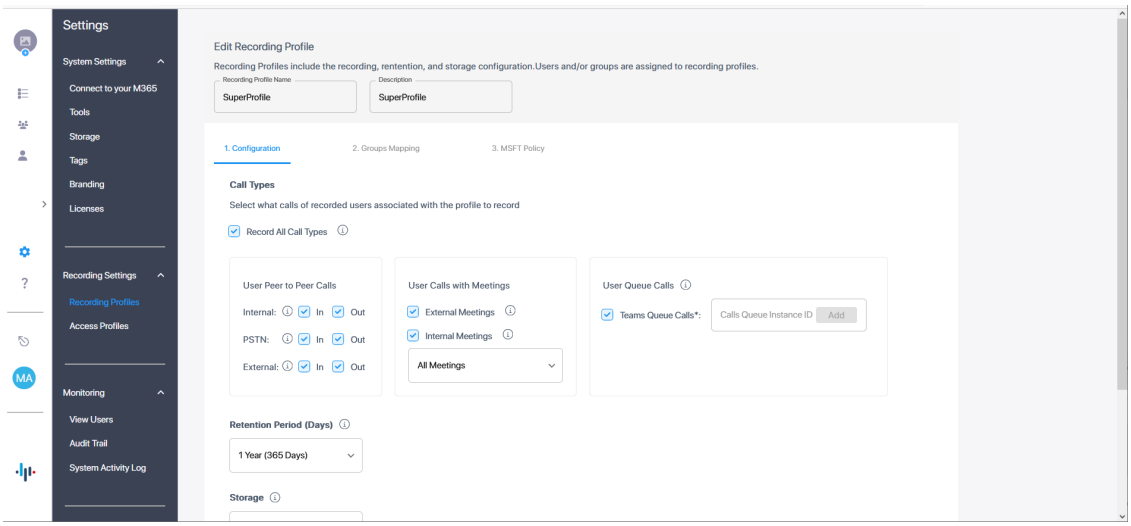


2. The following table describes the parameters in this screen.

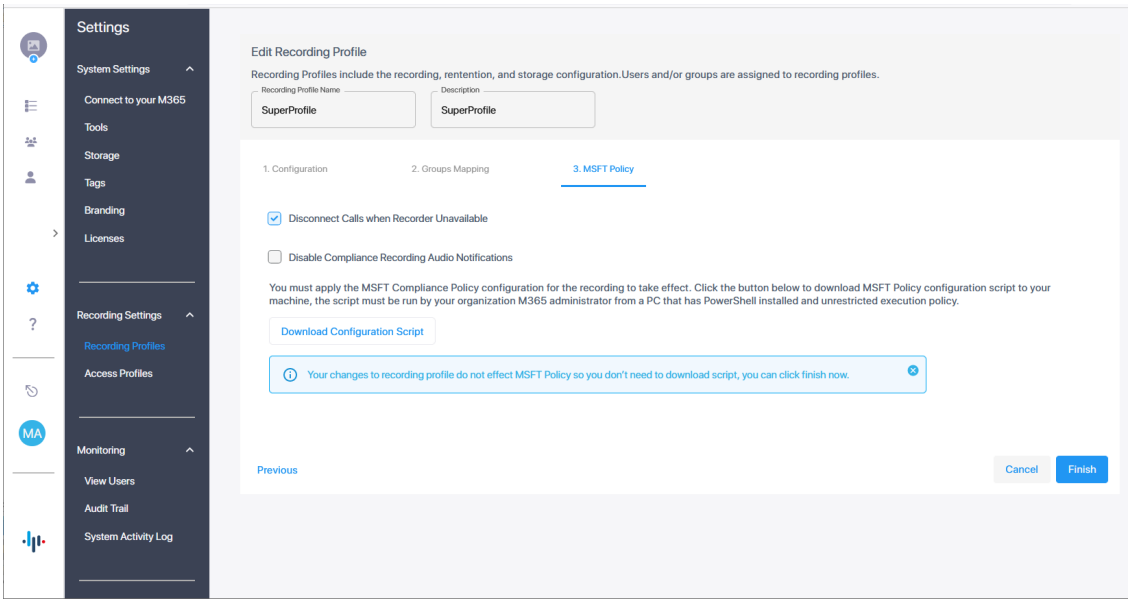
Parameter	Description
Profile Name	The name of the profile.
Total Users	The total number of licensed users according to the number of users attached to Recording profiles.
Retention	The Retention period according to the configuration in the Recording Profile.
Description	Brief description of the Recording profile.
Group Mapping	Indicates the names of the AAD groups that are mapped to the Recording profile.
Statuses	
#Not In Sync With AAD Groups	AAD Groups are not synchronized with your M365 platform due to one of the following: ■ Members have been added or removed from AAD groups on customer M365 platform. ■ AAD Groups have been added or removed from Recording Profile. See Synchronizing AAD Groups with M365 Tenant Platform
#Pending MSFT Policy Execution	Indicates that changes have been made to a Recording profile and as a result, the Microsoft script must be downloaded and run into to apply the changes to synchronize with your M365 platform.
#Disabled	Indicates that the profile has been disabled. See
#Successful	Indicates that the Recording Profile has been successfully synchronized with your M365 platform.
Error	Indicates that the Recording Profile has an error.

3. Click the dots adjacent to the profile that you wish to edit (see above), and then from the drop-down list, choose **Edit** (see below).





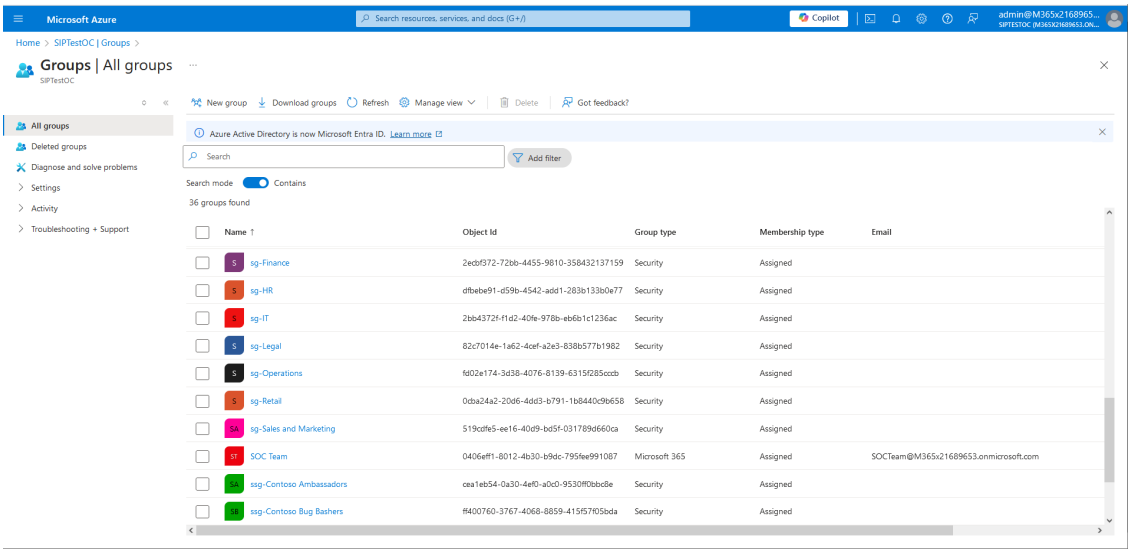
If you only update 1. Configuration and not Group Mapping and MSFT Policy, then you do not need to download and run the Microsoft Configuration screen as shown in the Figure below.

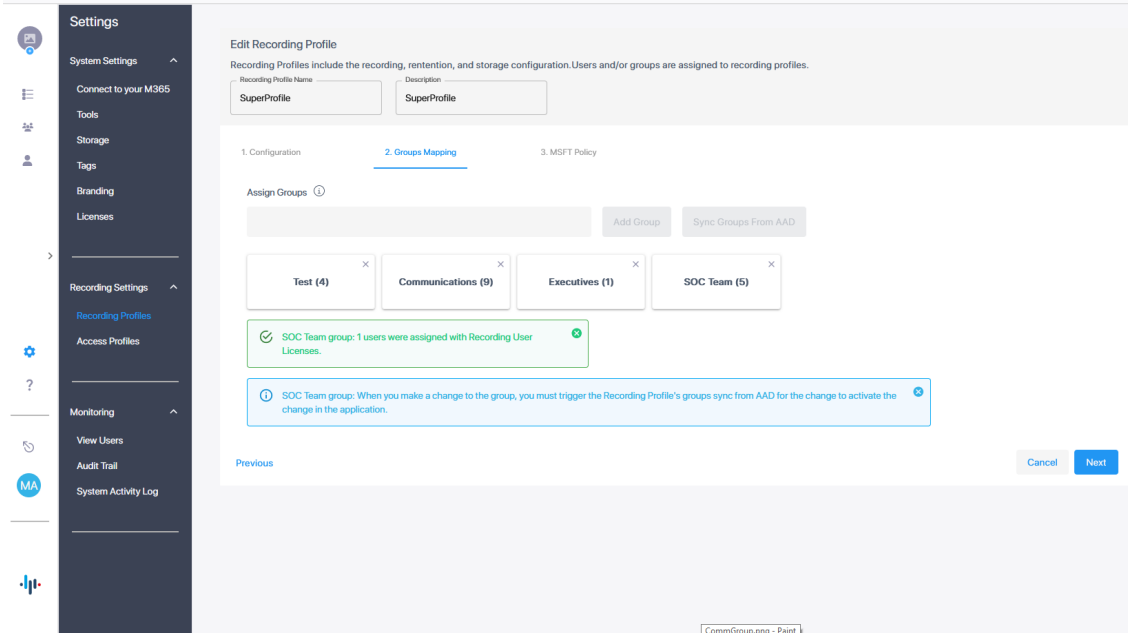


4. Configure fields according to the table in Adding Recording Profiles on page 48.
5. Click **Next** to configure additional groups.

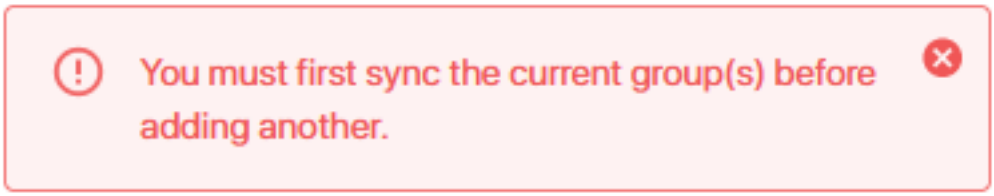
- Users can only be mapped to one Recording Profile and belong to one mapped group.
- At least one group must exist in the Recording Profile.

6. Add additional groups as required (login to your Azure portal to verify the groups and their respective members).
7. Open the Azure portal of your customer tenant to verify which groups you wish to add.



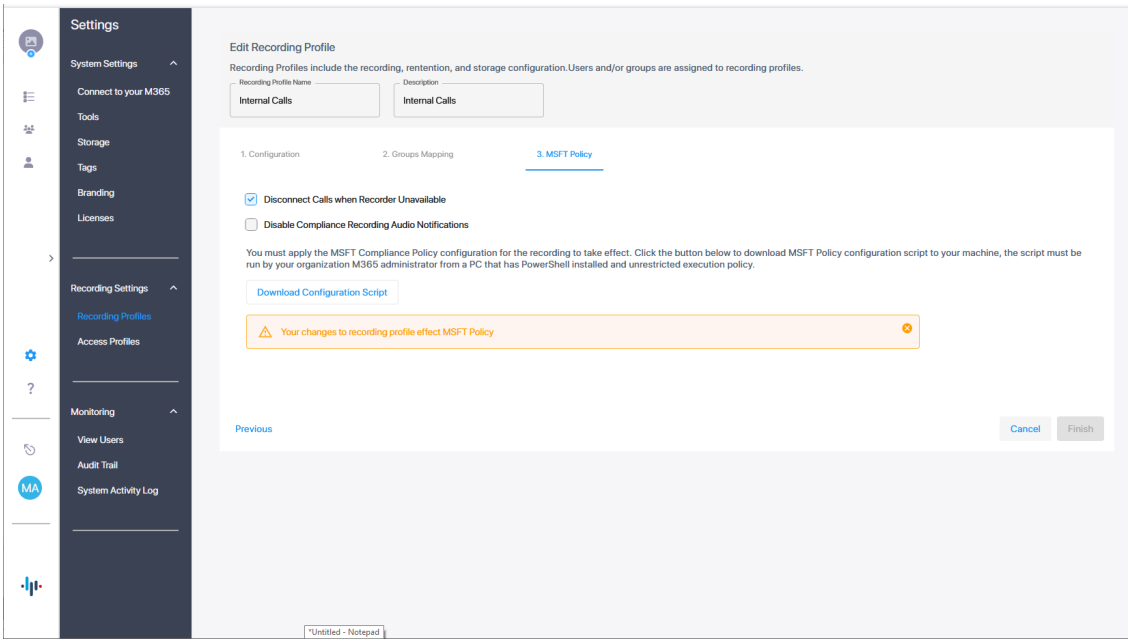


The following message is displayed if you have not yet synced groups with your M365 platform.



8. Perform the Sync; a confirmation message is displayed.

9. Click **Next** to continue.



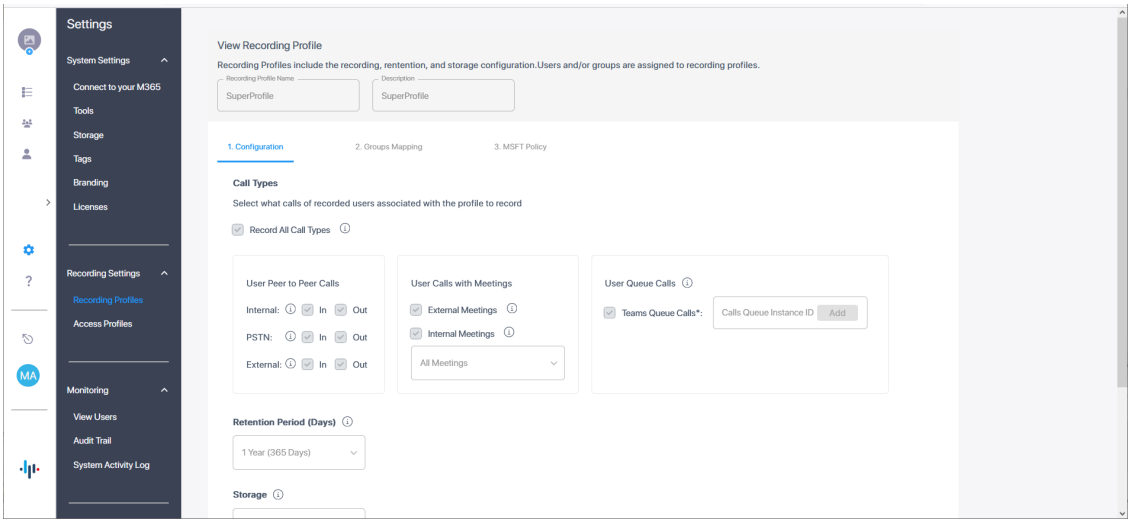
10. Configure the following Microsoft Teams Calling Policies:
    - Disconnect Calls when Recorder Unavailable: Calls are disconnected when recording functionality is not available.
    - Disable Compliance Recording Audio Notifications: Disable Microsoft Teams Recording notifications.
11. Click **Download Configuration Script** to download the script (see Downloading Microsoft PowerShell Script)

Viewing Recording Profiles

You can view the settings for an existing Recording profile.

➢ To view a recording profile:

1. In the Icon pane, click , and then in the Navigation pane, select **Recording Settings** > **Recording Profiles**.

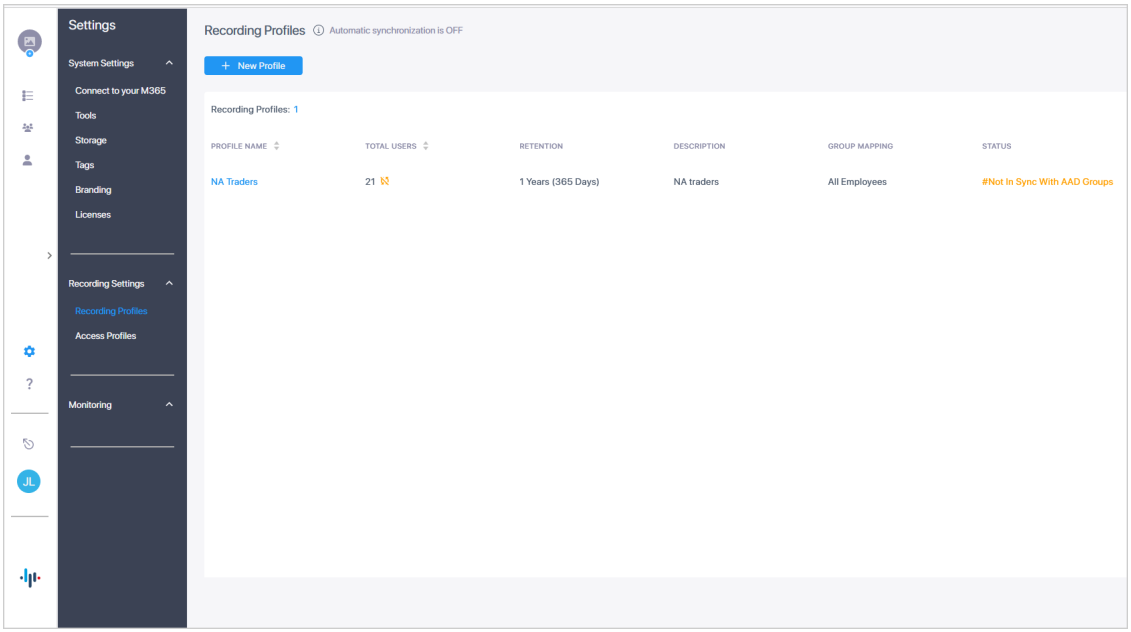


Synchronizing Recording Profiles

This option lets you synchronize your recording profiles with your M365 platform. You must perform this action each time you update AAD groups on your M365 tenant.

➢ Do the following:

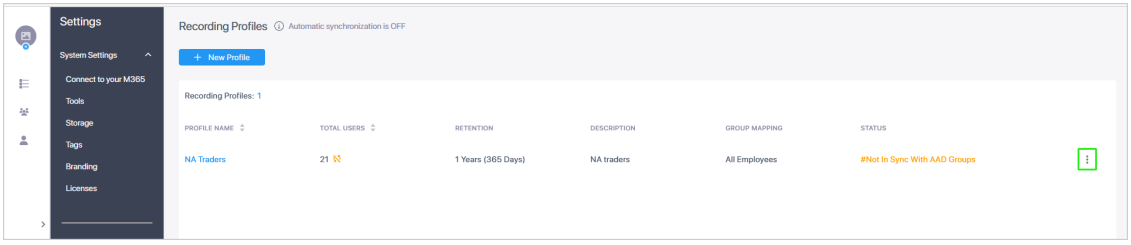
1. In the Icon pane, click , and then in the Navigation pane, select **Recording Settings** > **Recording Profiles**.

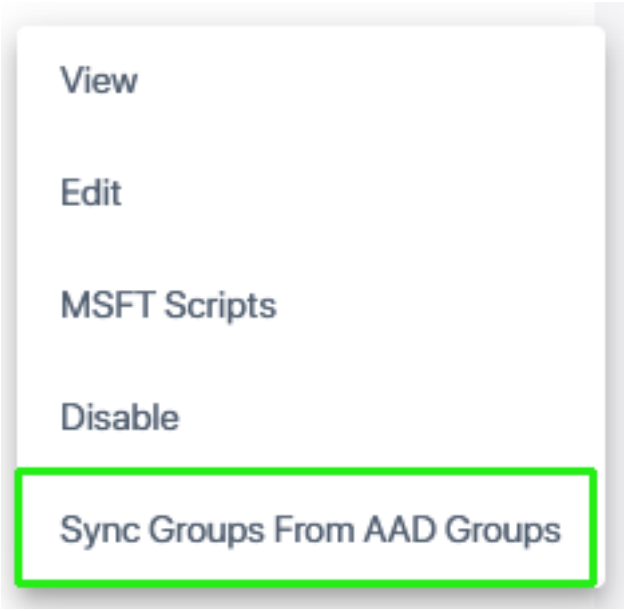


2. The following status is displayed when the Recording profile status is not synchronized.

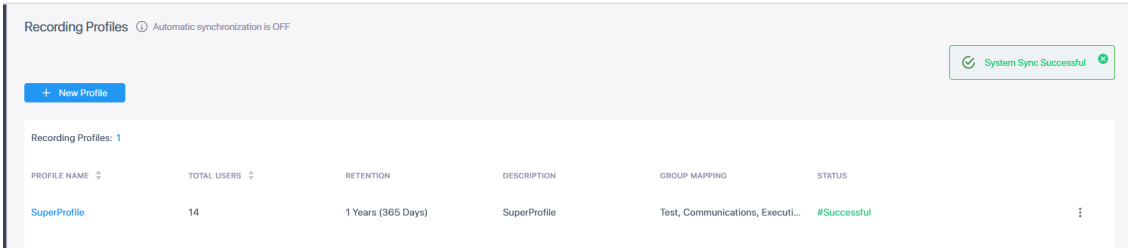
#Not In Sync With AAD Groups

3. Select the profile you wish to sync, click the right-click menu link, and then choose **Sync Groups From AAD Groups**.





A confirmation message is displayed when the Sync operations has completed successfully.



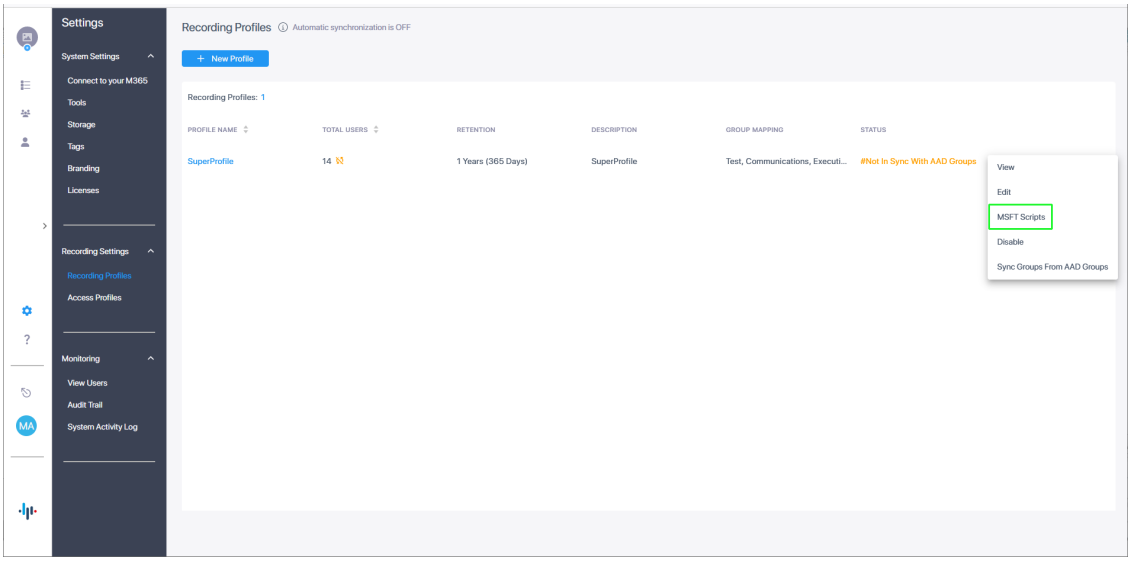
Download and Run Microsoft Script

The Microsoft Script must be run in Day Two whenever you update Group Mapping to Recording Profiles (adding or removing members on Azure Portal in AAD group or adding or removing groups in AudioCodes Live SmartTAP profile) and whenever you change MSFT Policy. This script synchronizes with your M365 platform.

> If you have already downloaded the script in Modifying Recording Profiles on page 66 proceed to Step 5 below.

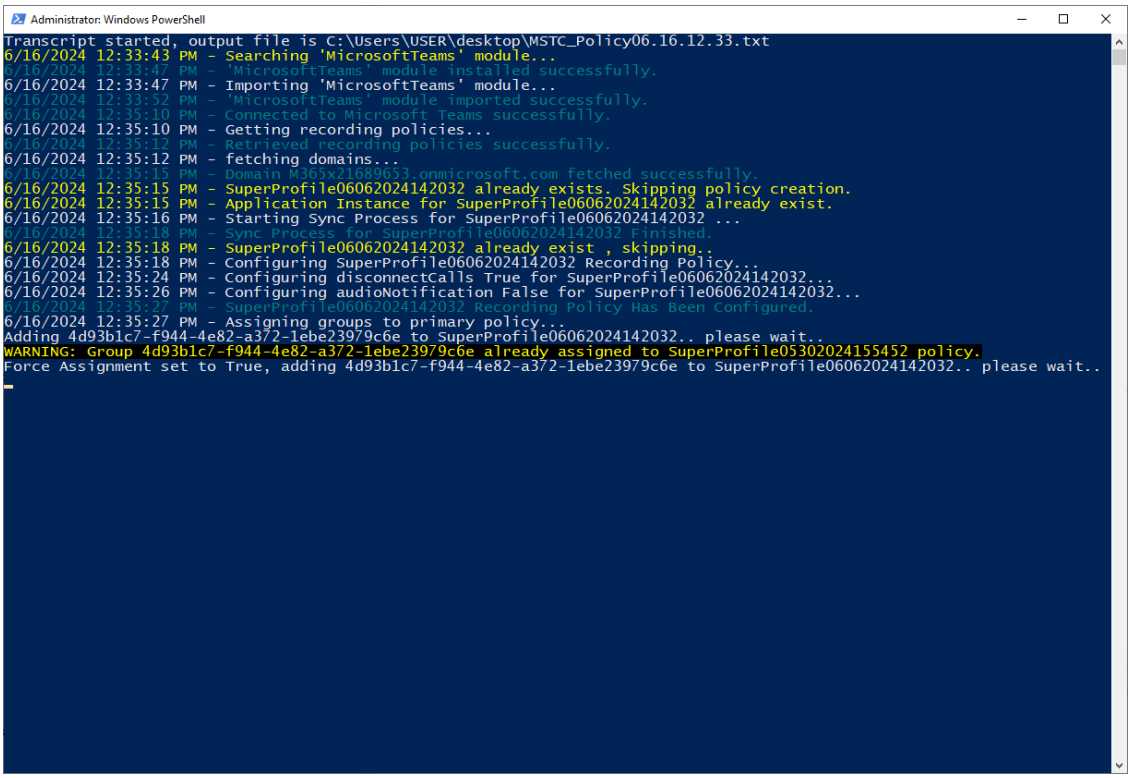
➢ Do the following:

1. In the Icon pane, click , and then in the Navigation pane, select **Recording Settings** > **Recording Profiles**.

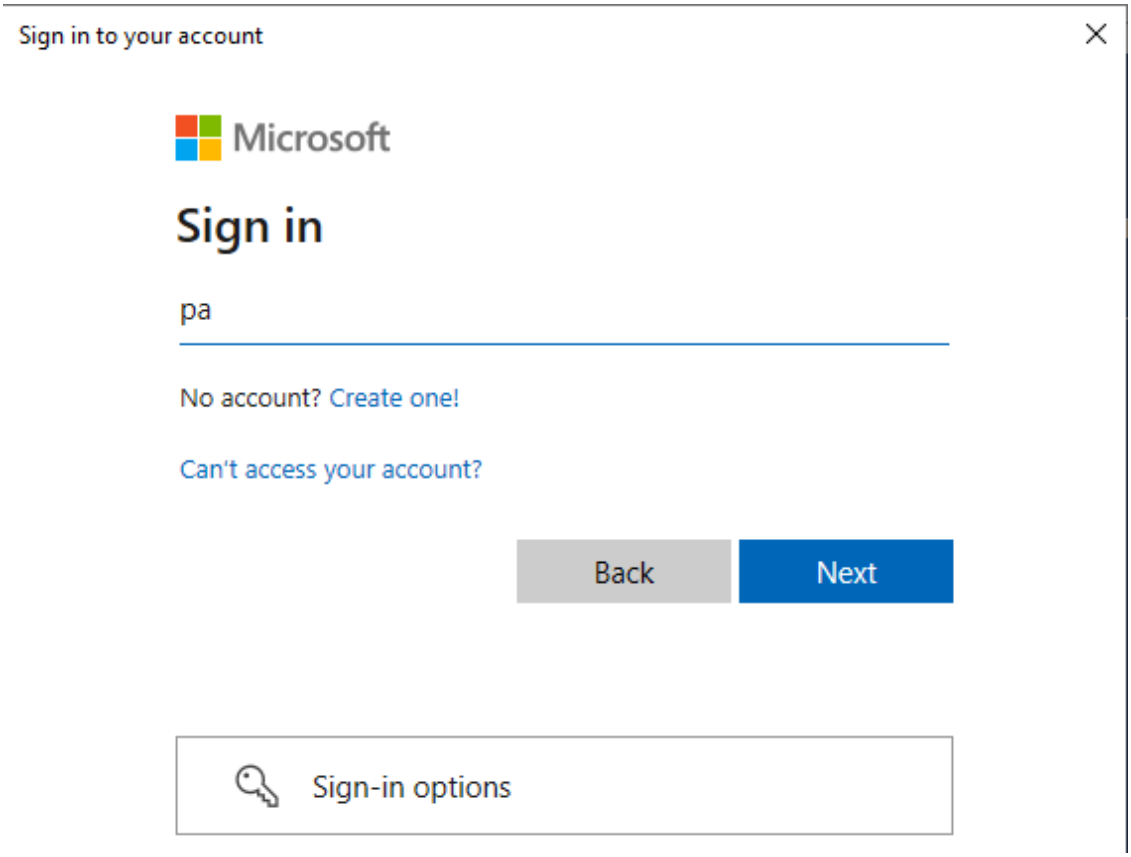


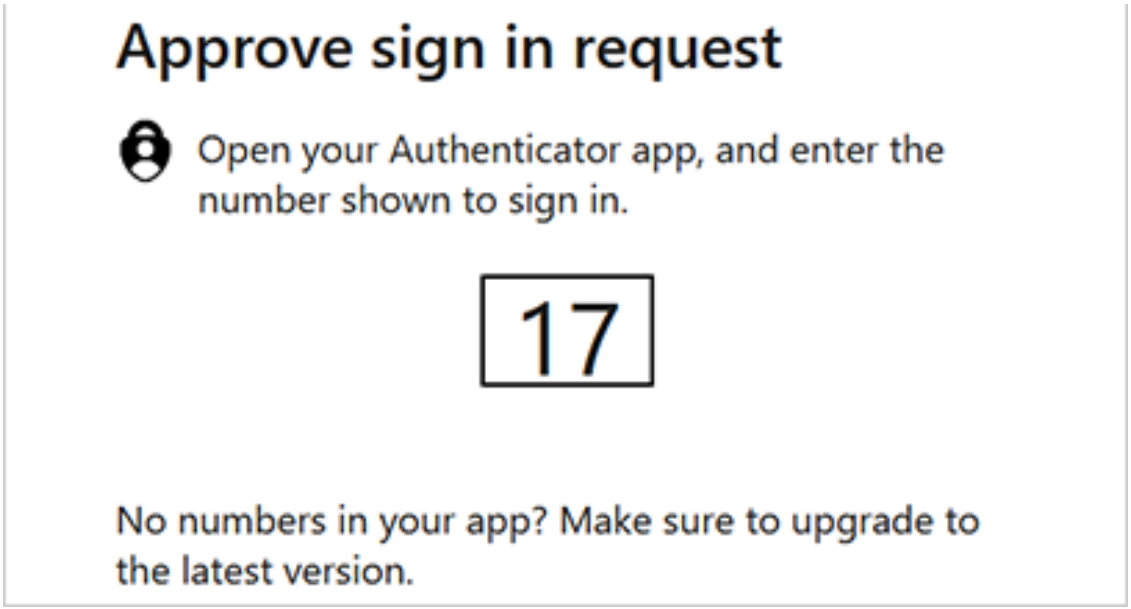
2. Select the Recording Profile whose script you wish to download, click the right-click menu link, and then choose **MSFT Scripts**.

3. Click the Download button to download the script or the copy button to copy the script to clipboard.
4. Click the **Download Configuration Script** link to download the PowerShell script to your PC.
5. Run the script createProfileSuperProfile-dd-m-yyyy.ps1 as Administrator.



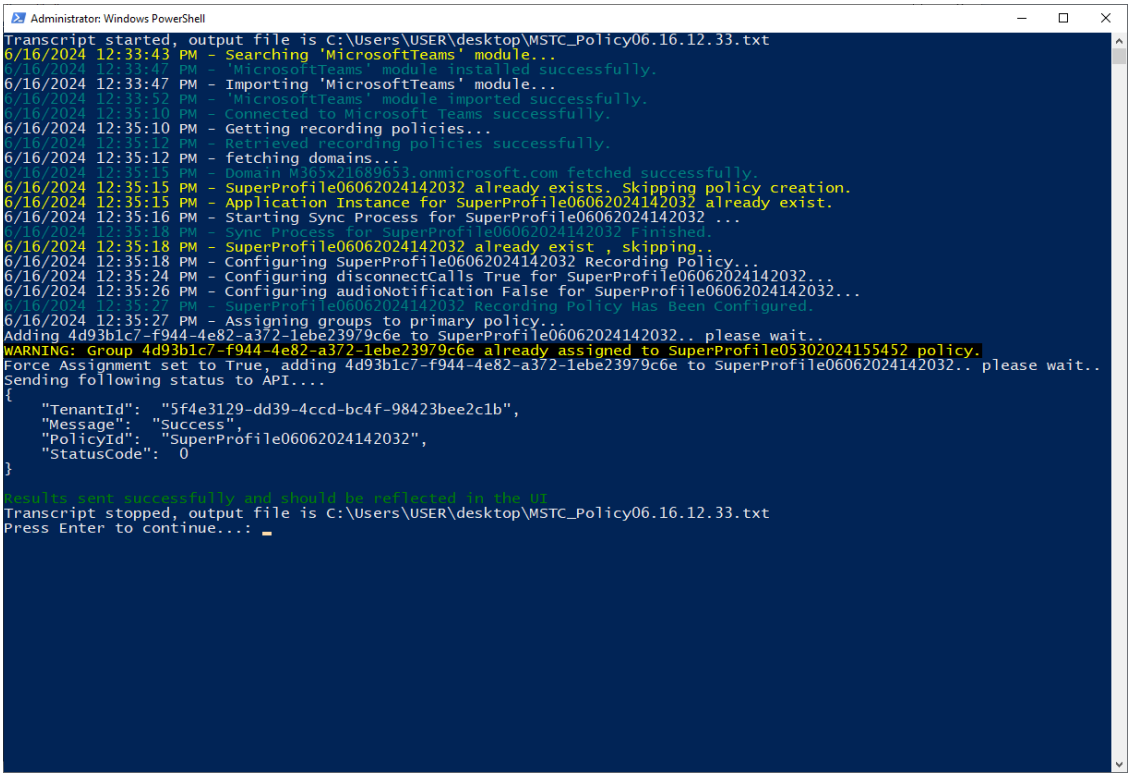
6. Enter the credentials of the Azure customer tenant account and authenticate using the Microsoft Authenticator when prompted.





The script supports Multifactor authentication.

Notice that the Recording Profile has already been created, therefore the script updates the existing policy.



See example log file below (saved to Desktop on PC where the script is run).

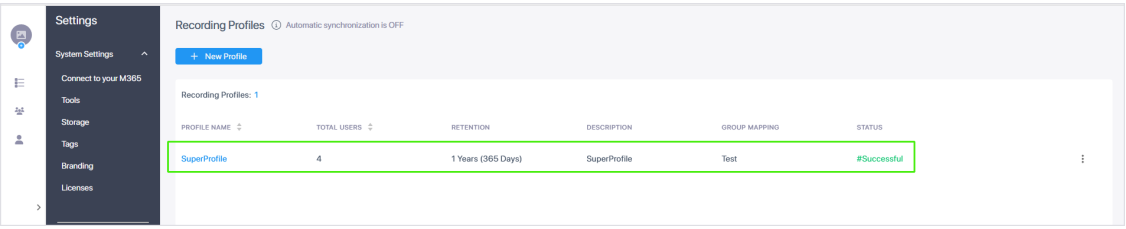
```
**********************

Windows PowerShell transcript start

Start time: 20240616123342

Username: LAPTOP-M8LNK8BQ\USER

RunAs User: LAPTOP-M8LNK8BQ\USER

Configuration Name:

Machine: LAPTOP-M8LNK8BQ (Microsoft Windows NT 10.0.19045.0)

Host Application: C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe
-NoProfile -ExecutionPolicy Bypass -File
C:\Users\USER\Desktop\Powershell\editProfileSuperProfile-16-6-2024.ps1

Process ID: 19148

PSVersion: 5.1.19041.4522
```

```
PSEdition: Desktop

PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.19041.4522

BuildVersion: 10.0.19041.4522

CLRVersion: 4.0.30319.42000

WSManStackVersion: 3.0

PSRemotingProtocolVersion: 2.3

SerializationVersion: 1.1.0.1

**********************

Transcript started, output file is C:\Users\USER\desktop\MSTC_
Policy06.16.12.33.txt

PS>TerminatingError(Invoke-RestMethod): "
{"type":"https://tools.ietf.org/html/rfc7231#section-
6.5.13","title":"Unsupported Media Type","status":415,"traceId":"00-
1fa6a9561e39115c5b5258f162c5540d-a5c8015bfcd9c025-00"}"

6/16/2024 12:33:43 PM - Searching 'MicrosoftTeams' module...

6/16/2024 12:33:47 PM - 'MicrosoftTeams' module installed successfully.

6/16/2024 12:33:47 PM - Importing 'MicrosoftTeams' module...

INFO: Loaded Module 'Microsoft.Teams.ConfigAPI.Cmdlets'

6/16/2024 12:33:52 PM - 'MicrosoftTeams' module imported successfully.

6/16/2024 12:35:10 PM - Connected to Microsoft Teams successfully.

6/16/2024 12:35:10 PM - Getting recording policies...

6/16/2024 12:35:12 PM - Retrieved recording policies successfully.
```

```
6/16/2024 12:35:12 PM - fetching domains...

6/16/2024 12:35:15 PM - Domain M365x21689653.onmicrosoft.com fetched
successfully.

6/16/2024 12:35:15 PM - SuperProfile06062024142032 already exists. Skipping
policy creation.

6/16/2024 12:35:15 PM - Application Instance for SuperProfile06062024142032
already exist.

6/16/2024 12:35:16 PM - Starting Sync Process for SuperProfile06062024142032
...

6/16/2024 12:35:18 PM - Sync Process for SuperProfile06062024142032
Finished.

6/16/2024 12:35:18 PM - SuperProfile06062024142032 already exist ,
skipping..

6/16/2024 12:35:18 PM - Configuring SuperProfile06062024142032 Recording
Policy...

6/16/2024 12:35:24 PM - Configuring disconnectCalls True for
SuperProfile06062024142032...

6/16/2024 12:35:26 PM - Configuring audioNotification False for
SuperProfile06062024142032...

6/16/2024 12:35:27 PM - SuperProfile06062024142032 Recording Policy Has Been
Configured.

6/16/2024 12:35:27 PM - Assigning groups to primary policy...

Adding 4d93b1c7-f944-4e82-a372-1ebe23979c6e to SuperProfile06062024142032..
please wait..

WARNING: Group 4d93b1c7-f944-4e82-a372-1ebe23979c6e already assigned to
SuperProfile05302024155452 policy.

Force Assignment set to True, adding 4d93b1c7-f944-4e82-a372-1ebe23979c6e to
SuperProfile06062024142032.. please wait..

Sending following status to API....
```

```
{
    "TenantId":  "5f4e3129-dd39-4ccd-bc4f-98423bee2c1b",
    "Message":  "Success",
    "PolicyId":  "SuperProfile06062024142032",
    "StatusCode":  0
}

Results sent successfully and should be reflected in the UI
**********
Windows PowerShell transcript end
End time: 20240616123533
**********
```

7. Once you have successfully run the script, verify that the Recording Profile status is 'Successful'.



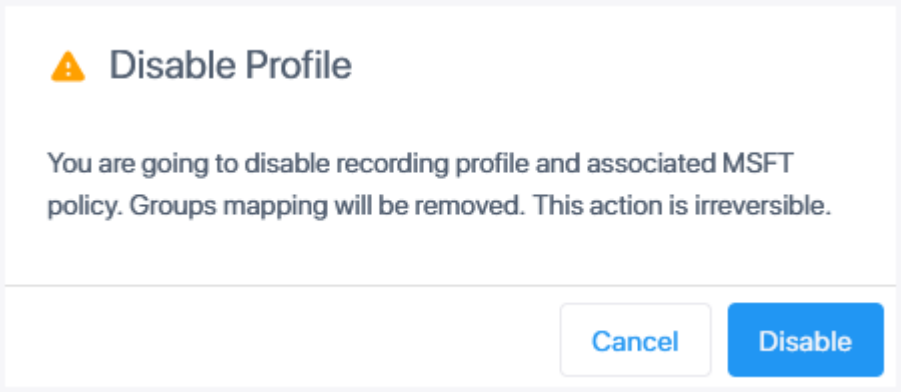
Disabling Recording Profile

You can disable a recording profile. Once disabled, the profile cannot be reenabled.

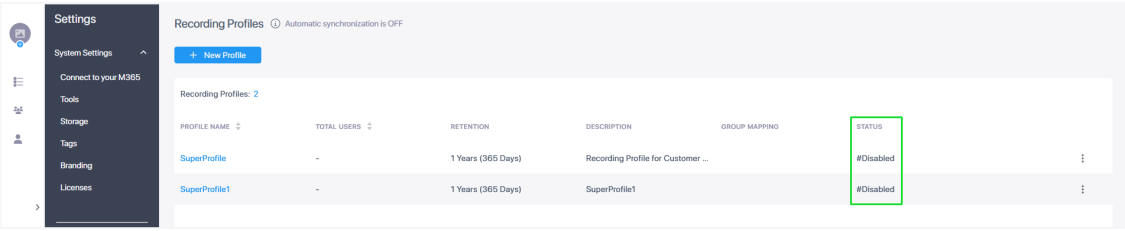
- A profile cannot be deleted if it has associated calls.
- The Call Retention period can be edited upon deletion.

➢ **Do the following:**

1. In the Icon pane, click , and then in the Navigation pane, select **Recording Settings** > **Recording Profiles**.
2. Select the Recording Profile that you wish to delete, and then from the right-click menu, choose **Disable Profile**. A confirmation dialog is displayed.



3. Click **Disable**. The profile is disabled.

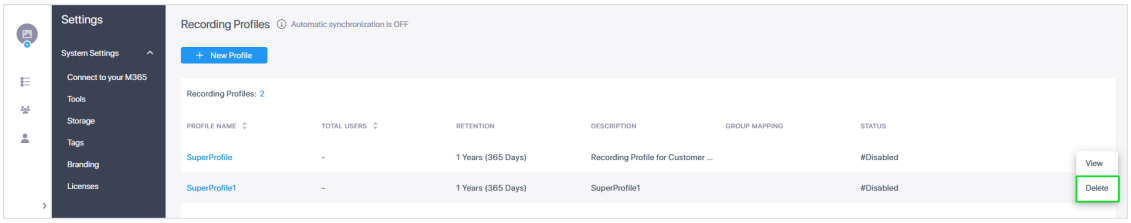


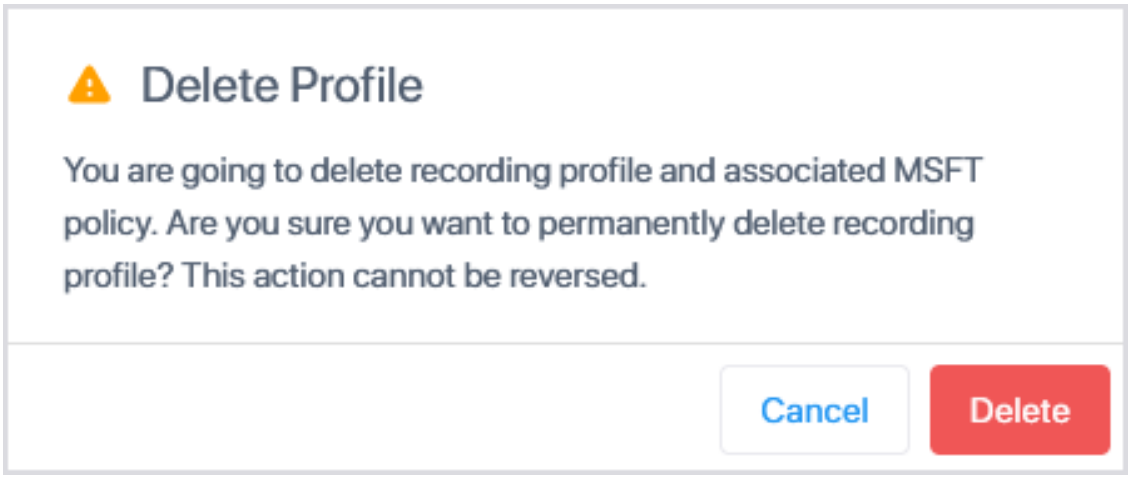
Deleting Recording Profile

You delete a recording profile that is no longer required.

➢ **Do the following:**

1. In the Icon pane, click , and then in the Navigation pane, select **Recording Settings** > **Recording Profiles**.
2. Select the Recording Profile that you wish to delete, and then from the right-click menu, choose **Delete Profile**. A confirmation dialog is displayed.



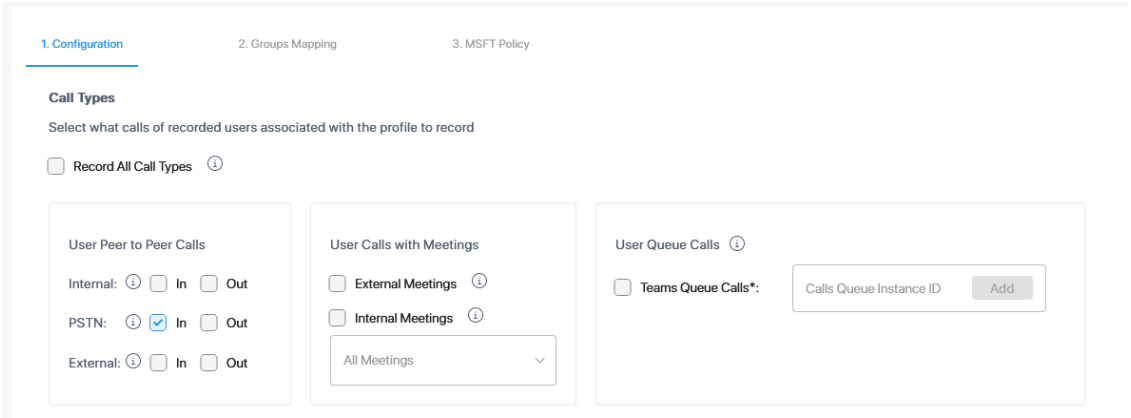


3. Click **Delete**. The profile is deleted.

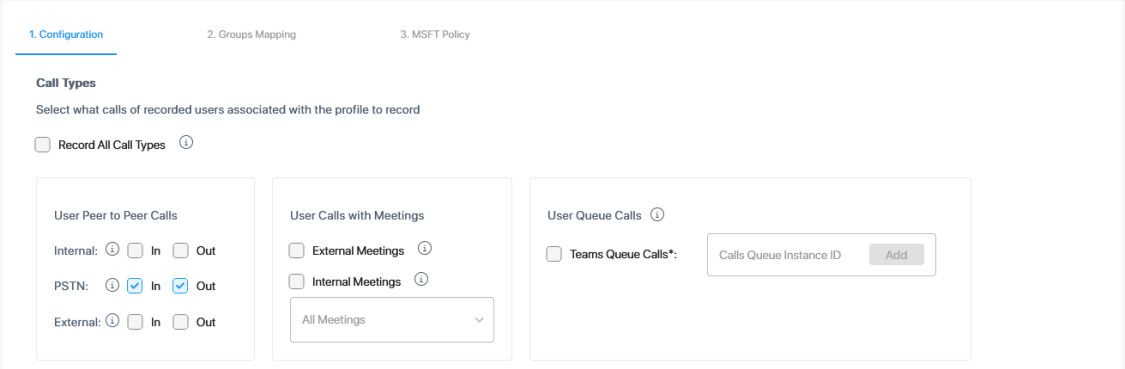
Recording Profile-Call Type Configuration Examples

The following shows configuration examples for different call type settings.

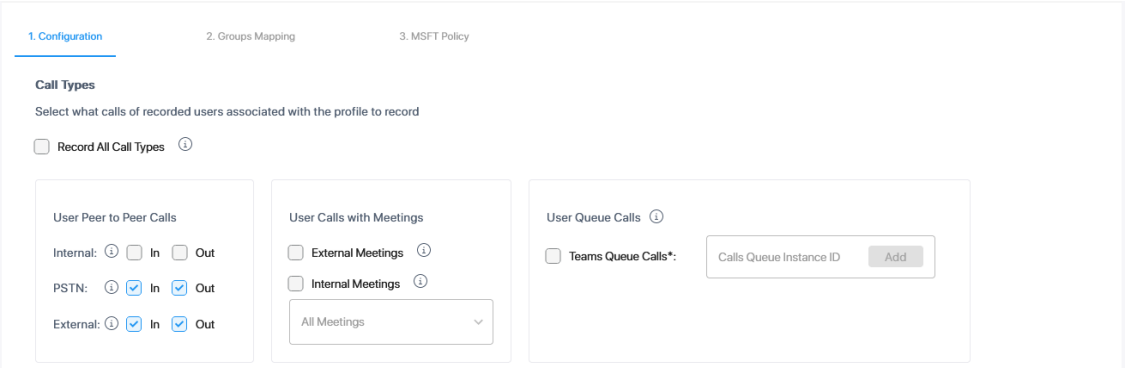
- Record inbound PSTN calls:



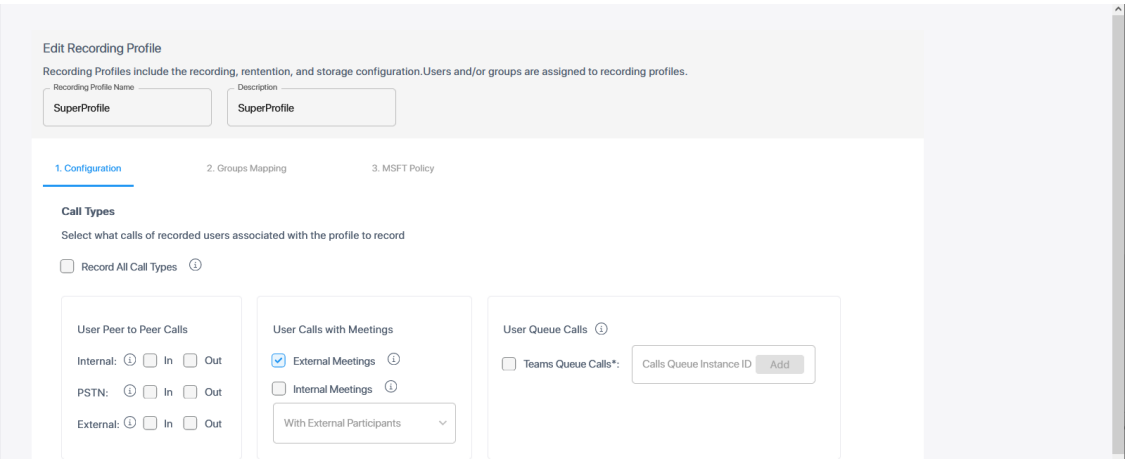
- Record all PSTN Calls:



- Record External calls (PSTN and Federation):



- Calls with External Meetings:



Managing Access Profiles

Access profiles lets you configure Call Permissions, Recording and Access Profiles and System Configuration Permissions. You can determine which calls the targeted users can access, which actions can be performed on the calls. You can determine whether operators can perform Global configuration in the Service Portal. AAD groups of the customer tenant including targeted users are mapped to the Access Profile.

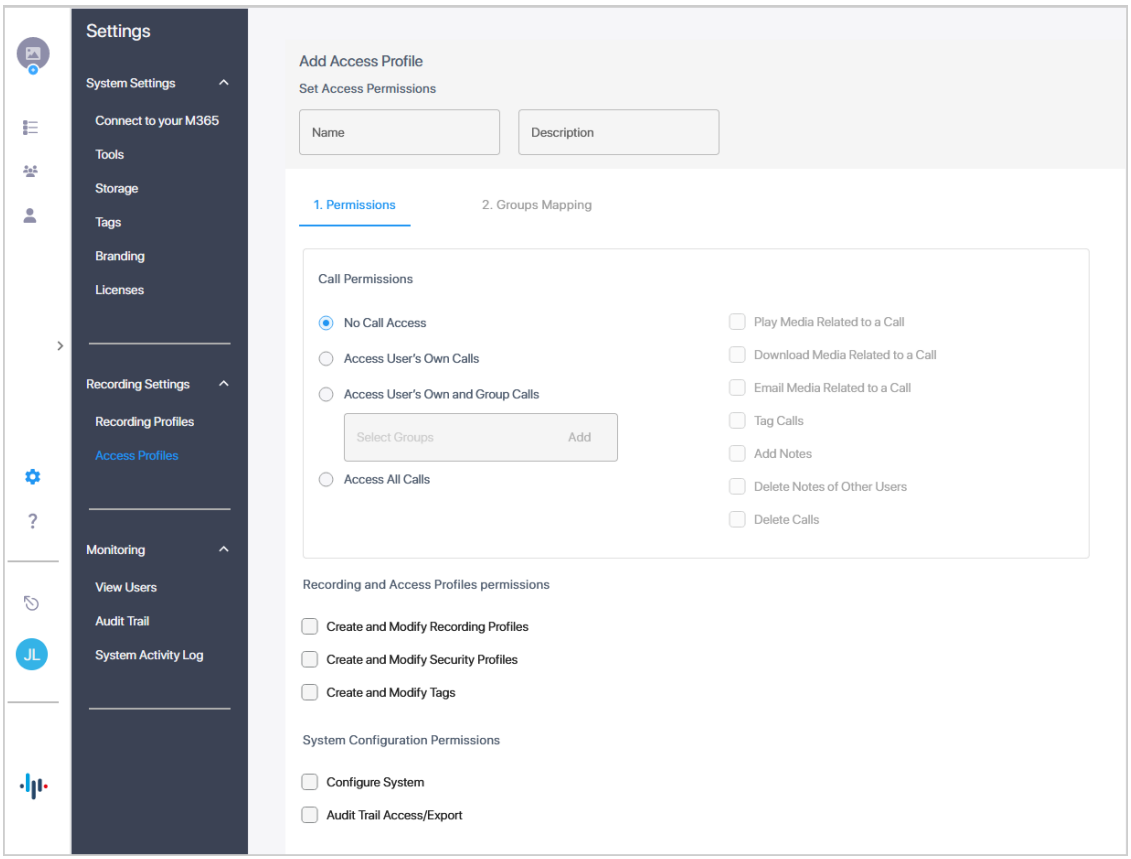
See also:

- Adding an Access Profile on the next page
- Modifying Access Profiles on page 88

- Viewing Access Profiles on page 90
- Deleting Access Profiles on page 92
- Viewing Global Admin Details on page 93

➢ **Do the following:**

1. In the Icon pane, click , and then in the Navigation pane, select **Recording Settings** > **Access Profiles**.

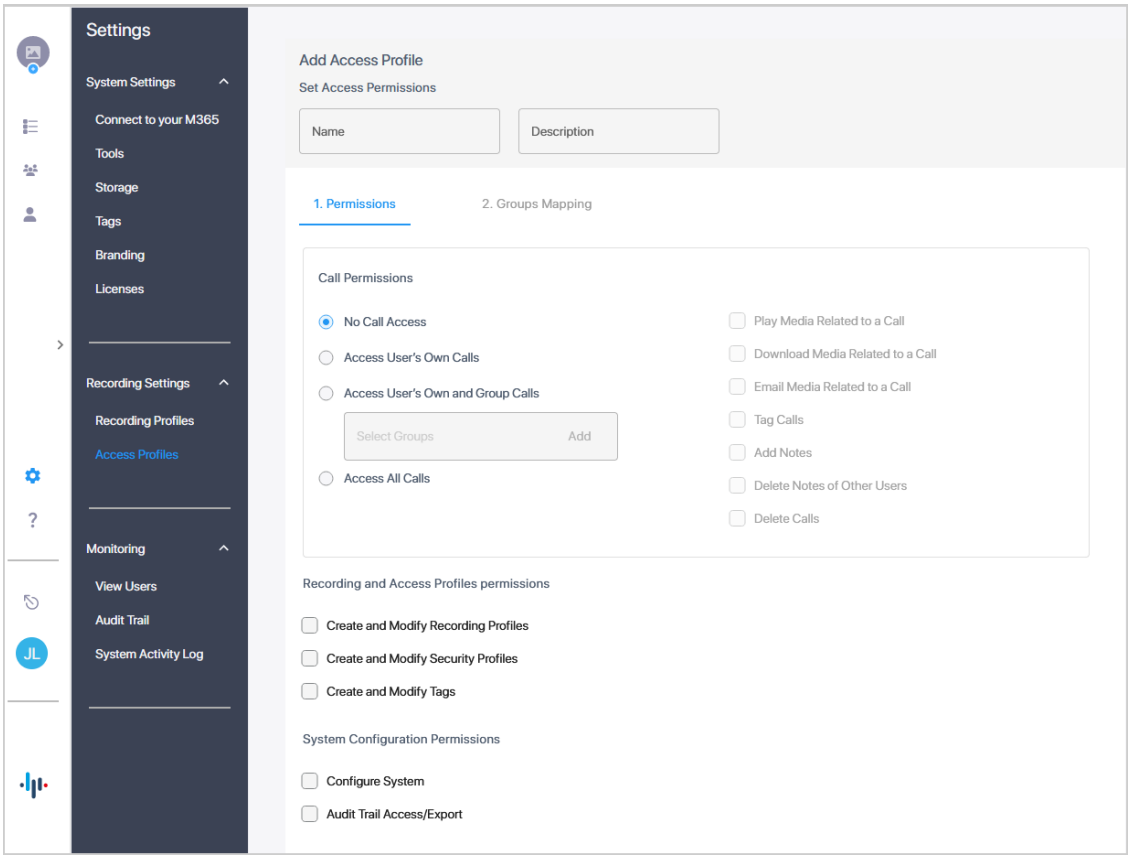


Adding an Access Profile

The Quick Start wizard process created an initial Access profile for your tenant. You can add additional profiles as required. For example, for new user groups or locations.

➢ **To add an Access Profile:**

1. In the Icon pane, click , and then in the Navigation pane, select **Recording Settings** > **Access Profiles**.

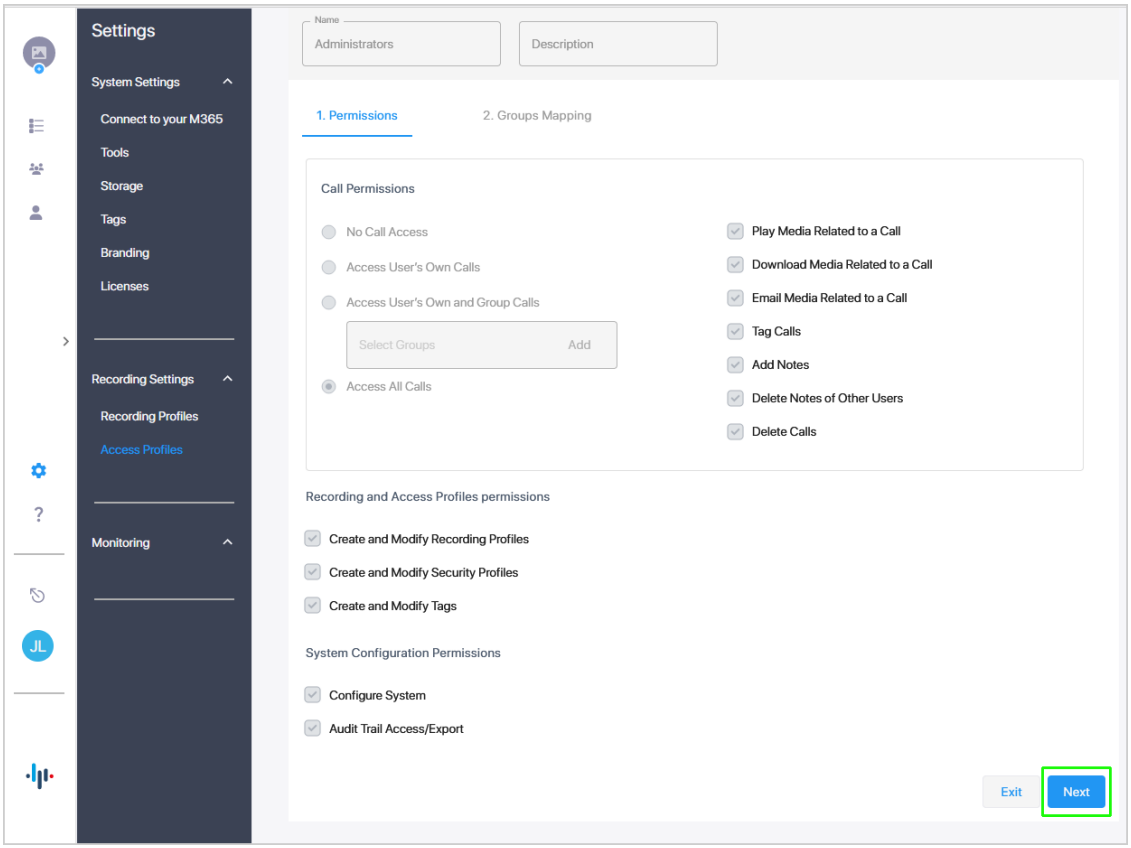


2. Configure parameters according to the table below.

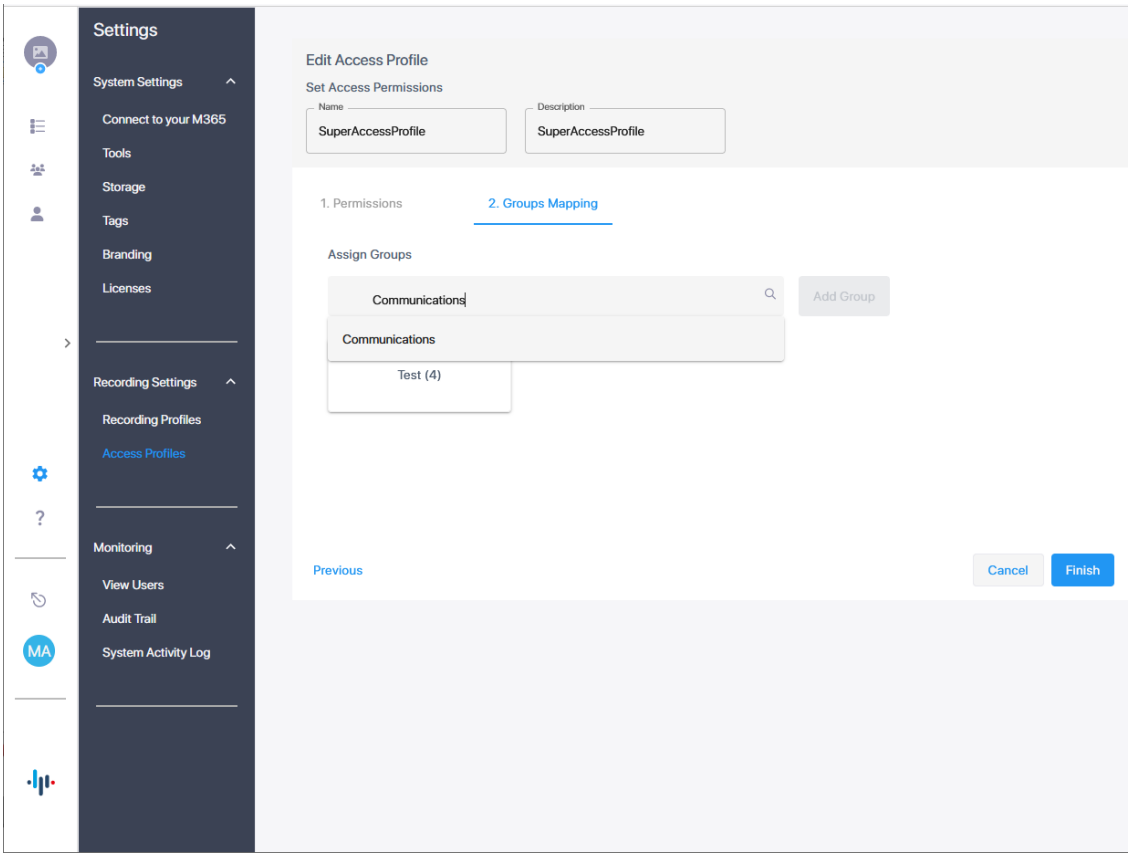
Field	Description
Name	Name of the Access Profile.
Description	Description of the Access Profile.
Call Permissions	
No Call Access	Prevent access to all calls.
Access User's Own Calls	Allow access of the Targeted user to their own calls.
Access User's Own and Group Calls	Click **Add** and then from the Drop-down list, select the M365 Azure group to add. Verify your group details in the Azure portal of your tenant.
Access All Calls	Allow access to all calls.
Play Media Related to Call	Allows the plays back of media for the call
Download Media Related to a Call	Allows the download of call media.

Field	Description
Tag Calls	Allows the creation of call tags.
Add Notes	Allows the adding of notes.
Delete Notes of Other Users	Allows the Global admin to delete notes created by tenant users.
Delete Calls	Allows the deletion of calls.
Recording and Access Profiles permissions	
Create and Modify Recording Profiles	Allows users to create and modify Recording profiles.
Create and Modify Access Profiles	Allows users to create and modify Access profiles (change the screen, it says Security Profiles).
Create and Modify Tags	Allows users to create and modify tags.
System Configuration Permissions	
Configure System	Allows users to configure System settings. If you wish to create and modify tags, you must select 'Create and Modify Tags' option above.
Audit Trail Access/Export	Allows users to access and export Audit trails.

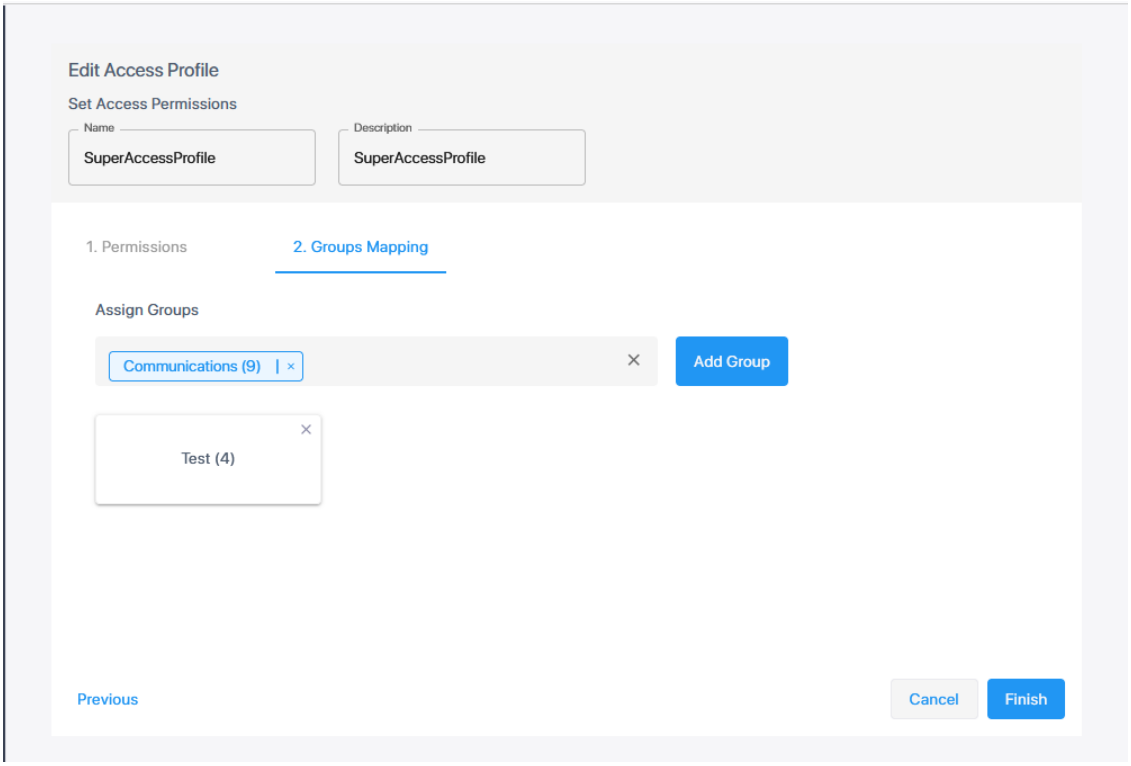
3. Click **Next** to configure groups.



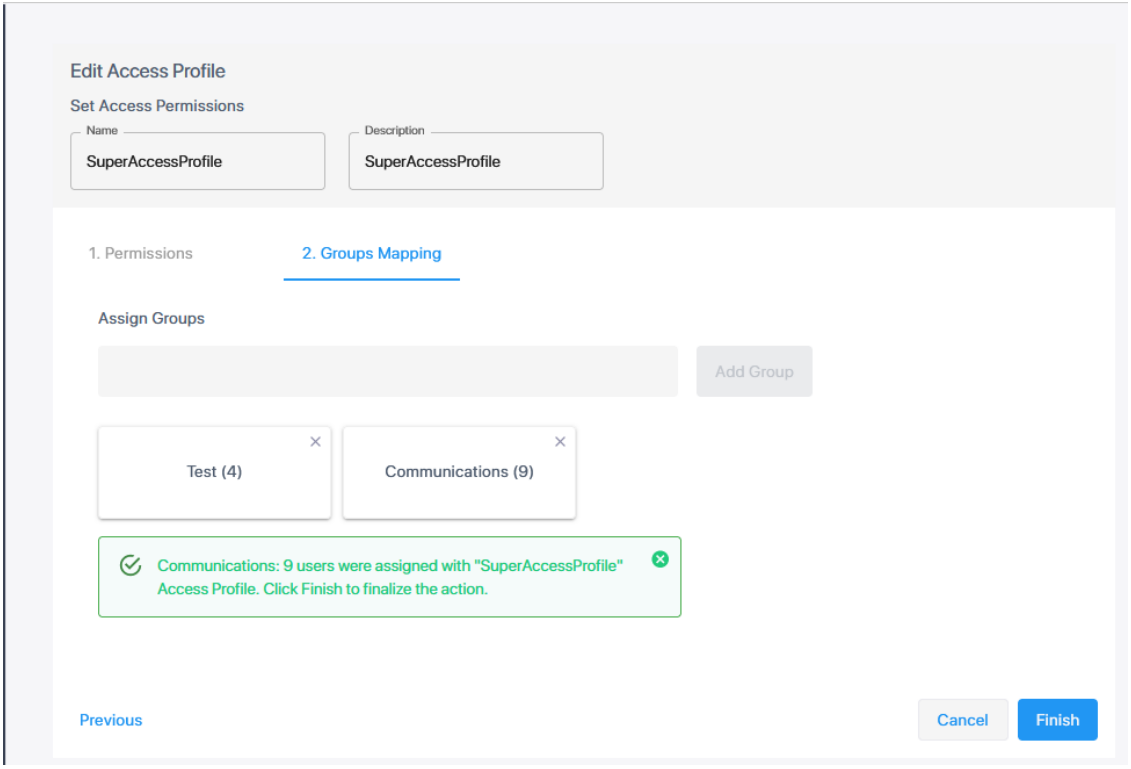
4. In the Assign Groups field, start typing the name of the group that you wish to assign; the field is auto-populated.



5. Click **Add Group**.



A confirmation message is displayed.



6. Click **Finish** to complete the configuration.

- Access profiles are synchronized automatically with the your M365 platform. This process may take a few minutes.
- The Sync Groups to AAD action is not applicable.

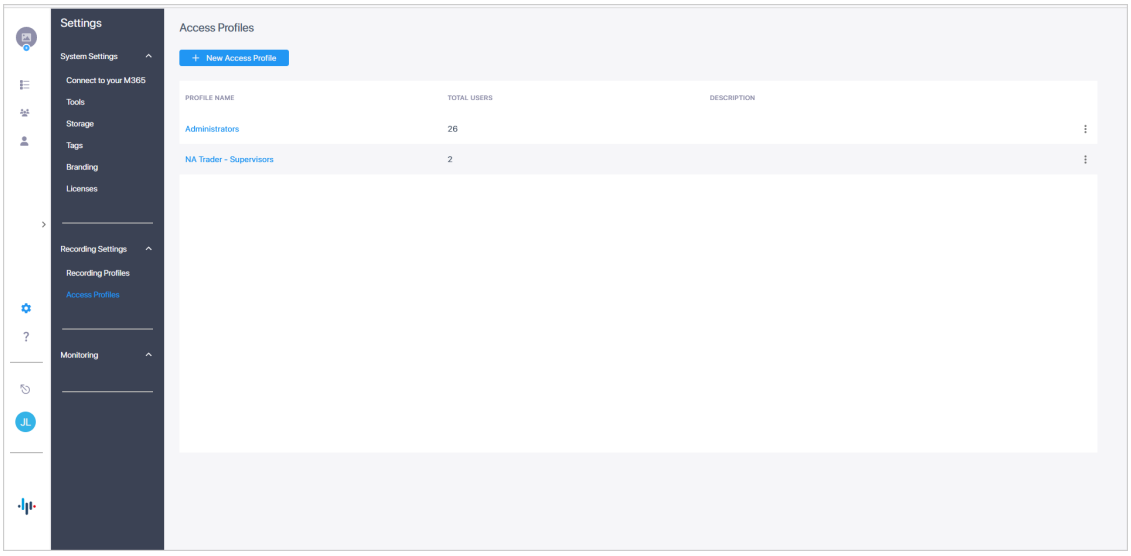
Modifying Access Profiles

This option lets you modify existing Access profiles. For example, you may decide that users can access not only their own calls, but also calls made by other users in their group.

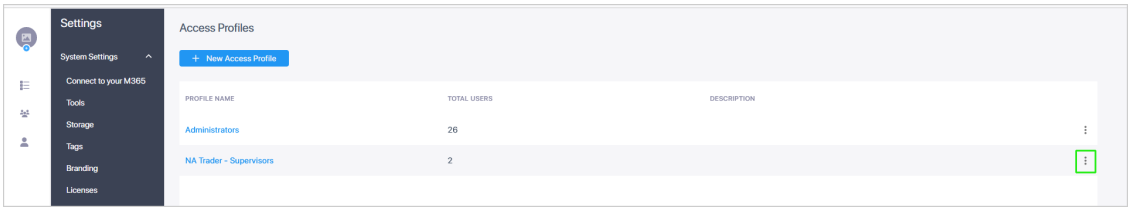
- Access profiles are synchronized automatically with the your M365 platform. This process may take a few minutes.
- The Sync Groups to AAD action is not applicable.

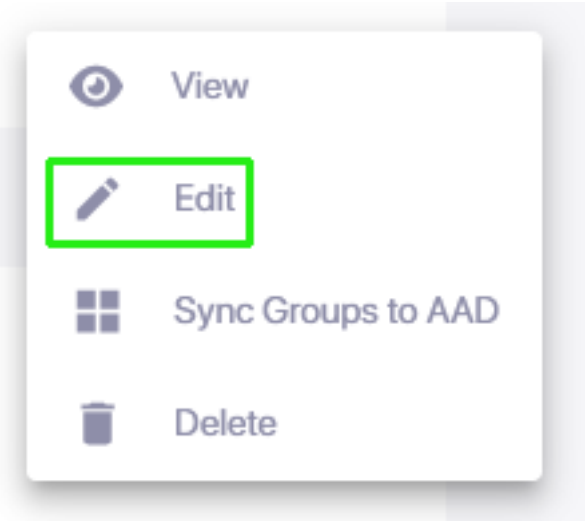
➢ **Do the following:**

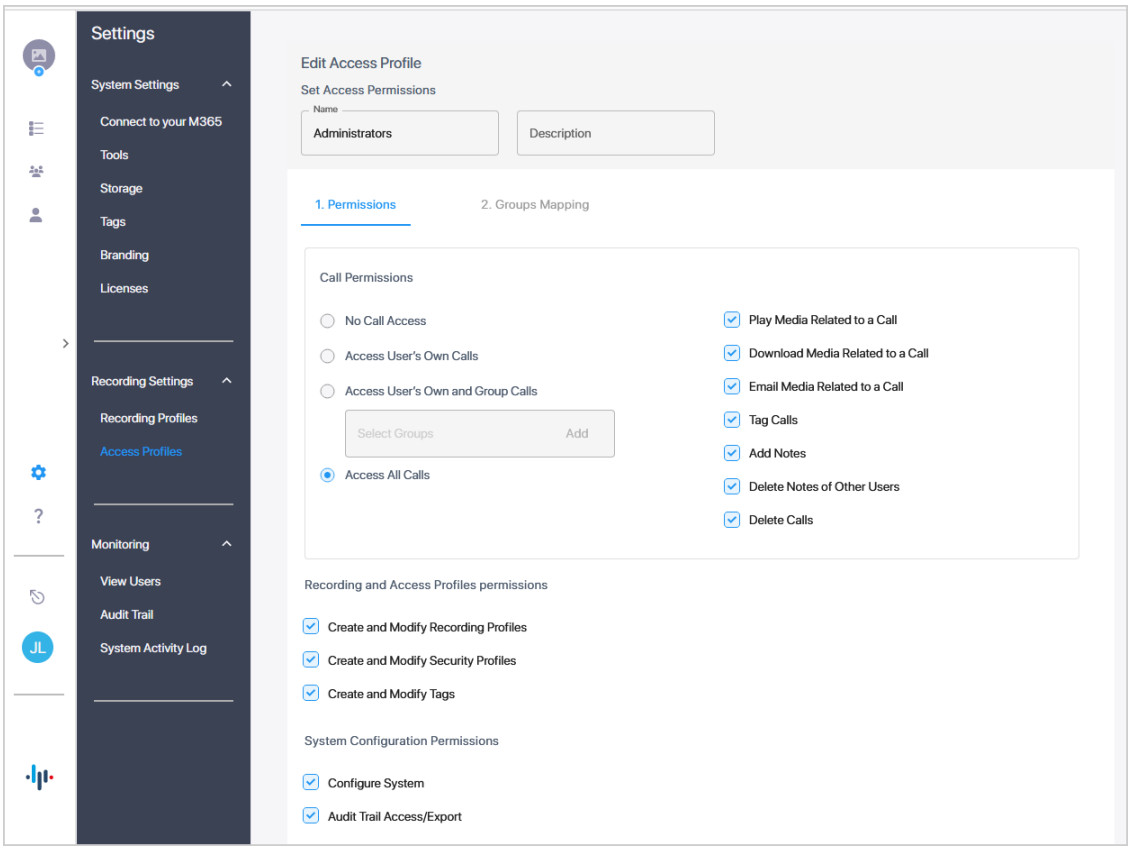
1. In the Icon pane, click , and then in the Navigation pane, select **Recording Settings** > **Access Profiles**.



2. Select the profile you wish to edit, click ... to open the right-click menu, and then choose **Edit**.







3. Edit parameters according to the table below.

Field	Description
Name	Name of the Access Profile.
Description	Description of the Access Profile.
Call Permissions	
No Call Access	Prevent access to all calls.

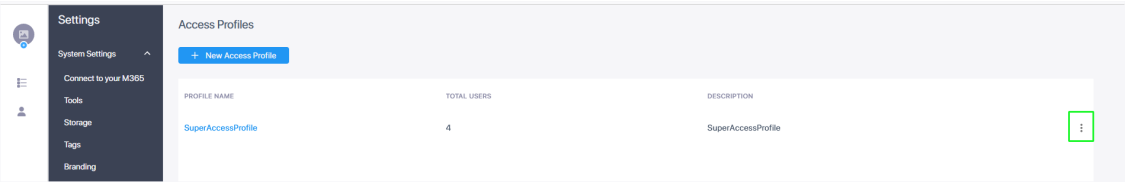
Field	Description
Access User's Own Calls	■ Play Media Related to Call ■ Download Media Related to a Call ■ Tag Calls ■ Add Notes ■ Delete Notes of Other Users ■ Delete Calls
Access User's Own and Group Calls	Click **Add** and then from the Drop-down list, select Security group to add.
Access All Calls	Allow access to all calls.
Recording and Access Profiles permissions	
Create and Modify Recording Profiles	Allows users to create and modify Recording profiles.
Create and Modify Security Profiles	Allows users to create and modify Security profiles
Create and Modify Tags	Allows users to create and modify tags.
System Configuration Permissions	
Configure System	Allows users to configure System settings.
Audit Trail Access/Export	Allows users to access and export Audit trails.

Viewing Access Profiles

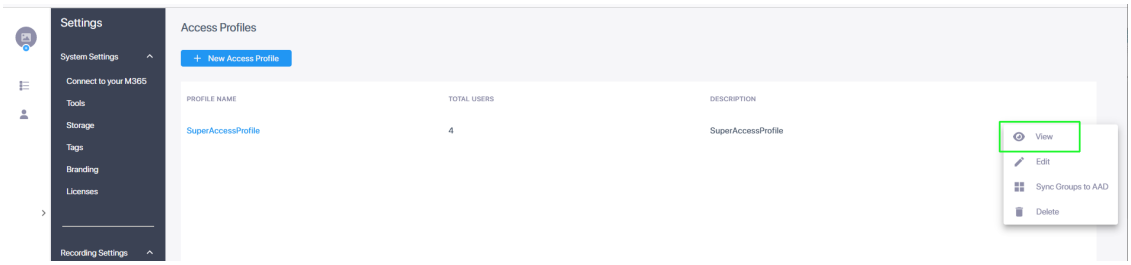
You can view the details of an existing Access Profile in Read-only view.

➢ **To view Access Profiles:**

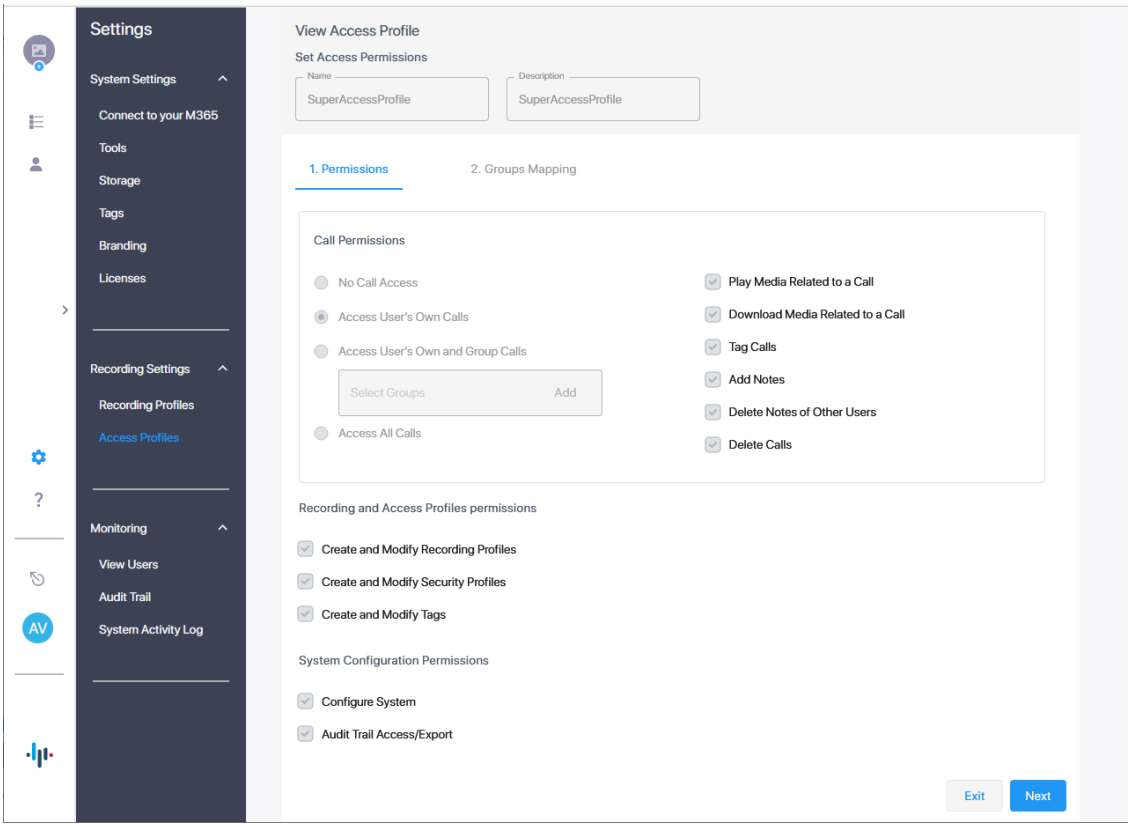
1. In the Icon pane, click , and then in the Navigation pane, select **Recording Settings** > **Access Profiles**.



2. Click the relevant Access Profile or click its right-click menu, and then choose **View**.



The Access Profile is displayed.



3. Refer to the parameter descriptions below.
4. Click **Next** to view attached Azure Groups.

Field	Description
Name	Name of the Access Profile.
Description	Description of the Access Profile.
Call Permissions	
No Call Access	Prevent access to all calls.
Access User's Own Calls	■ Play Media Related to Call ■ Download Media Related to a Call ■ Email Media Related to a Call

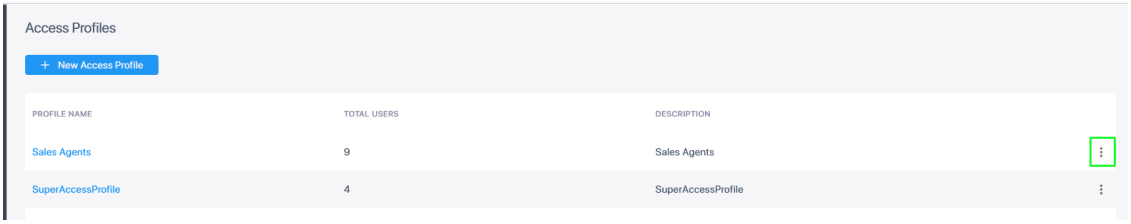
Field	Description
	■ Tag Calls ■ Add Notes ■ Delete Notes of Other Users ■ Delete Calls
Access User's Own and Group Calls	Click **Add** and then from the Drop-down list, select Security group to add.
Access All Calls	Allow access to all calls.
Recording and Access Profiles permissions	
Create and Modify Recording Profiles	Allows users to create and modify Recording profiles.
Create and Modify Security Profiles	Allows users to create and modify Security profiles
Create and Modify Tags	Allows users to create and modify tags.
System Configuration Permissions	
Configure System	Allows users to configure System settings.
Audit Trail Access/Export	Allows users to access and export Audit trails.

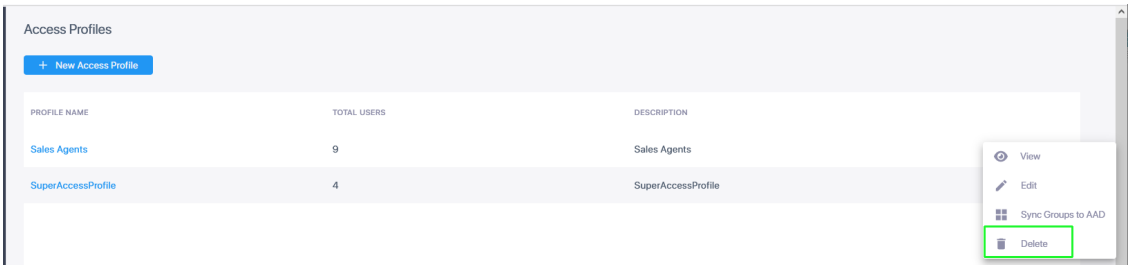
Deleting Access Profiles

You can delete an Access Profile that is no longer required.

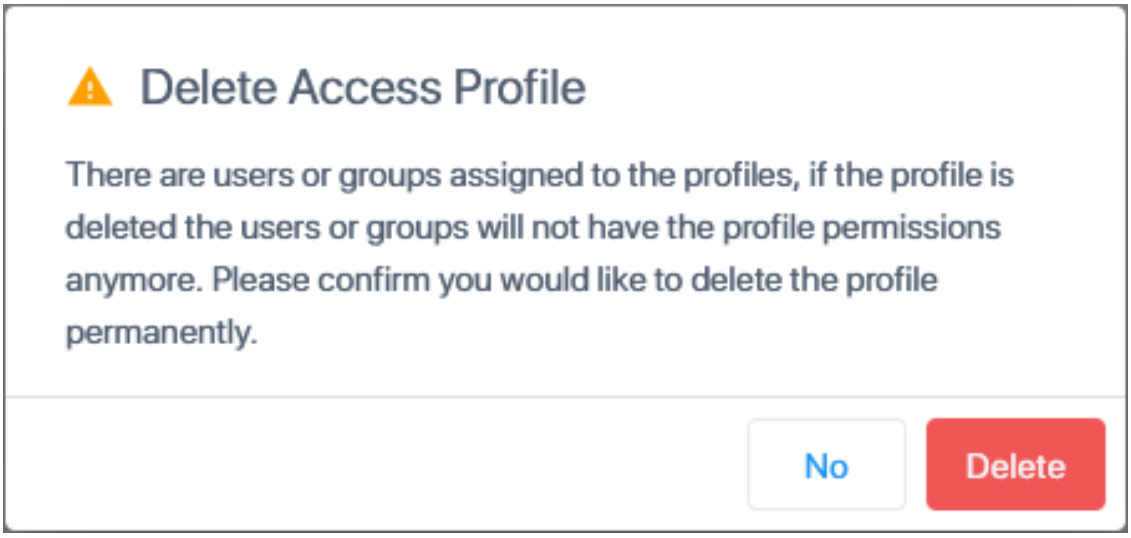
➢ To delete profile:

1. In the Icon pane, click , and then in the Navigation pane, select **Recording Settings** > **Access Profiles**.





2. Click the relevant Access Profile or click its right-click menu, and then choose **Delete**.

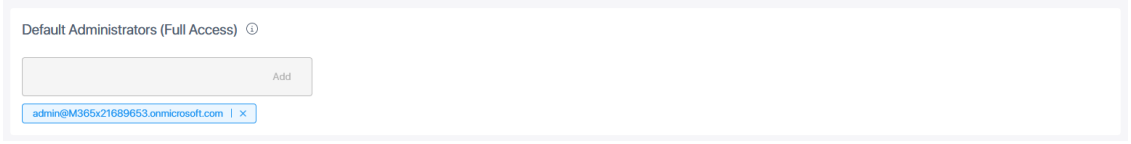


3. Click **Delete** to confirm.

Viewing Global Admin Details

The details of the Global Admin of the customer tenant are displayed at the bottom of the Access Profiles page.

> The permissions of this default administrator cannot be modified, and the user cannot belong to a mapped AAD group.



Interactions

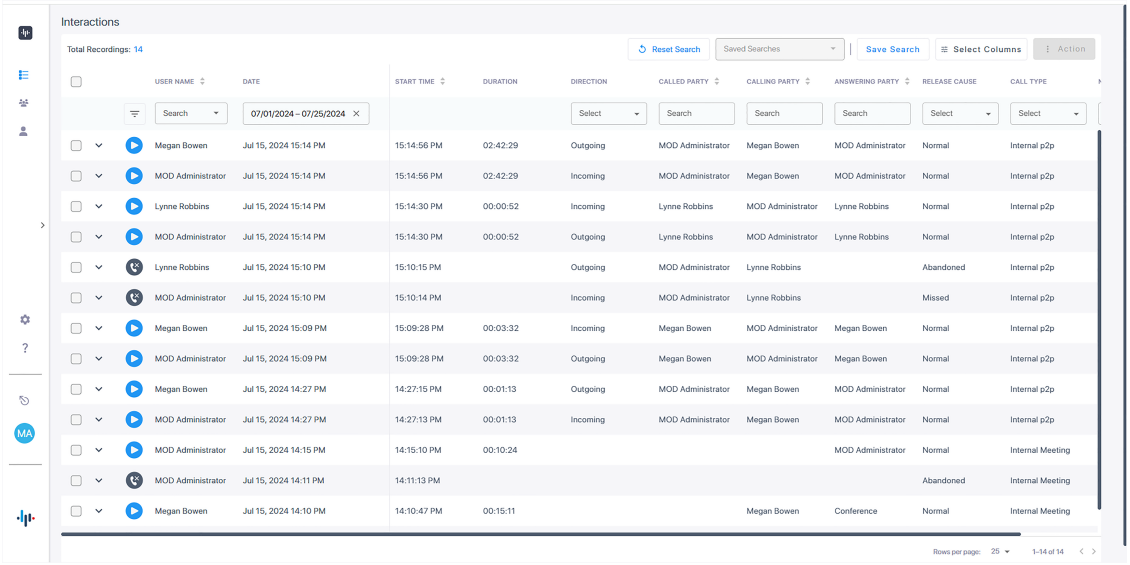
The Interactions page lets you manage voice interactions of Targeted users. Active recordings are shown in red. Once a recording has ended, and is successfully synchronized with the database, you can playback the recording using the Media player. The Interactions page of the Global Admin user displays interactions for all Targeted users of the M365 tenant. The Interactions page for a specific user displays interactions according to the configuration of the attached Access Profile of this user's AAD group. For example, if Adele Vance is attached to the Sales-US AAD group whose profile is configured with full access, then this user can also access interactions of all users of the M365 tenant. For each interaction, you can open the Media Player to view the Time line of the call and details. The details displayed under the Time line is determined by whether the columns are displayed on the page itself. When you hide columns in the page (seeCustomizing Columns on page 124), then the column data that is removed from page view is displayed under the Time line of the call. You can filter interactions according to specified search criteria and export data to an Excel file.

See also:

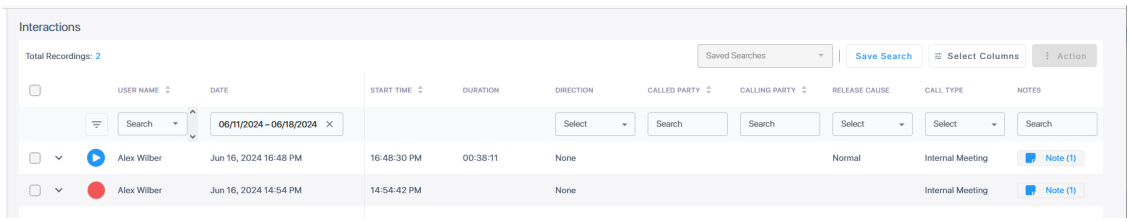
- Filtering Interactions and Active Calls Information on page 100
- Listening to Voice Interaction on page 112
- Downloading an Audio Call on page 117
- Exporting Interaction to Excel on page 118
- Deleting Calls on page 122
- Assigning Tags to Interactions on page 126
- Adding Notes to Interactions on page 129
- Customizing Columns on page 124

➢ **To manage interactions:**

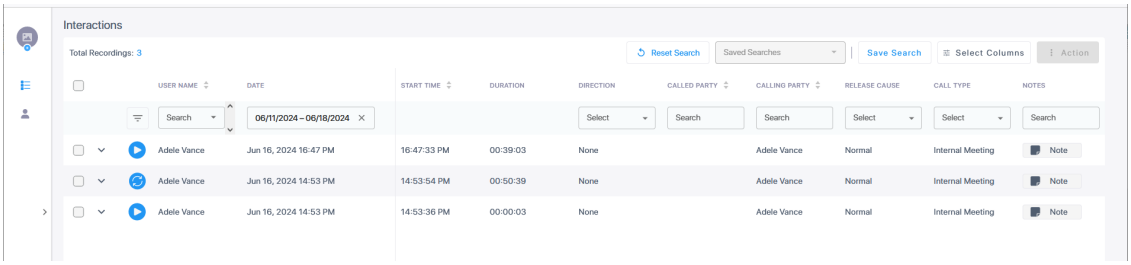
1. In the Icon pane, click . The figure below displays the Interactions page for a Global admin user who manages all Targeted users in the tenant.



The figure below displays the Interactions page for a logged in user Alex Wilber.

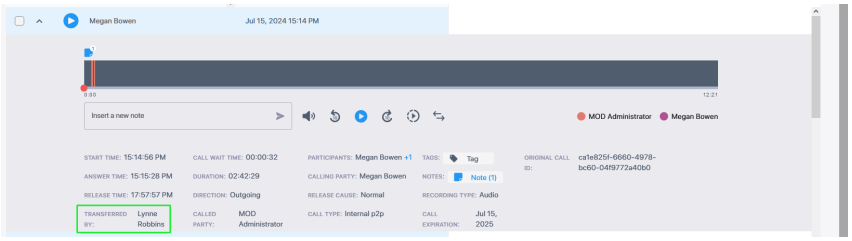


The figure below displays the Interactions page for a logged in user Adele Vance.



The table below describes the parameters in this screen.

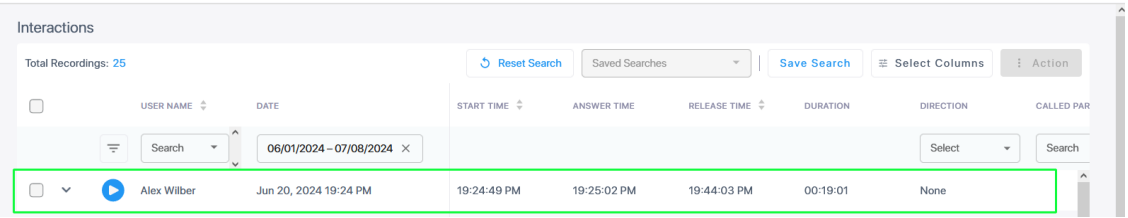
Parameter	Description
	Opens Media player.
User name	M365 Tenant user name. For example, Alex Wilber. Hover over the name to display the UPN e.g. AlexW@M365x21689653.OnMicrosoft.com
Date field	Indicates the date and time when the call is started by the Calling party. In the format Mon Day, YYYY HH:MM:SS AM/PM. For example, Jun 20, 2024 19:24 PM.

Parameter	Description
Start time	Indicates the date and time when the call is started i.e., when targeted user either receives or makes the call. In the format HH:MM:SS AM/PM. See example in figure below.
Answer Time	Indicates the time when the call is answered by the Called party; when the Targeted user answers the incoming call and the Called party answers the call made by the Targeted user. In the format HH:MM:SS AM/PM. See example in figure below.
Release Time	Indicates the date and time when the call is released; when the Targeted user terminates the call or the other party in the call terminates. In the format HH:MM:SS AM/PM. See example in figure below.
Hold/Retrieve Time	Indicates the time when the call was placed on hold and when it was retrieved. The field includes a list of time offsets from the start of the call and the name of the action. This value is not supported in this release.
On Behalf Of	Indicates the name of the party to whom the call is made on their behalf. For example, a sales representative places a call on behalf of the Brand Manager; Bill is Sales representative and Bob is the Brand Manager, when Bill makes a call on behalf of Bob, the recording associated with Bill should display 'On behalf of Bob'. When available, the party should include the user name (first and last name) and user UPN upon hover over.
Transferred By	Indicates the number or name of the party that transferred the call to another user. In the example below, Lynne Robbins transferred the call to Megan Bowen. The Transferred By party is Lynne Robbins. 
Transferred To	Indicates the number or name of the party to whom the call is transferred. For example, when Bob is on call with Brian, and Bob transfers the call to Bill, the 'Transferred To' party is Bill. When available, the party should include user name (first and last name) and user UPN upon hover over.

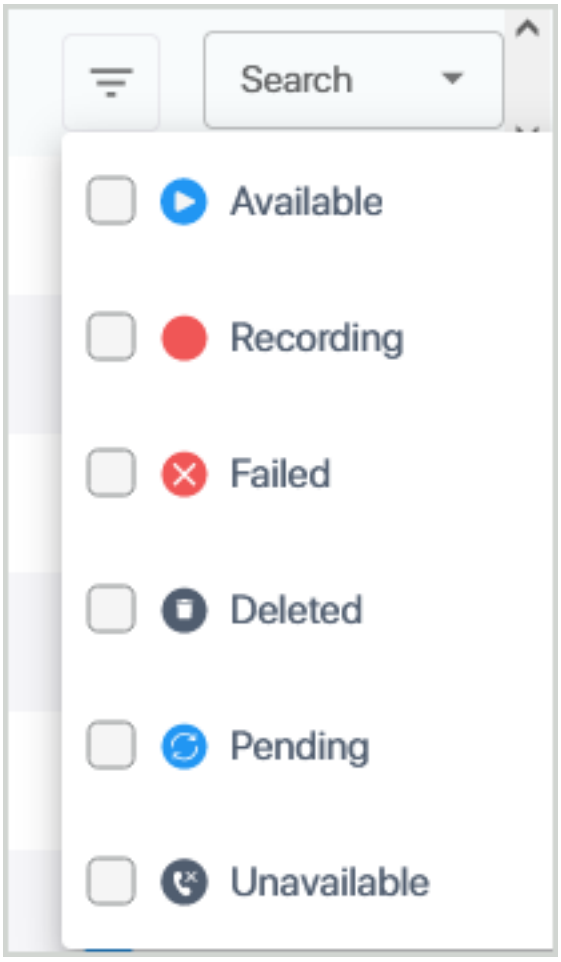
Parameter	Description
Call Wait Time	Indicates the Wait time until the call is answered by the Called party.
Duration	Duration of the recording (this value increments on-the-fly when a recording is active, see Managing Active Calls on page 132). It measures from the time the call is answered until the time it is released. In format HH:MM:SS. Value of zero indicates Unanswered calls.
Direction	Indicates if the call is 'Incoming' or 'Outgoing'. ■ Incoming: The associated targeted user receives the call. ■ Outgoing: The associated targeted user makes the call. ■ None: Conference call.
Called Party	Indicates the number or name of the party who receives the call. It may be the Targeted user for whom the call is recorded where the Targeted user receives the call. When available Called party should include user name (first and last name) and user UPN when hovered over. ⚠ The called party and answered party might not be the same if the call is answered on behalf of another user. For example, a secretary answers a call on behalf of their manager; Bob calls Brad; however, Bill answers the call. In this case, the answered part is Bill.
Participants	The name of the participants in the call (the Caller party is displayed with link to the names of the other participants).
Calling Party	Indicates the number or name of the party placing the call. It may be the Targeted user for whom the call is recorded where the Targeted user makes the call. When available Calling party should include user name (first and last name) and user UPN when hovered over.
Answering Party	The name of the party who answers the call. For transferred calls, party is displayed as 'Conference'.
Release Cause	Indicates the reason why a call is disconnected. One of the following values: ■ Normal – the call was answered and then released. ■ Failure – the call or recording was stopped due to an error. ■ Missed – the Targeted user didn't answer an incoming call. ■ Abandoned – the Targeted user made an outgoing call and hanged up before the call was answered

Parameter	Description
	■ Transferred – the call was transferred to another call.
Call Type	Indicates the type of the call. One of the following values: ■ Internal Meeting ■ External Meeting ■ Internal Meeting with External Participants ■ Externalp2p ■ PSTN p2p
Tags	Indicates the tags assigned to the interaction and a number representing the number of tags assigned (seeAssigning Tags to Interactions on page 126).
Notes	Indicates the notes assigned the Interaction and a number representing the number of notes assigned (see Adding Notes to Interactions on page 129).
Recording Type	Default: Full Time
Call Expiration	Indicates the date that the call recording is purged as defined in the Recording profile.
Original Call ID	Indicates the ID used to identify the call (also known as the 'SysCallId'). This value may be either the original call id or scenario id (Microsoft Teams). For example, when recording a Teams call between user A and B the id of the call between A and B is displayed. This ID is also displayed in the Teams CDR.

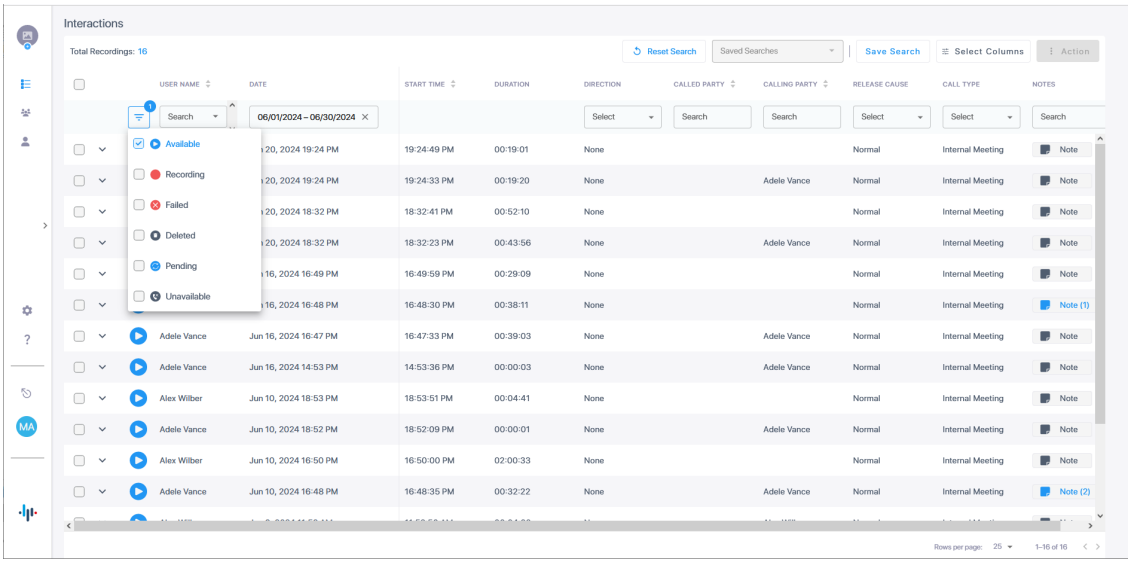
See example for Date and Time information below.



The table below describes the SmartTAP statuses.



In the Status filter drop-down list, select the check box filter(s) that you wish to retrieve.



The following table describes the Media Audio Statuses.

Icon	Status	Description
	Available	The interaction is available for playback.
	Pending	The interaction is pending database synchronization.
	Recording	The Interaction is currently being recorded.
	Failed	The recording failed.
	Unavailable	The recording is unavailable.
	Deleted	The recording has been deleted.

Filtering Interactions and Active Calls Information

The tables below describes the filters that can be applied to filter information in the Interactions and Active Calls screens.

Search Criteria	Interactions	Active Calls
Filtering by Call Status on the next page	☑	×
Filtering by Users and Groups on page 103	☑	×
Filtering by Date on page 104	☑	×
Filtering by Call Direction on page 106	☑	☑
Filtering by Participants on page 108	×	☑
(Filtering by Called or Calling Party on page 107)	☑	☑

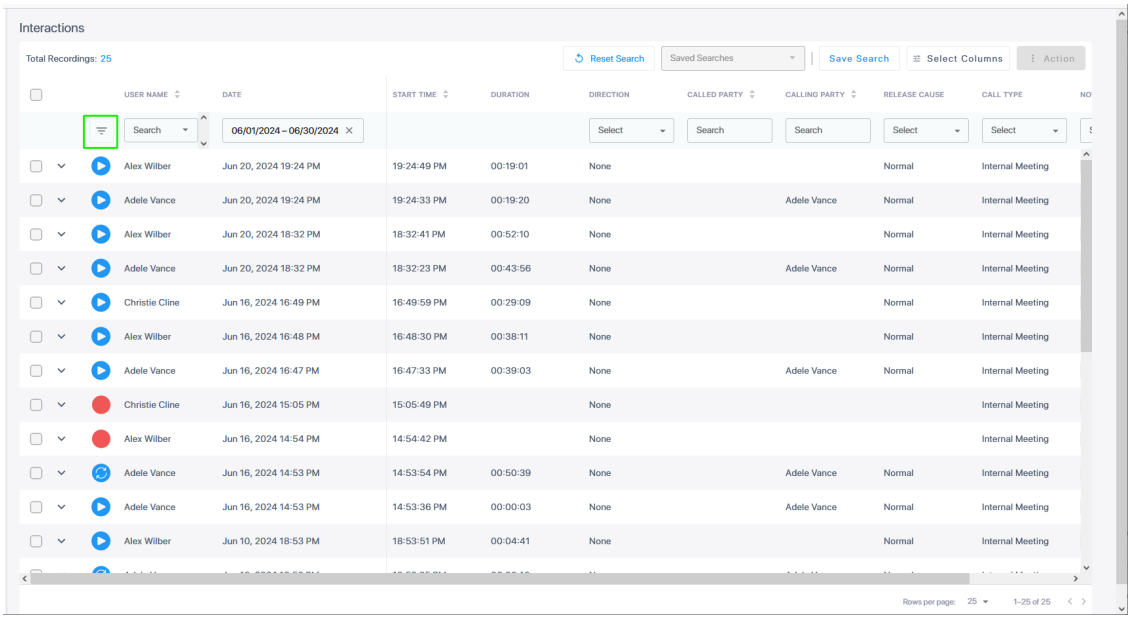
Search Criteria	Interactions	Active Calls
(Filtering by Called or Calling Party on page 107)	☑	☑
Filtering by Answering Party on page 107	☑	✖
Filtering by Call Tags on page 106	✖	☑
Filtering by Release Cause on page 110	☑	✖
Filtering by Call Type on page 109	☑	✖
Filtering by Notes on page 110	☑	☑
Filtering in Time line on page 116	☑	✖

Filtering by Call Status

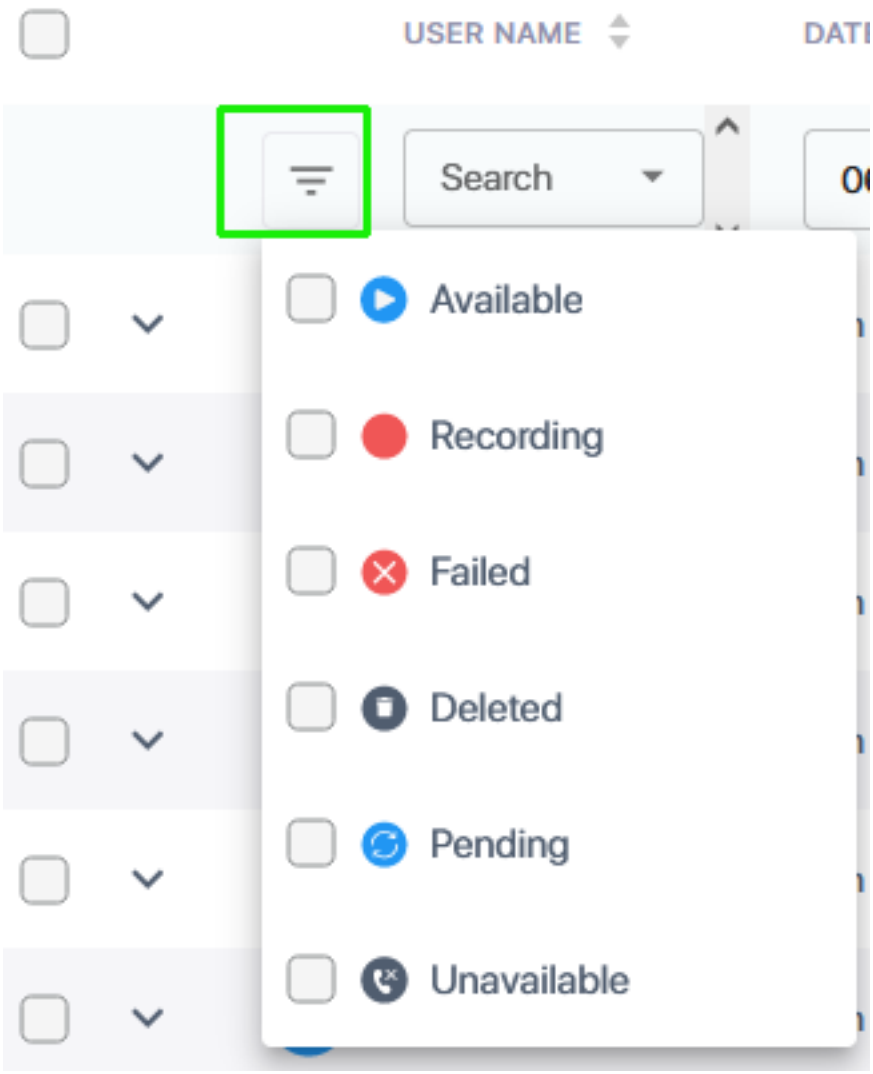
You can filter interactions according to the status of the recording.

➢ **Do the following:**

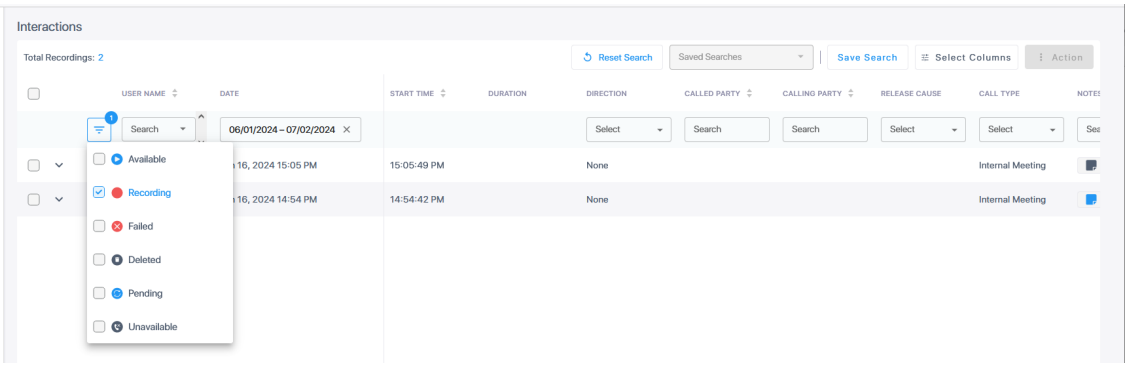
1. In the Icon pane, click .

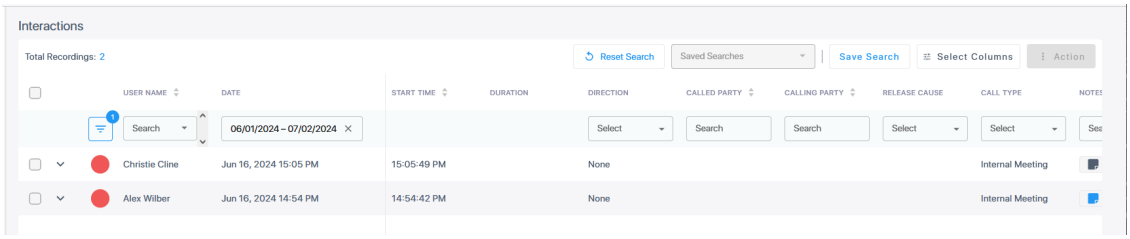


2. Click the Status icon.



3. Select the check box adjacent to the status for which you wish to filter search. In the example below, interactions are filtered according to 'Recording' status.



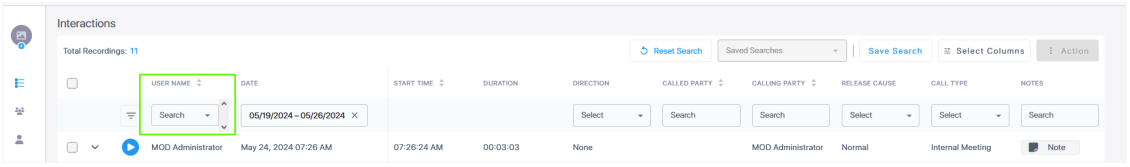


Filtering by Users and Groups

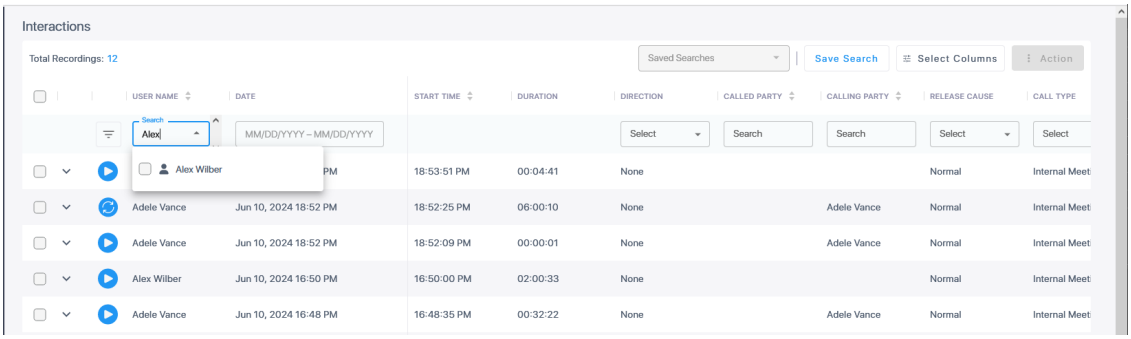
You can filter data according to specific group names that you have configured in one of your Recording profiles or by user names belonging to one these groups.

➢ Do the following:

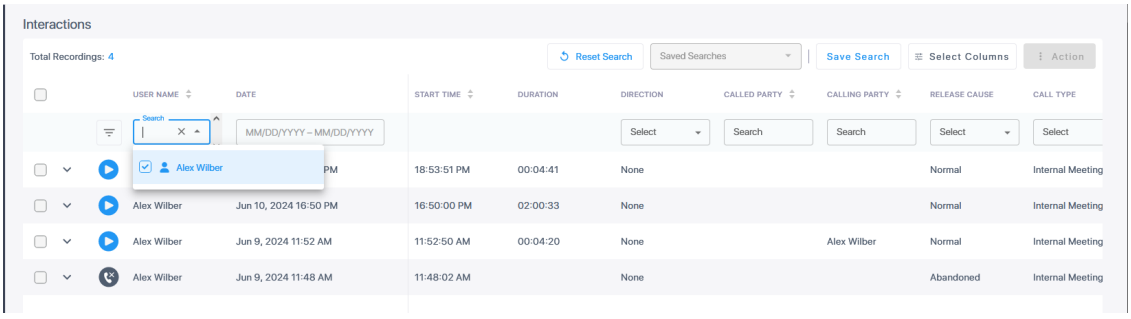
1. In the Icon pane, click either or .



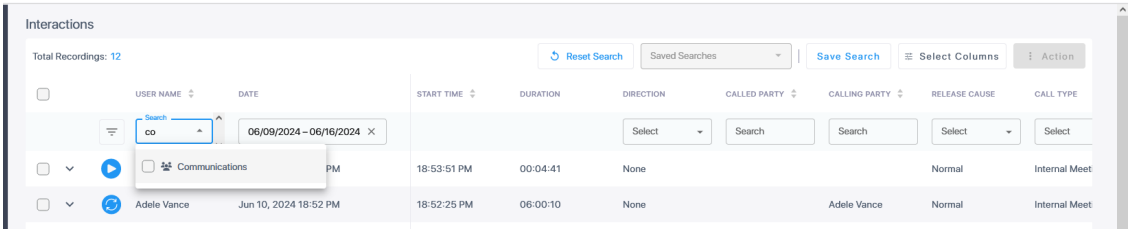
2. In the User Name search field, start typing the text string for the user that you wish to search.



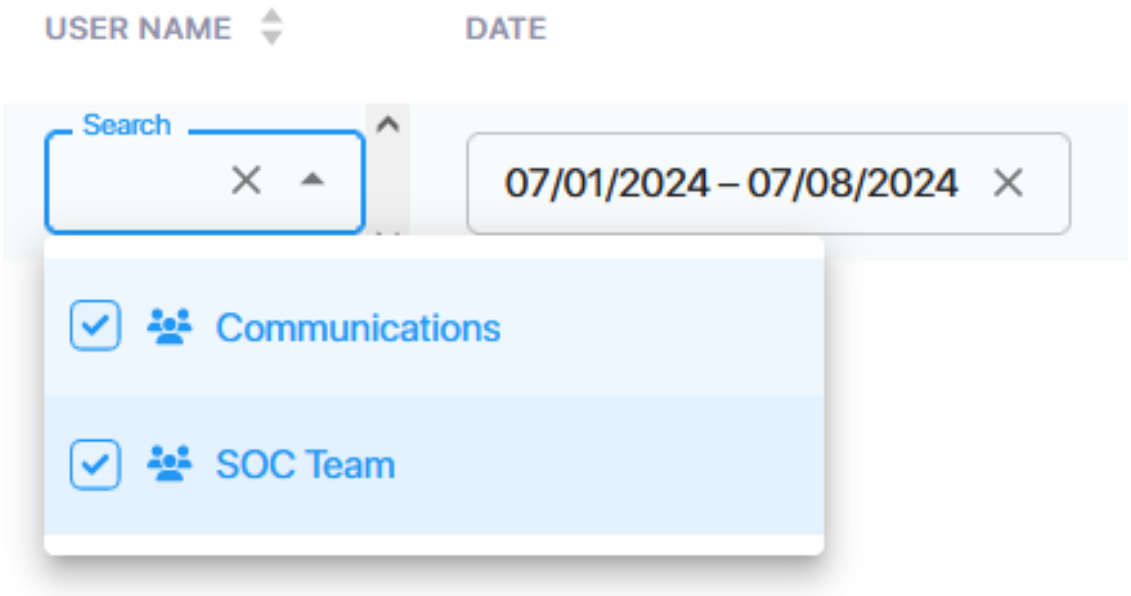
3. Select the check box adjacent to the username.



4. To search by group name, start typing the group name that you wish to search, and then select the check box adjacent to the group name.



You can also search for multiple groups.

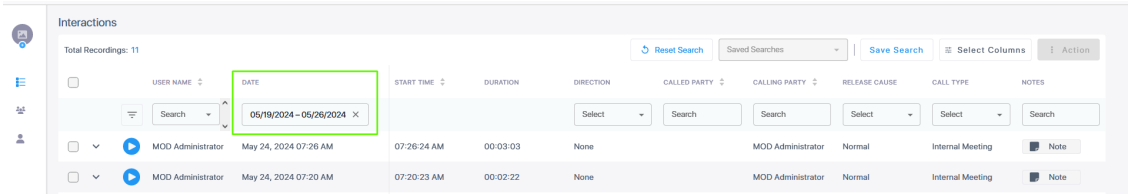


Filtering by Date

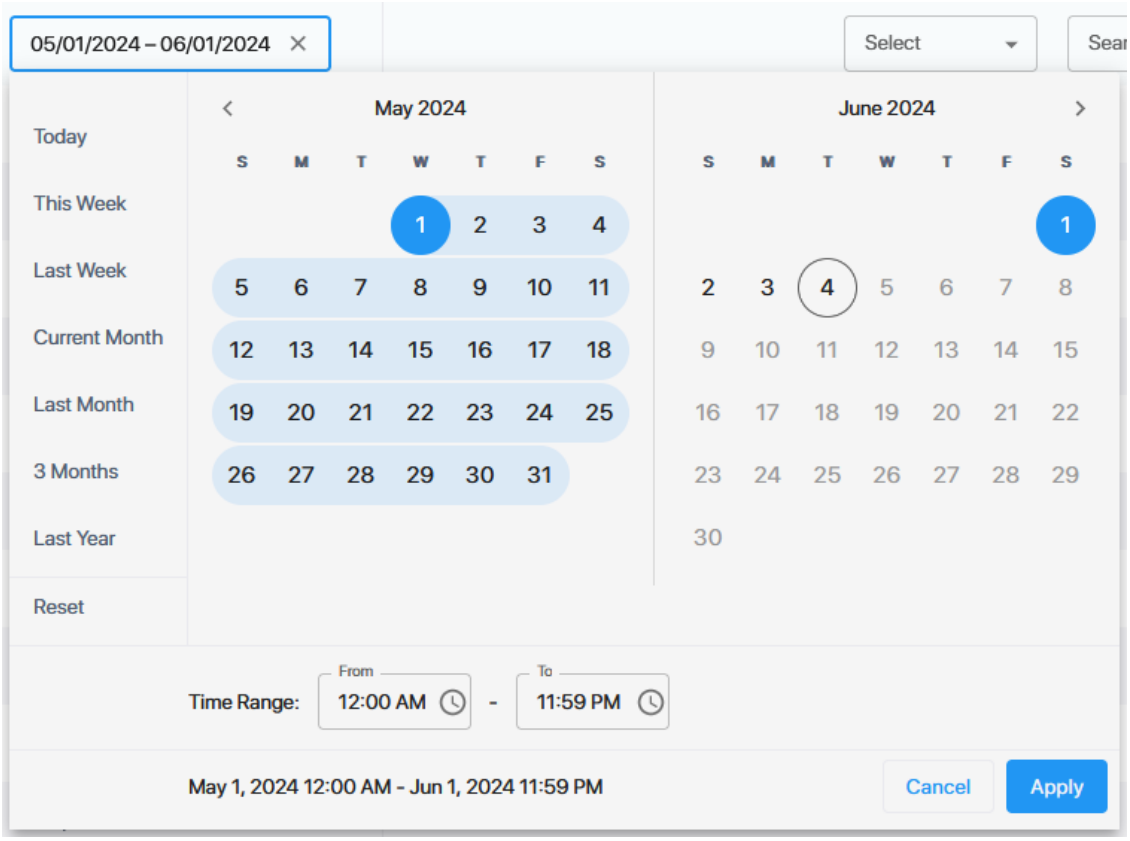
You can filter data according to specific date range.

➢ **Do the following:**

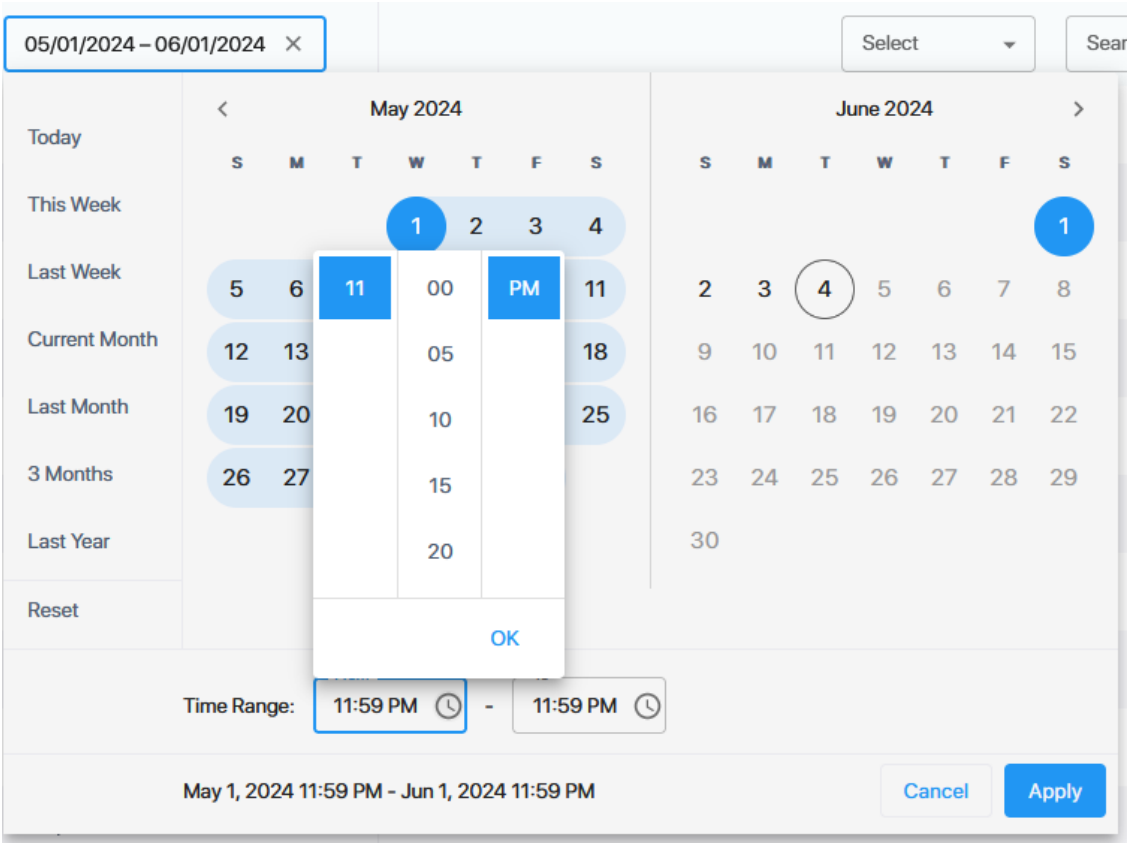
1. In the Icon pane, click .



2. Double click inside the Date field to open the Calendar. On the left-hand side, select the desired month and day to commence the search range. In the 'From' Time range field, double-click the clock, and then drag the scrolling bars to the desired hour and minutes to commence the search range.
3. On the right-hand side, select the desired month and day to end the search range. In the 'To' Time range field, double-click the clock and then drag the scrolling bars to the desired hour and minutes to end the search range.



4. To set the time of day, click inside the Time Range fields and roll the slider to set the desired times.



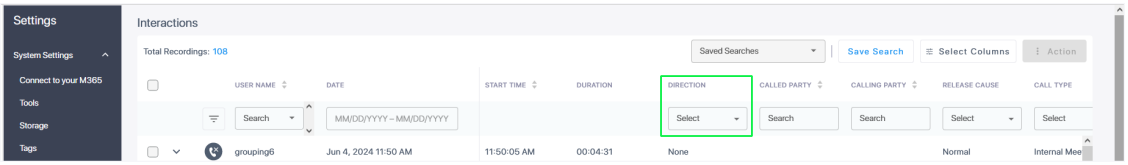
5. Click **Apply**.

Filtering by Call Direction

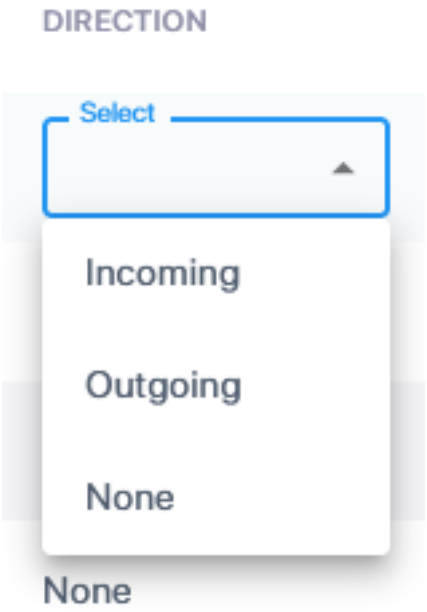
You can filter data according to call direction.

➢ **Do the following:**

1. In the Icon pane, click either or .



2. In the Direction field Drop-down list, select one of the following:
   - Incoming
   - Outgoing
   - None (indicates a Conference Call)

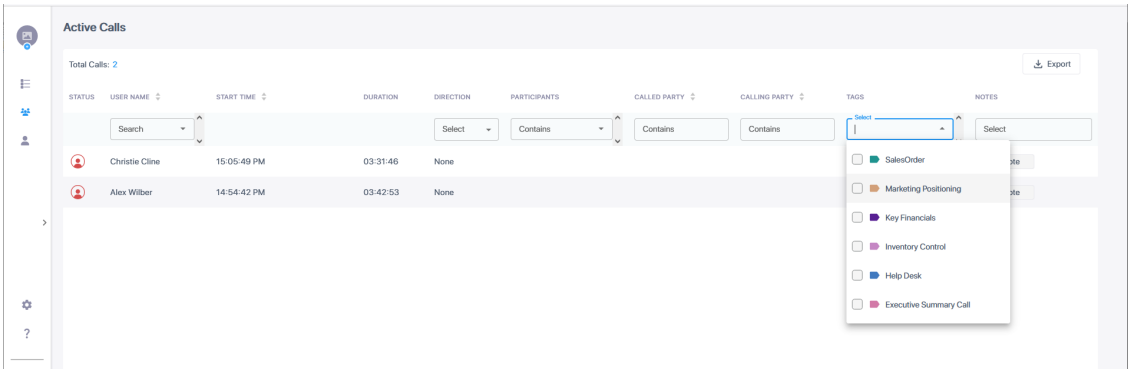


Filtering by Call Tags

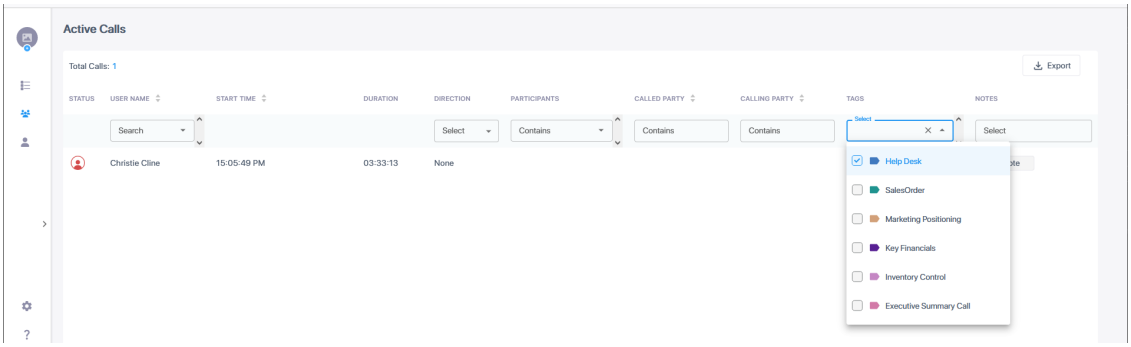
This section describes how to search by Call Tags.

➢ **To search for calls by call tags:**

1. In the Icon pane, click .



2. Select the check box adjacent to the tag that you wish to filter. The data is filtered.

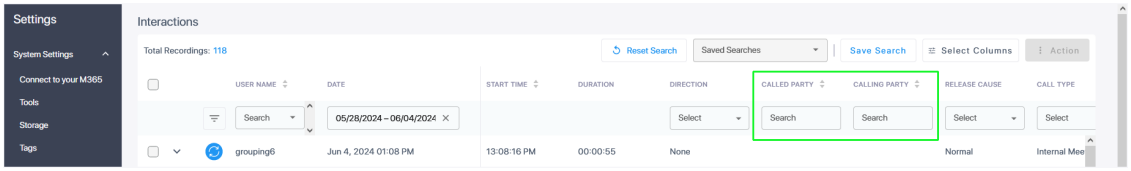


Filtering by Called or Calling Party

You can filter data by Called or Calling party.

➢ **Do the following:**

1. In the Icon pane, click either or .



2. In the Called Party or Calling Party search field, enter the name of the party to search.

   Enhance the search by specifying the Calling (Caller ID), Called and/or Answering party. Use a wild card to broaden the search

   Example

   732 will return all calls with 732 anywhere in the number

   732* will return all calls that start with 732

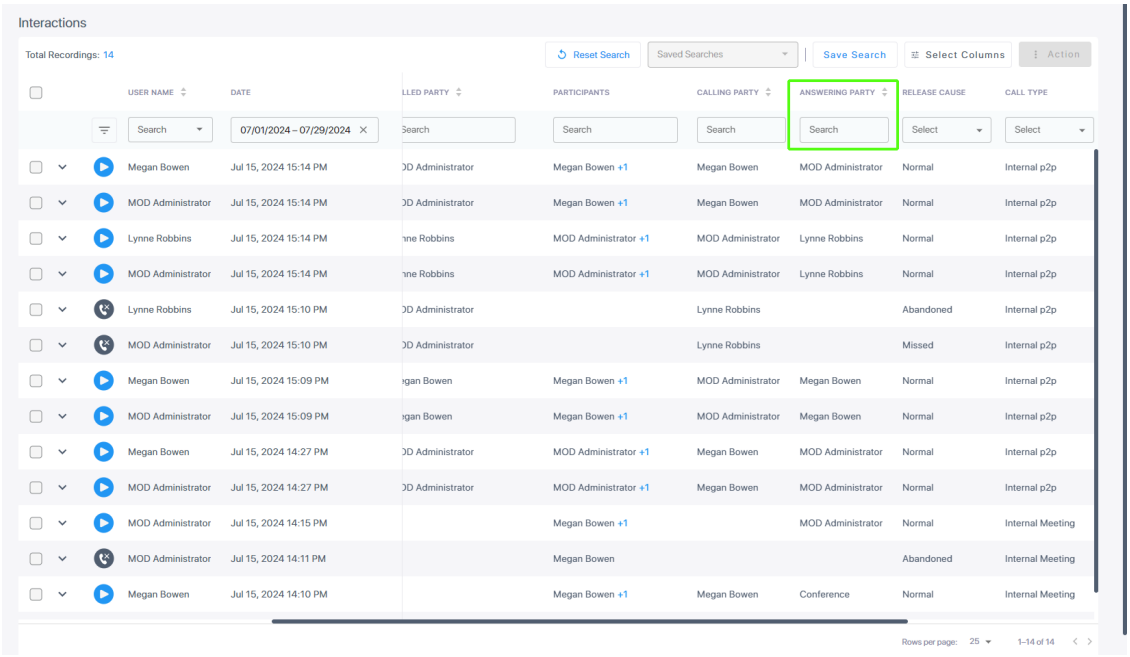
   *Bill will return all calls with a user participant with a name that contains the word 'Bill'.

Filtering by Answering Party

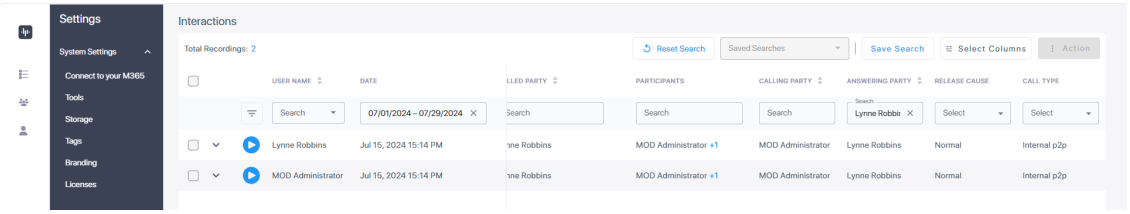
You can filter data by Answering party.

➢ **Do the following:**

1. In the Icon pane, click .



2. In the Answering party search field, start typing the name of the party to search. The filter results are shown.

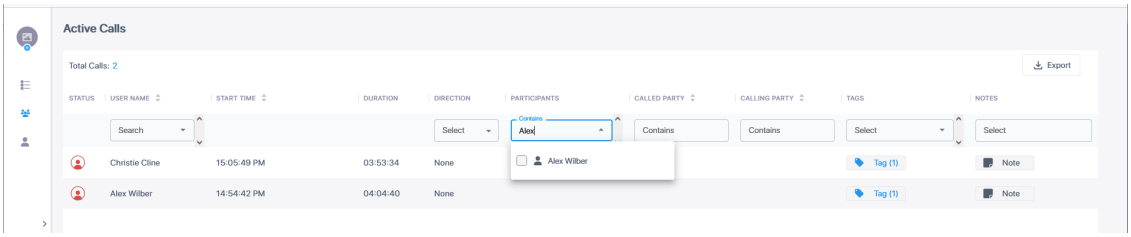


Filtering by Participants

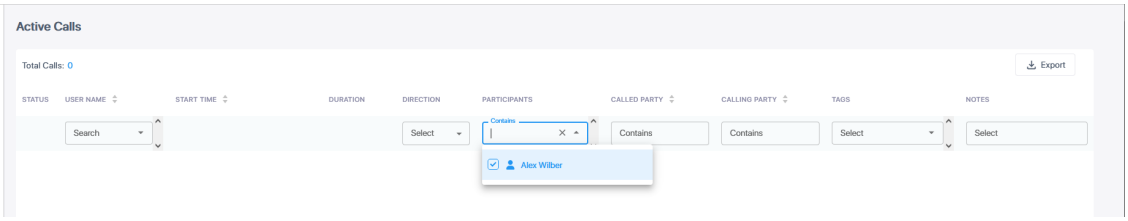
You can search by a Call participant.

➢ **Do the following:**

1. In the Icon pane, click .



2. In the Participants search field, enter the name of the participant user to search.
3. Select the entry.

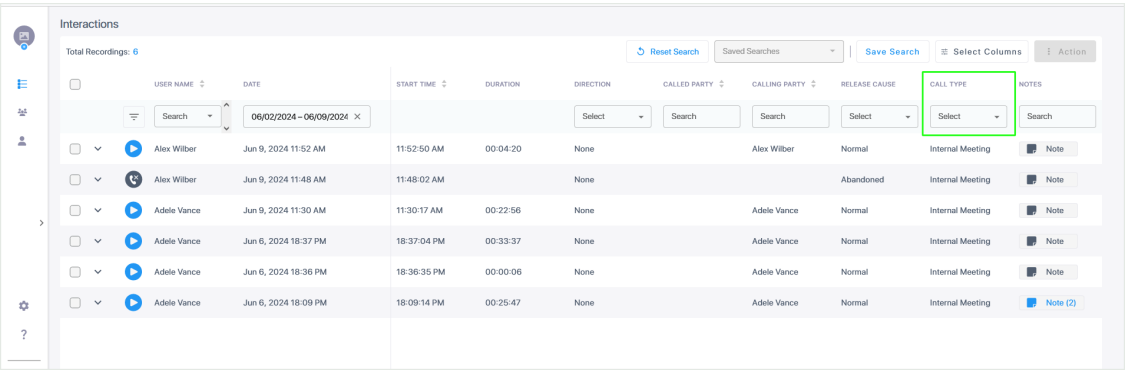


Filtering by Call Type

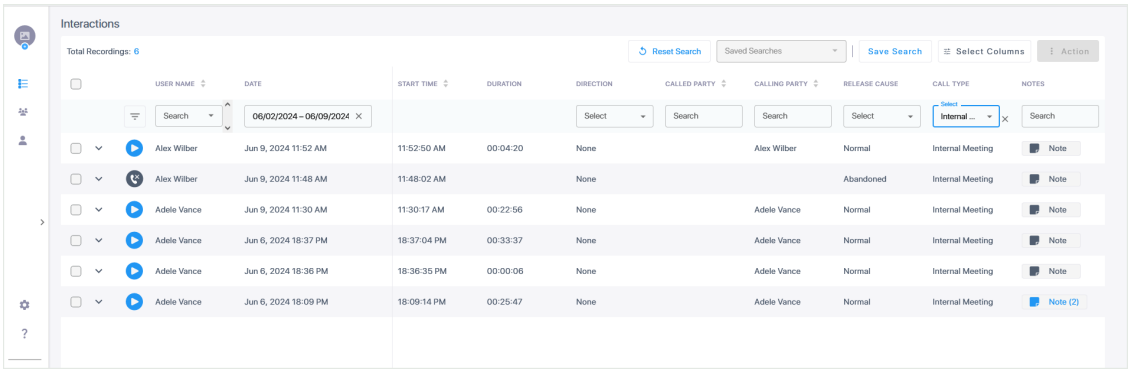
You can search by Call Type

➢ Do the following:

1. In the Navigation pane, select **Active Calls**.



2. From the Call Type drop-down list ,choose the call type to search. Select one of the following values:
   - Internal p2p: Call between two users who belong to the recorded organization domain.
   - External p2p: Call with a user that doesn't belong to the organization of the recorded/targeted user; a user from a Federated domain or any public Teams.
   - PSTN p2p: Call with a party on PSTN trunk.
   - Internal Meeting: Internal conference call
   - External Meeting: Calls with external conferences (Federated bridges)
   - Internal Meeting with External Participants: Call with internal conference that has external participants, where the external participant is a Federated user or a guest.
   - Queue Call: Name of the Queue name for calls routed from a queue.



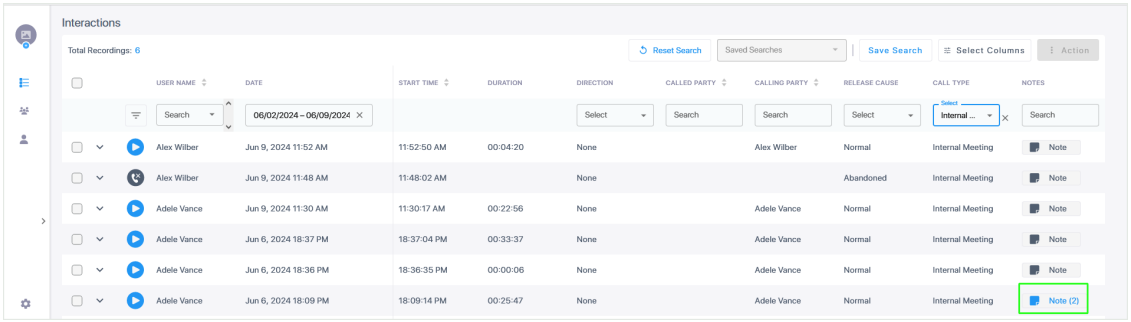
Filtering by Notes

You can search by notes that have been defined for a call.

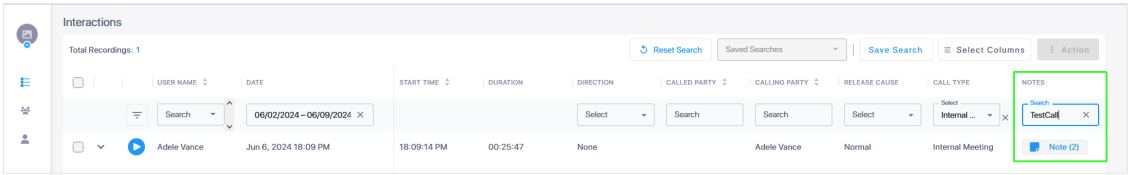
> You can only filter text strings using whole words.

➢ **Do the following:**

1. In the Icon pane, click either or .



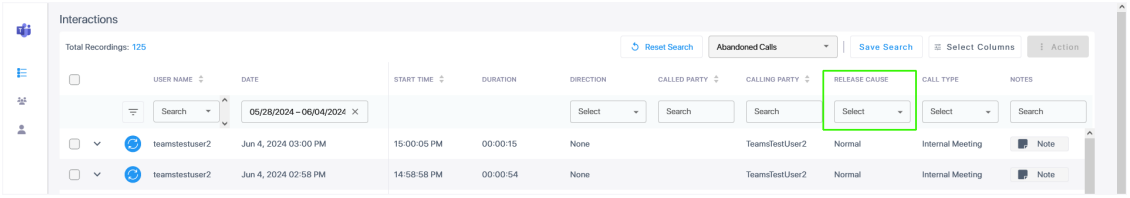
2. In the Notes field, enter text to search contained in the note. Notes containing text are indicated in blue as shown in the figure below. The number adjacent to the note icon indicates the number of notes that have been created for the interaction.



Filtering by Release Cause

➢ **Do the following:**

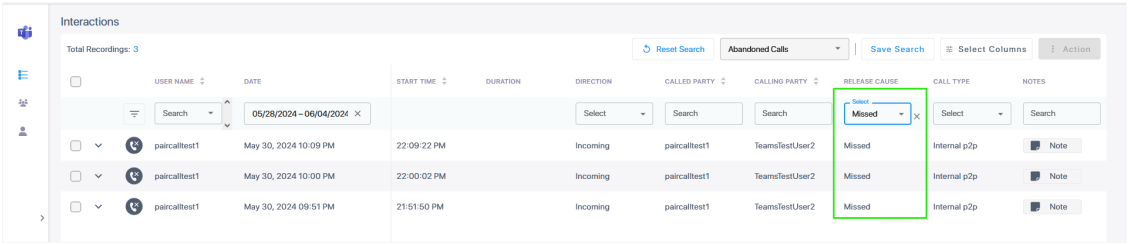
1. In the Icon pane, click .



2. From the Release Cause drop-down list, select one of the following Release Causes to filter data:

   - Normal
   - Abandoned
   - Failure
   - Missed

   In the example below, data has been filtered to retrieve "Missed Calls"

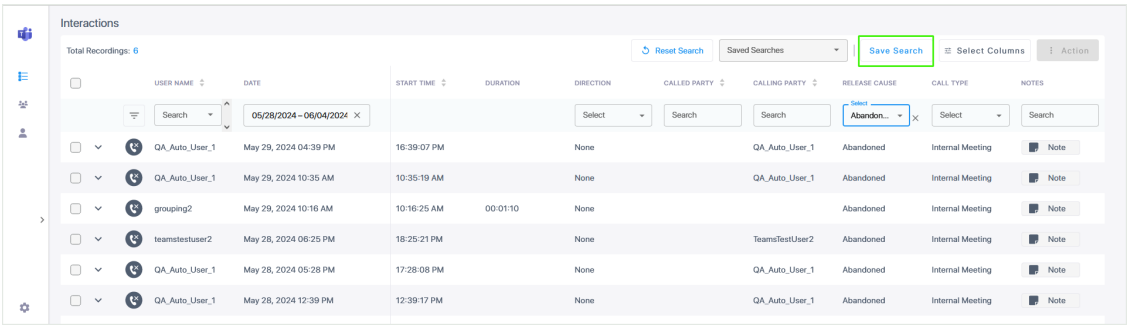


Saving Queries

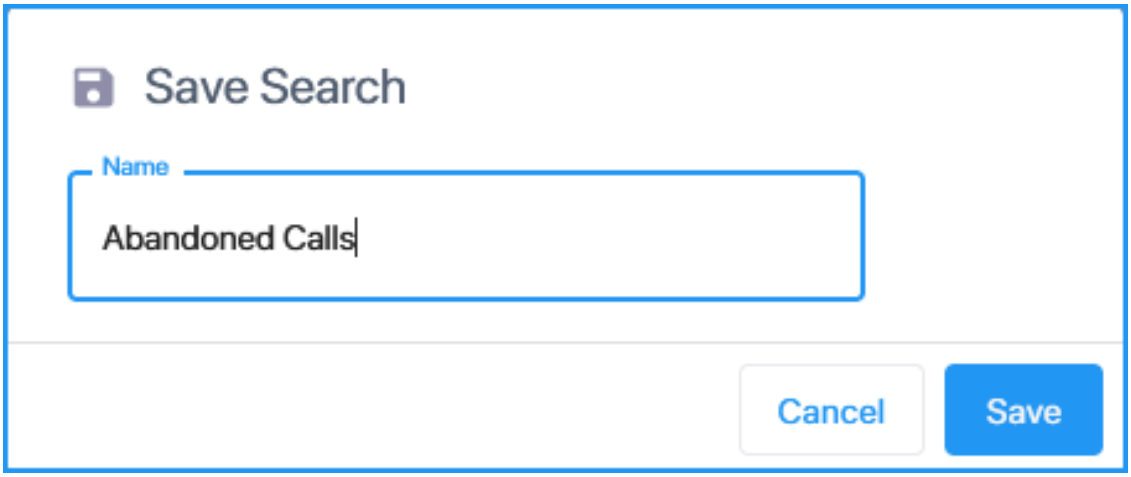
You can save search criteria as a query and then later retrieve it.

➢ Do the following:

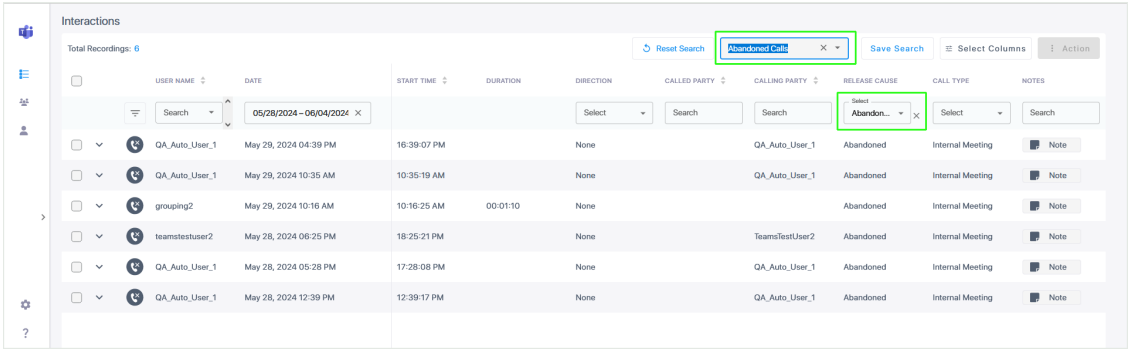
1. In the Icon pane, click .



2. Run a query using one of the filter criteria, and then select **Save Search**.



3. Enter a name for the Search result and then click **Save**.
4. You can toggle in the adjacent search box to view your saved search.



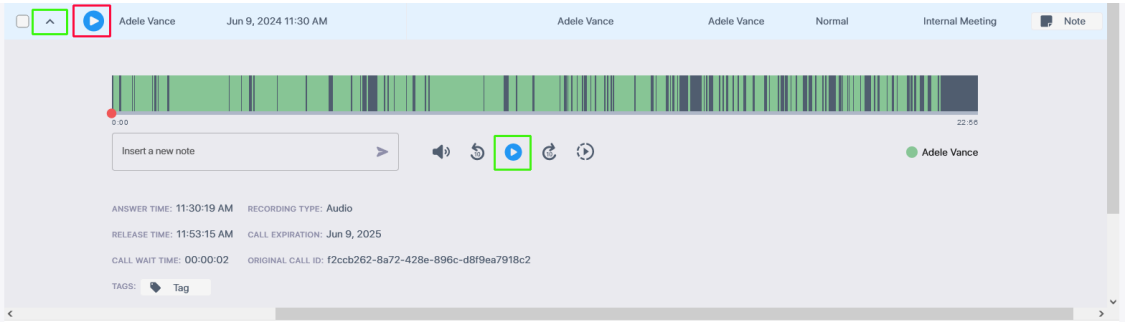
Listening to Voice Interaction

Once a voice interaction is Available, you can open the Media player and listen to it.

See also Filtering in Time line on page 116.

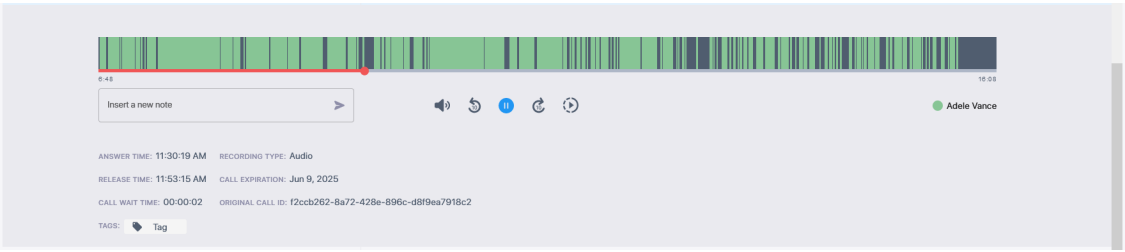
➢ **Do the following:**

1. In the Navigation pane, click **Interactions** .
2. Follow the instructions described in Filtering Interactions and Active Calls Information on page 100 to search filter for calls.
3. In the retrieved calls list, select the desired call. The call recorder is displayed with the frequency spectrum of the call.



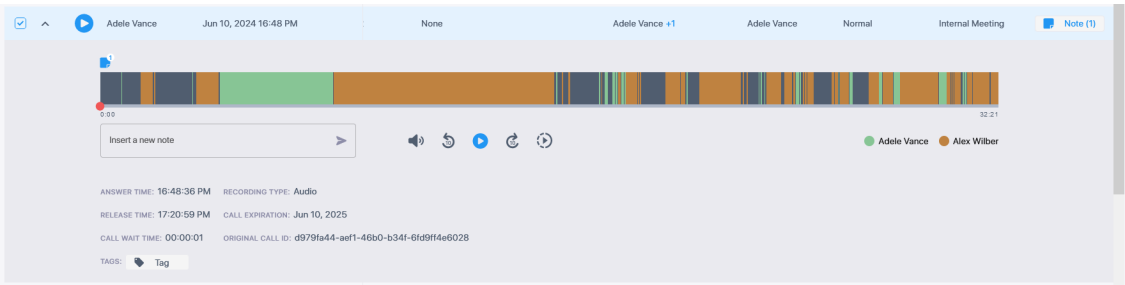
4. Click below the Media player to start listening to the call. Click again to pause while the call is playing (the button changes to) to allow the administrator to pause the player while playing the audio.

> The Play button adjacent to the name of the Caller (shown in Red in the figure above) in not functional.

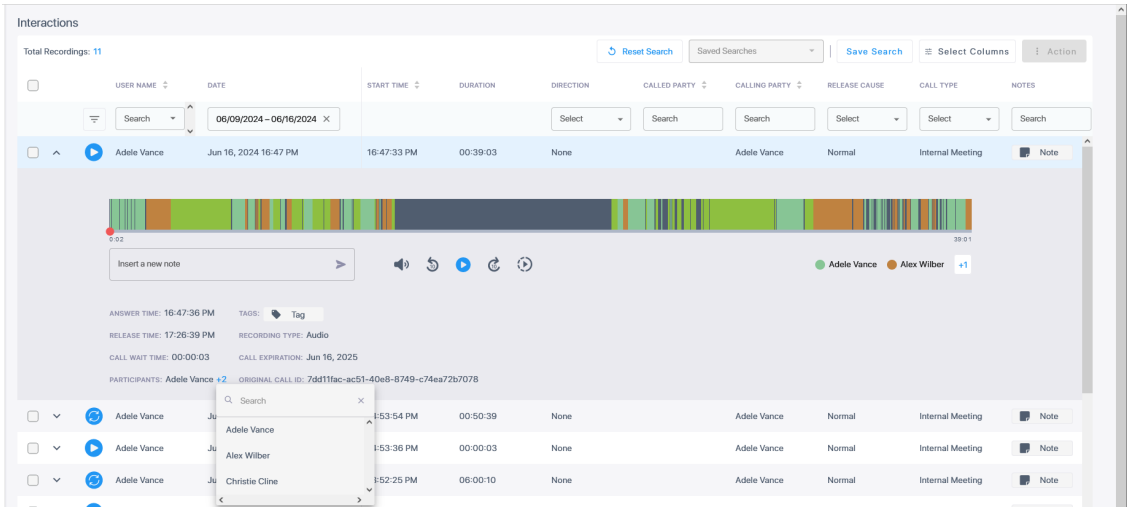


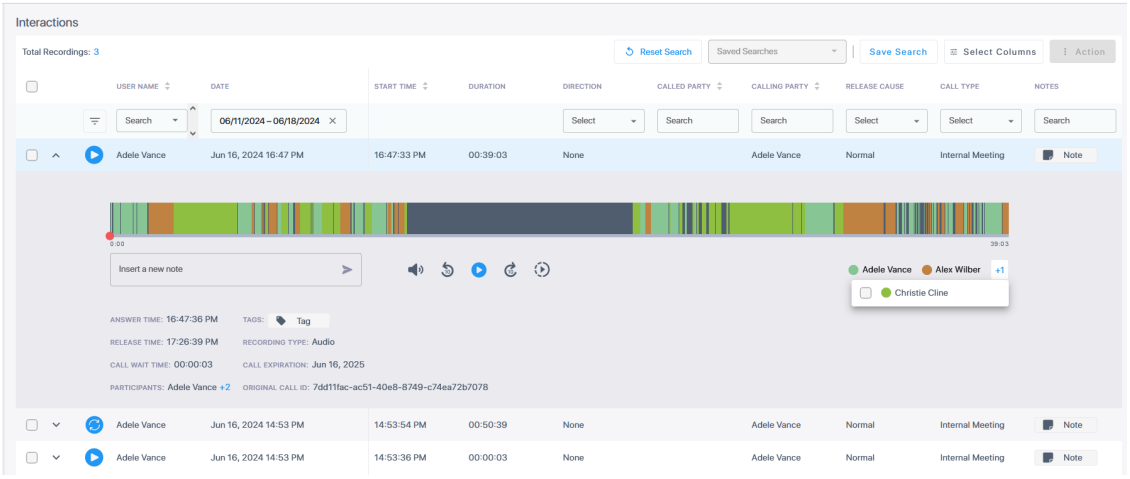
Information at the top-left hand side of the screen includes the user name, date and time and status e.g. “PLAYING”. On the top-right hand side of the screen includes the elapsed playback time and the total playing time.

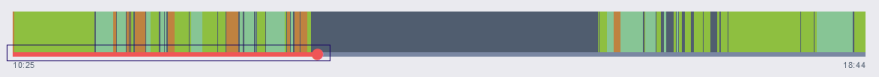
The figure below displays a call with two participants.

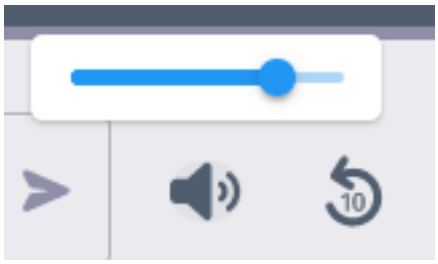
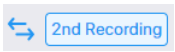


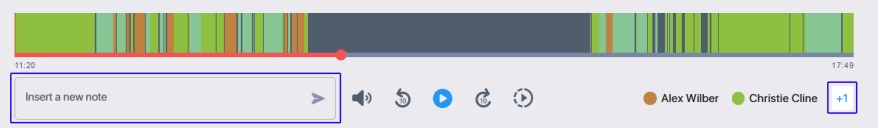
The figures below displays a call with three participants.





Field	Description
Time line	The Time line displays the call segments of the recording which are color-coded according to the speaker. In the example below, there are two participants in the call, Alex Wilber and Christie Cline.
Time line scroll bar	Drag the Time line scroll bar to the desired segment of the recording; the elapsed time is displayed below the scroll bar. 
Player Controls	

Field	Description
	Adjusts playback volume. Hover over to display the scroll bar.  Click the speaker to mute sound.
	Jumps to previous segment in the recording.
	Jumps to next segment in the recording.
	Playback speed levels: ■ .5 (slowest) ■ .75 ■ 1 (default normal speed) ■ 1.25 ■ 1.5 ■ 1.75 ■ 2 (fastest)
  	Switches between Single and Double Recording BOT applications.
Information Fields	Information Fields (see Interactions on page 94): ■ Answer Time ■ Release Time ■ Call Wait Time

Field	Description
	■ Tags (click to display tags defined for the call). ■ Recording Type ■ Call Expiration ■ Original Call ID
Notes	Insert a new note in the text box. Click the note icon to view an existing note. 

Filtering in Time line

The Time line lets you filter display according to the recorded voice of each participant. A Unique color-code is assigned to each participant where the colored segment indicates the voice recorded for the participant.

➢ To filter in the Time line:

1. Under the Time line, click the name of the participant whose recorded segments you wish to view.
2. If the interaction includes three or more participants, click the +<number of additional participants> link and then select the check box is the speaker to view their recorded segments.

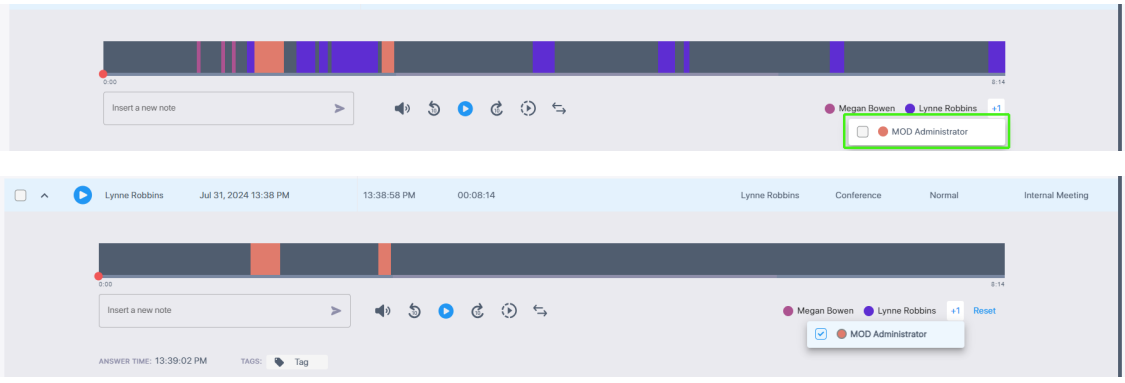


Figure 5-1: Recorded Segments for Lynne Robbins

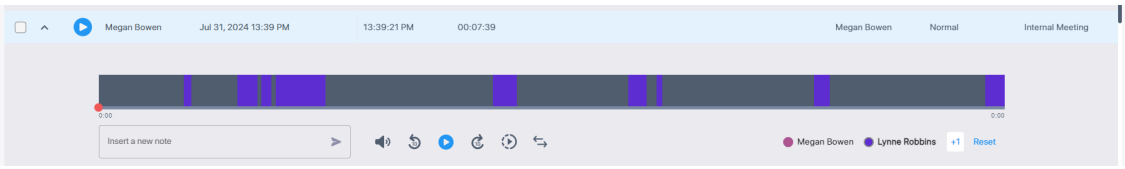
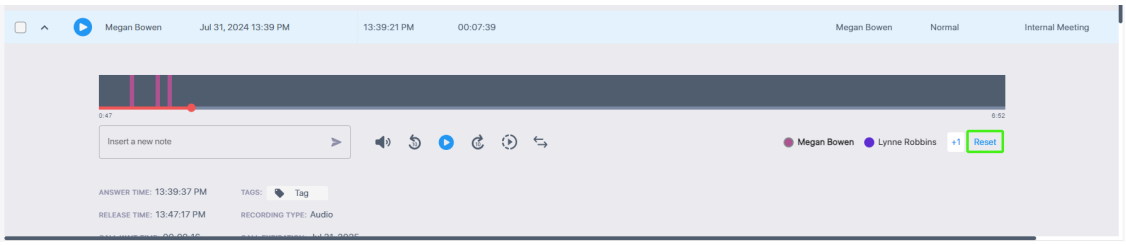
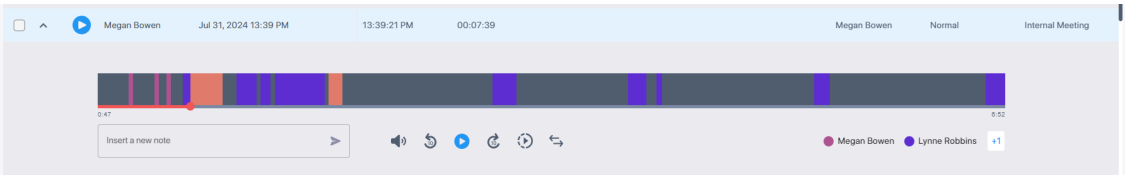


Figure 5-2: Recorded Segments for Megan Bowen



3. Click **Reset** to display recorded segments for all participants.

Figure 5-3: Recorded Segments for All Participants

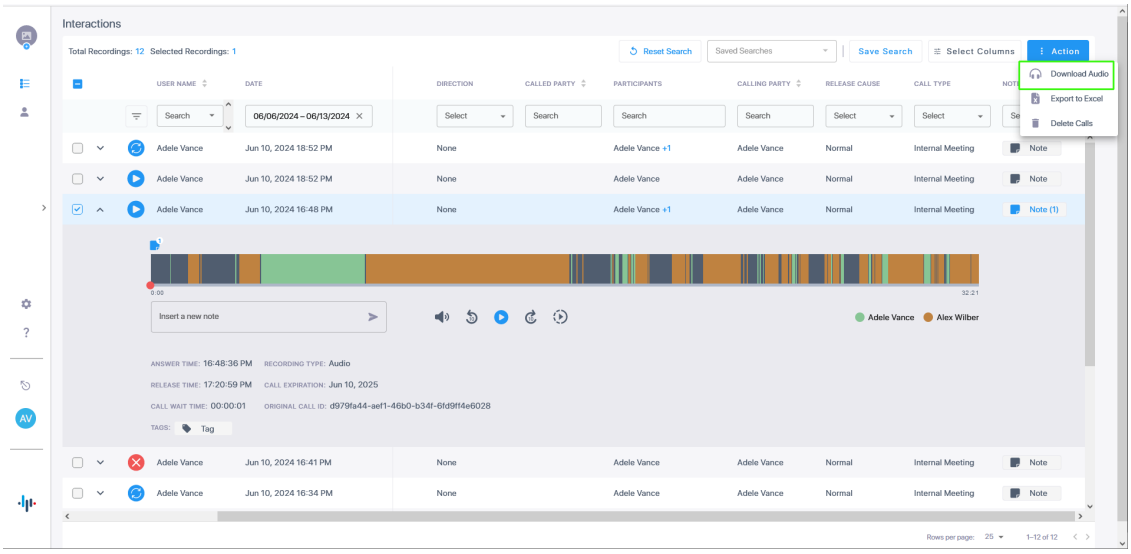


Downloading an Audio Call

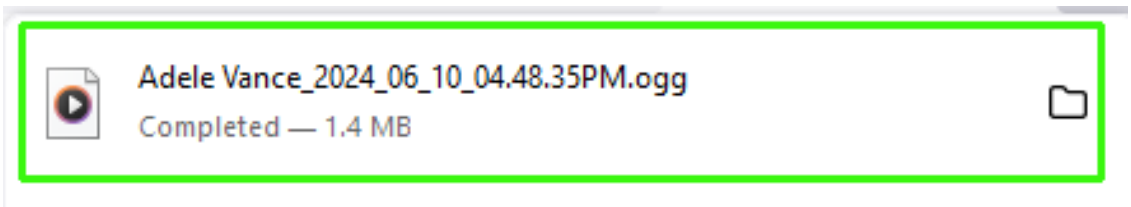
You can download an audio call. The file is downloaded in **.ogg** format.. Calls can be downloaded one at a time.

➢ To download an audio call:

1. In the Interactions page, select the check box adjacent to the call that you wish to download.



2. From the Action menu, choose **Download Audio**.



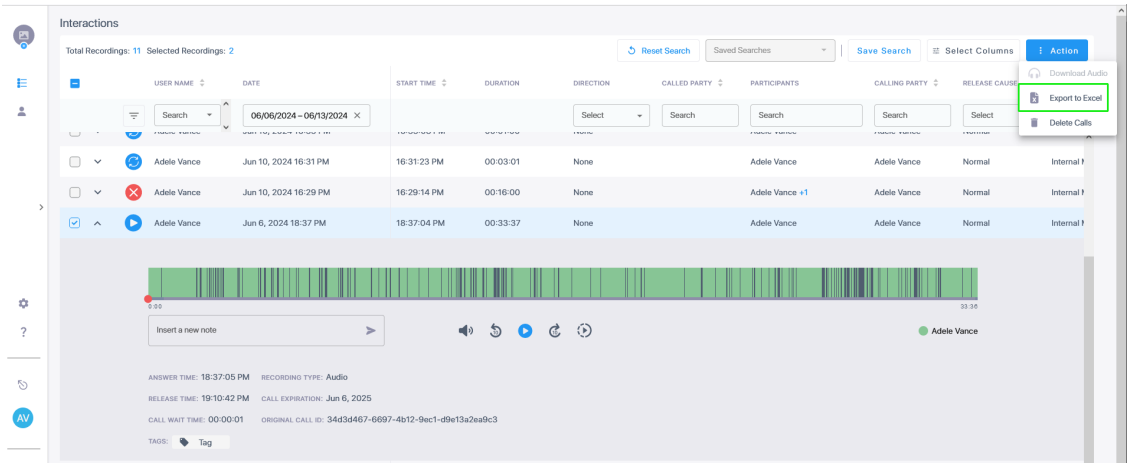
An **.ogg** file is downloaded.

Exporting Interaction to Excel

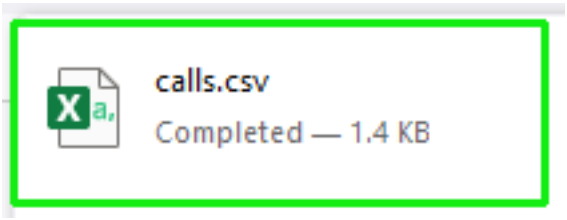
You can export an interaction to an Excel file.

➢ To export a call:

1. In the Icon pane, click .
2. Select the check box adjacent to the call that you wish to export.



3. From the Actions drop-down list, choose **Export to Excel**. A .csv file is downloaded.




```
Report Header

Requested By    Adele Vance

Created At    2024-06-13T10:08:05.058Z


Call Id    Target Display Name    Target
Upn    OnBehalfOf    TransferredBy    TransferredTo    Called
Party    Calling Party    Answered By    Answered time    Start
Time    Release Time    SipCallId    SysCallId    Call Direction    Call
Type    Release Cause    Notes    Participants    Files    Media Audio
Status    Expiration    QueueName    DoubleRecordingType    PairedCall    T
```

```
ags    Call Link

6661d7a0dd2ca9b8cf1f0879    AdeleV@M365x21689653.OnMicrosoft.com    AdeleV@
M365x21689653.OnMicrosoft.com                    Adele
Vance    Conference    2024-06-06T15:37:05.617Z    2024-06-
06T15:37:04.000Z    2024-06-06T16:10:42.667Z    e31f6000-c738-46c1-b1a0-
3eaa4bc415cf    34d3d467-6697-4b12-9ec1-d9e13a2ea9c3    None    Conference_
Internal    Normal        Adele Vance    e31f6000-c738-46c1-b1a0-
3eaa4bc415cf_05_6166.opus    Available    2025-06-
06T15:37:04.000Z        Primary            https://stngqa.ai-
logix.net/ui/interactions/6661d7a0dd2ca9b8cf1f0879

66670433055f2769a12f2019    AdeleV@M365x21689653.OnMicrosoft.com    AdeleV@
M365x21689653.OnMicrosoft.com                    Adele
Vance    Conference    2024-06-10T13:48:36.867Z    2024-06-
10T13:48:35.000Z    2024-06-10T14:20:59.056Z    6a1f5c00-ff9c-41dd-aabd-
0ec1d2232efd    d979fa44-aef1-46b0-b34f-6fd9ff4e6028    None    Conference_
Internal    Normal    Call with Alex    Adele Vance;Alex Wilber    6a1f5c00-
ff9c-41dd-aabd-0ec1d2232efd_36_8665.opus    Available    2025-06-
10T13:48:35.000Z        Primary            https://stngqa.ai-
logix.net/ui/interactions/66670433055f2769a12f2019
```

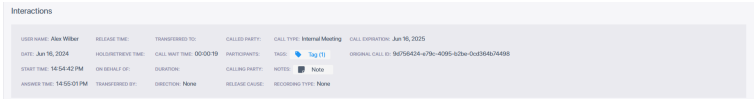
The following shows an exported interaction for a Conference call between two participants.

```
Call Id    Target Display Name    Target
Upn    OnBehalfOf    TransferredBy    TransferredTo    Called
Party    Calling Party    Answered By    Answered time    Start
Time    Release Time    SipCallId    SysCallId    Call Direction    Call
Type    Release Cause    Notes    Participants    Files    Media Audio
Status    Expiration    QueueName    DoubleRecordingType    PairedCall    T
ags    Call Link

666eed2e2a44e64a82cda43a    AlexW@M365x21689653.OnMicrosoft.com    AlexW@M3
65x21689653.OnMicrosoft.com                    Alex Wilber    2024-06-
16T13:48:49.381Z    2024-06-16T13:48:30.343Z    2024-06-
16T14:27:01.034Z    1-8692352b214e4a418aaea352fd63fd35-
2024061613483034    7dd11fac-ac51-40e8-8749-
c74ea72b7078    None    Conference_Internal    Normal    Sales Meeting;
Sales feedback    Adele Vance;Alex Wilber;Christie Cline    de1f5c00-ce35-
4e78-a89f-e02e6ee28165_30_3438.opus    Available    2025-06-
16T13:48:30.343Z        Primary        Help Desk    https://stngqa.ai-
logix.net/ui/interactions/666eed2e2a44e64a82cda43a

66744b879f40fd53de91e70e    AdeleV@M365x21689653.OnMicrosoft.com    AdeleV@
M365x21689653.OnMicrosoft.com                    Adele
Vance    Conference    2024-06-20T15:32:25.266Z    2024-06-
20T15:32:23.000Z    2024-06-20T16:16:22.014Z    761f5c00-da6f-4283-8c58-
c25f349f167f    cd05e4fb-b37b-4843-a1c2-36413f6fcad0    None    Conference_
Internal    Normal        Adele Vance;Alex Wilber    761f5c00-da6f-4283-
8c58-c25f349f167f_25_2654.opus    Available    2025-06-
20T15:32:23.000Z        Primary            https://stngqa.ai-
logix.net/ui/interactions/66744b879f40fd53de91e70e
```

The table below describes the fields in the exported data record.

Field	Description
Call Id	Unique call id
Target Display Name	The M365 username of the targeted user.
Target Upn	The M365 username of the targeted user.
OnBehalfOf	The name of the party for whom the call was transferred.
TransferredBy	The name of the party who transferred the call.
TransferredTo	The name of the party to whom the call was transferred.
Called Party	The M365 user receiving the call.
Calling Party	The M365 user initiating the call.
Answered By	The party who answered the call.
Answered time	The time that the call was answered.
Start Time	The time when voice recording commenced.
Release Time	The time the call was released.
SipCallId	The SIP CallId passed in the SIP Header.
SysCallId	Indicates the ID used to identify the call (also known as 'Original Call ID'). This value may be either the original call id or scenario id (Teams). For example, when recording a Teams call between user A and B the id of the call between A and B is displayed. This ID is also displayed in the Teams CDR.
Call Direction	Incoming or Outgoing
Call Type	Indicates the type of the call. One of the following values: ■ Internal Meeting ■ External Meeting ■ Internal Meeting with External Participants

Field	Description
	■ Externalp2p ■ PSTN p2p
Release Cause	Indicates the reason why a call is disconnected. One of the following values: ■ Normal – the call was answered and then released. ■ Failure – the call or recording was stopped due to an error. ■ Missed – the Targeted user didn't answer an incoming call. ■ Abandoned – the Targeted user made an outgoing call and hanged up before the call was answered ■ Transferred – the call was transferred to another call.
Notes	Option to add notes to the Interaction record (see Adding Notes to Interactions on page 129).
Participants	The names of the call participants.
Files	This field is currently not supported.
Media Audio Status	One of the following values: ■ Available: The interaction is available for playback. ■ Pending: The interaction is pending database synchronization. ■ Recording: The Interaction is currently being recorded. ■ Failed: The SmartTAP failed. ■ Unavailable: The recording is unavailable. ■ Deleted: The recording has been deleted.
Expiration	Indicates the date that the call recording is purged as defined in the Recording profile.
QueueName	Teams Queue Call Instance ID when configured in the Recording profile.
DoubleRecordingType	Indicates whether Essentials (Single Recording Audio License) or Pro (Double Recording Audio &Redundancy license) is configured for the service.
PairedCall	Indicates whether Geographical Redundancy Storage is enabled

Field	Description
	in a paired region for data disaster recovery (enabled by default when a Pro License is configured for the service).
Tags	Names of any tags assigned to the calls.
Call Link	Opens a summary of the call details with the Call Id in the URL . For example https://stngqa.ai-logix.net/ui/interactions/666ed2822a44e64a82cda302 

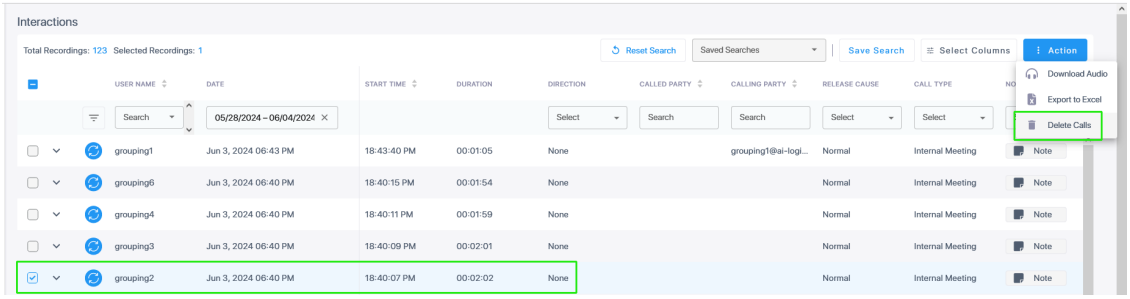
Deleting Calls

AudioCodes Live SmartTAP is deployed in several recording scenarios such as compliance, quality monitoring and for malicious call recordings. While regulatory compliance requires that recordings are deleted automatically after a regulated time frame, quality monitoring scenarios requires the ability to manually delete recordings. Consequently, calls can be deleted on demand by users with the appropriate permissions in security profiles (see Managing Security Profiles).

- This feature is enabled through the SmartTAP 360° Call Deletion license (SW/SMTP/CALLDEL).
- If a user in on Legal Hold, their Calls cannot be deleted (see Managing Users).
- When calls are deleted, any associated evaluations are also deleted.

➢ To delete calls:

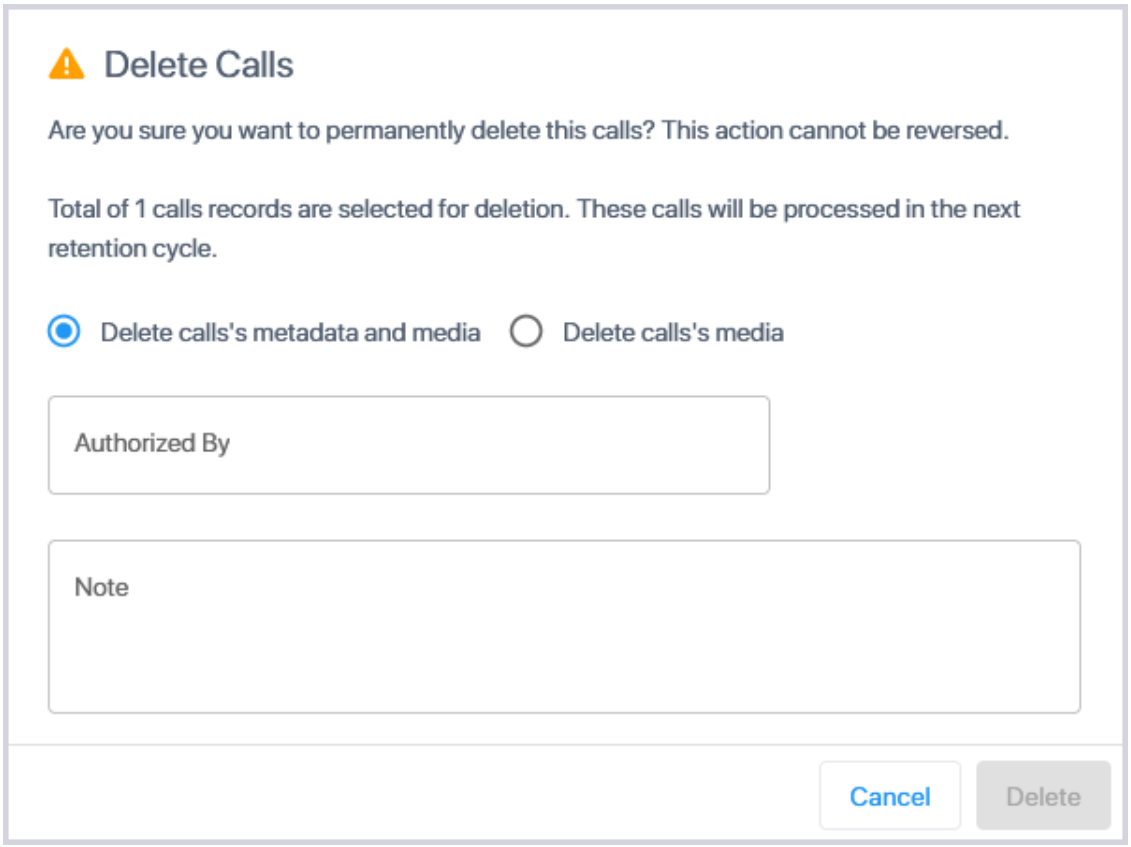
1. Search for calls according to desired search criteria (see Filtering Interactions and Active Calls Information on page 100).

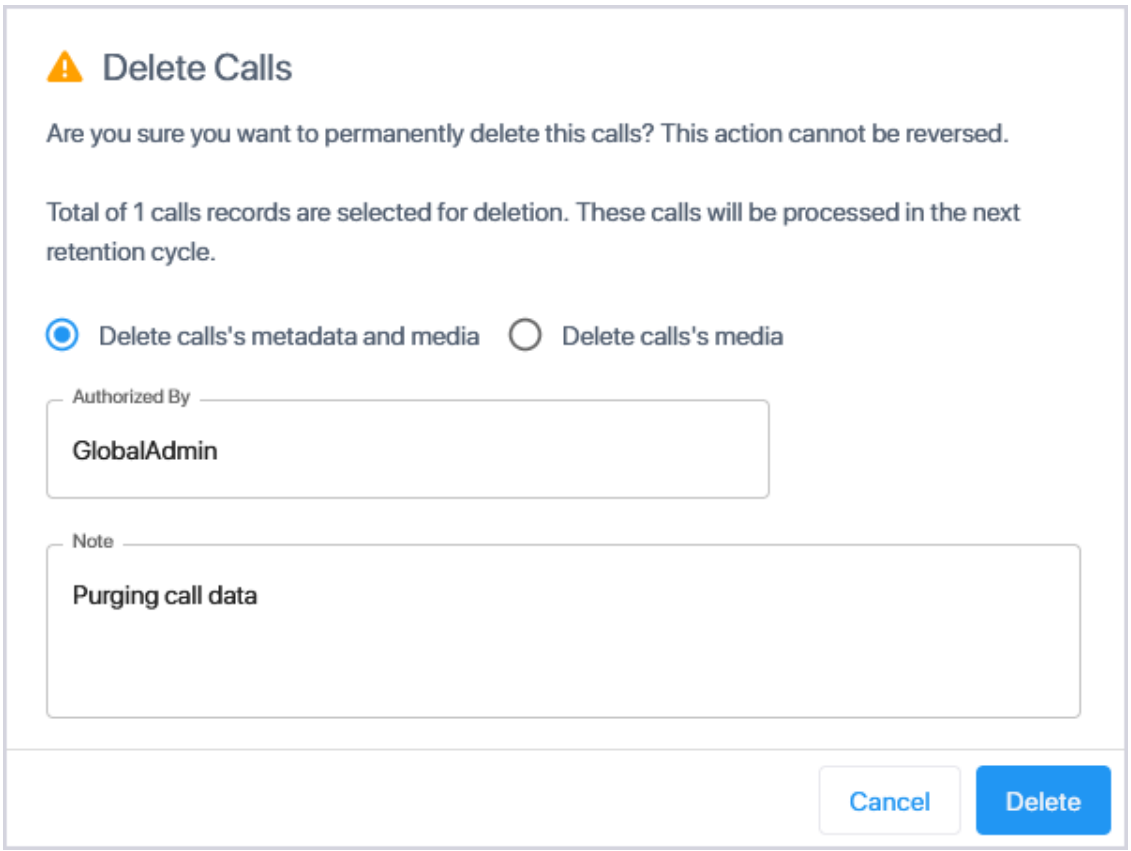


2. Select the check box adjacent to each call that you wish to delete.

Only the filtered and selected recordings are deleted.

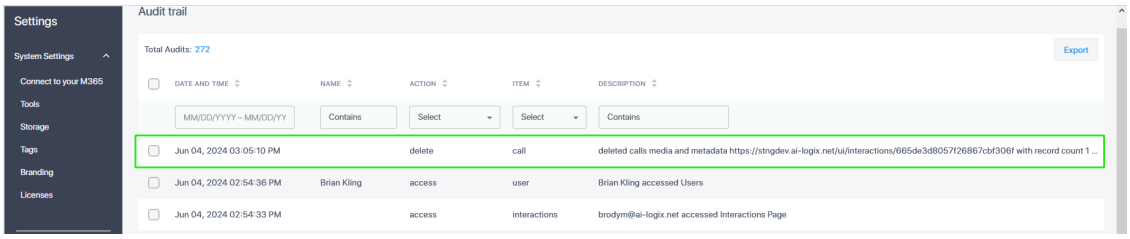
3. From the Action drop-down list, select **Delete Calls**.





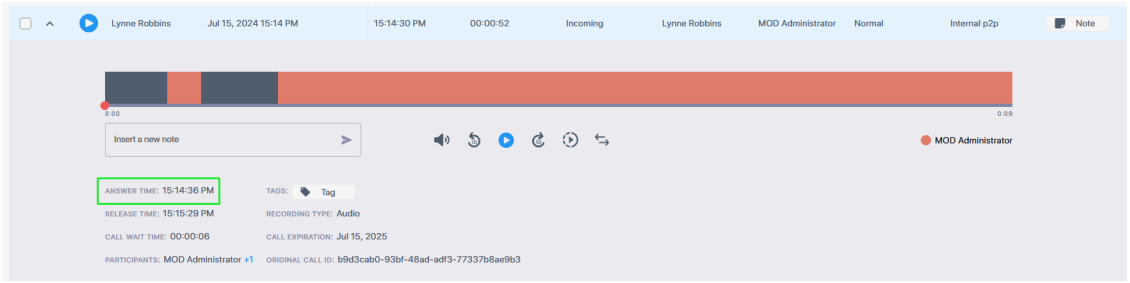
4. Select **Delete call's metadata and media** to delete both call metadata and media or select **Delete call's media** to delete only media.

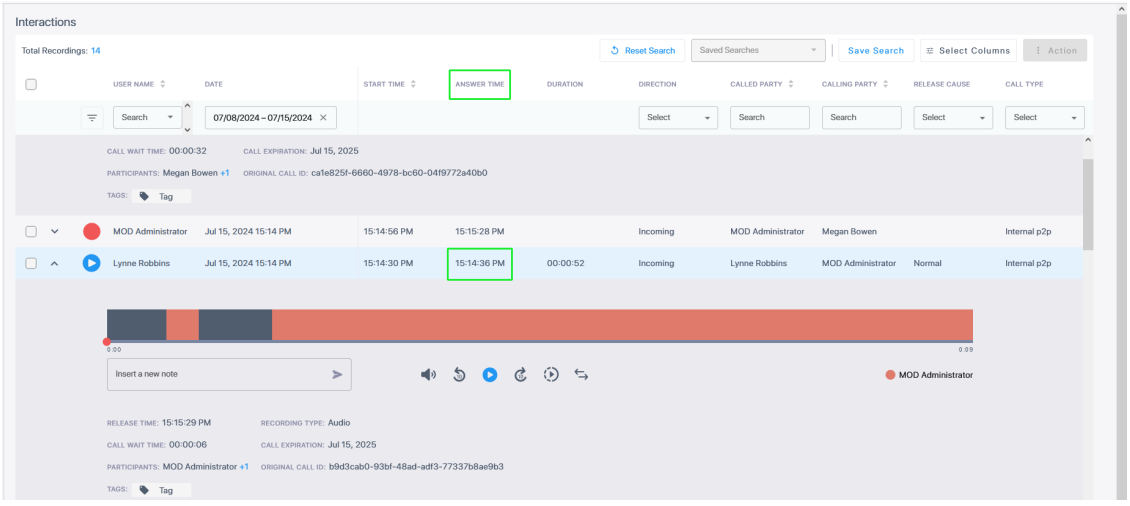
5. In the Authorized By text box, enter the name of the operator approving the action.
6. In the Note text box, enter free text describing the reason for the delete, and then click **Delete**.
7. Open the Audit Trails page to monitor the deletion process.



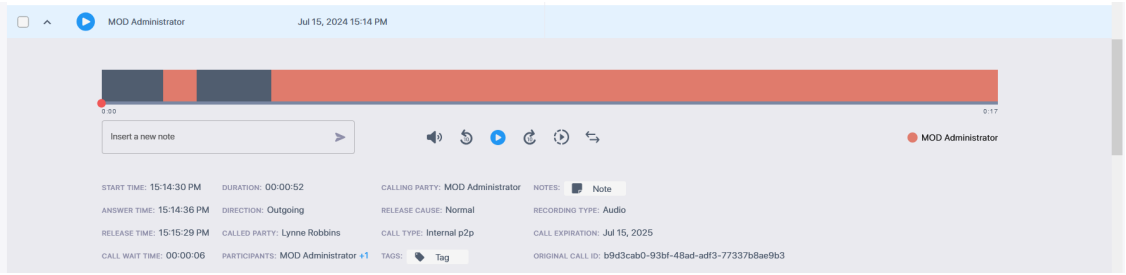
Customizing Columns

You can customize the columns that are displayed to remove clutter and optimize the page display according to analysis requirements. Displaying and hiding columns affects whether the same information is displayed below the Call Time line. In the example below, the 'Answer Time' is shown below the Time line; however, once the 'Answer Time' column is enabled, the 'Answer Time' data column is displayed, and this data is removed from the Time line display.



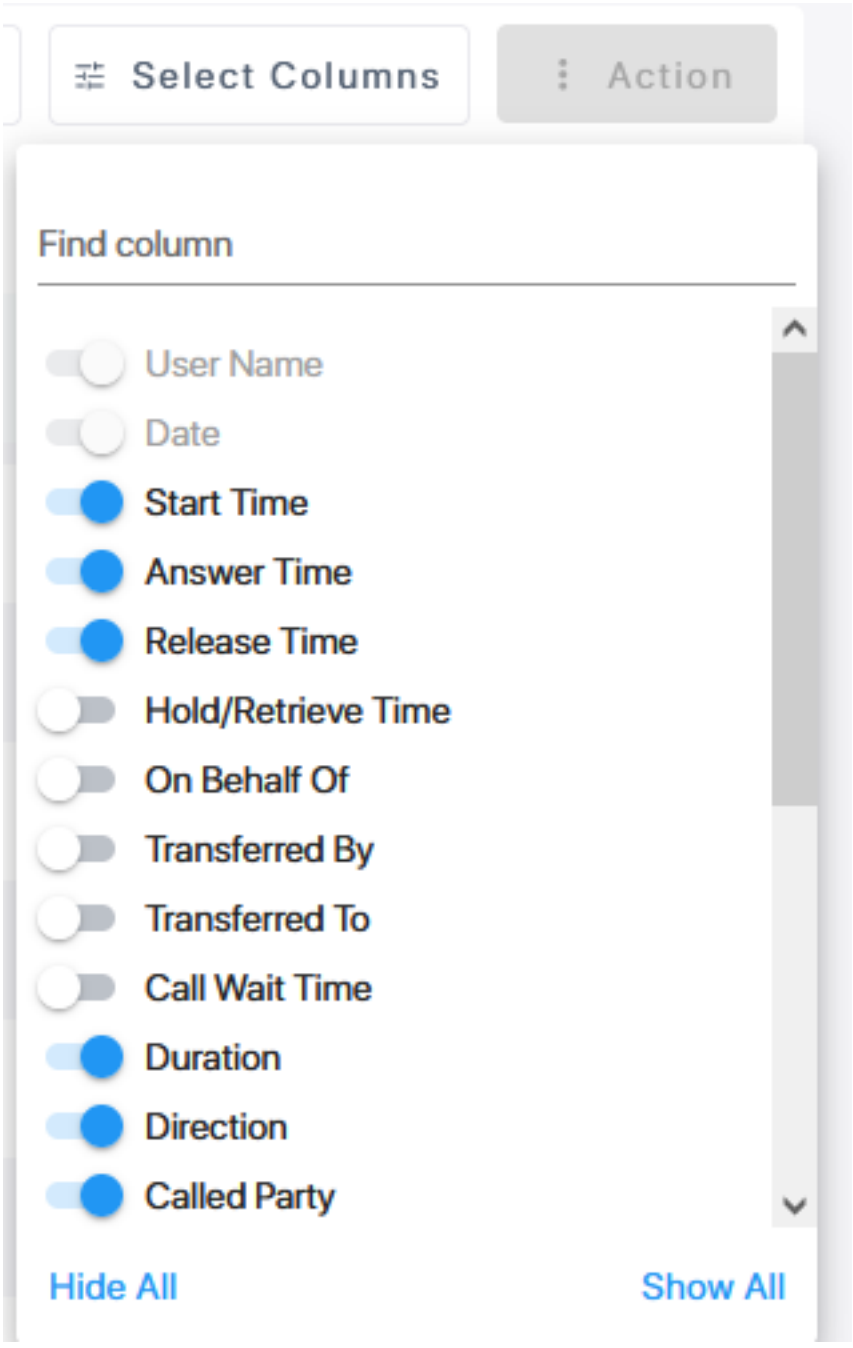


The following list displays the maximum number of parameters that are displayed under the Time line (when all columns are disabled).



➢ To customize columns:

1. In the Toolbar, select **Select Columns**.



2. Slide the roller to the right adjacent to the column that you wish to display.

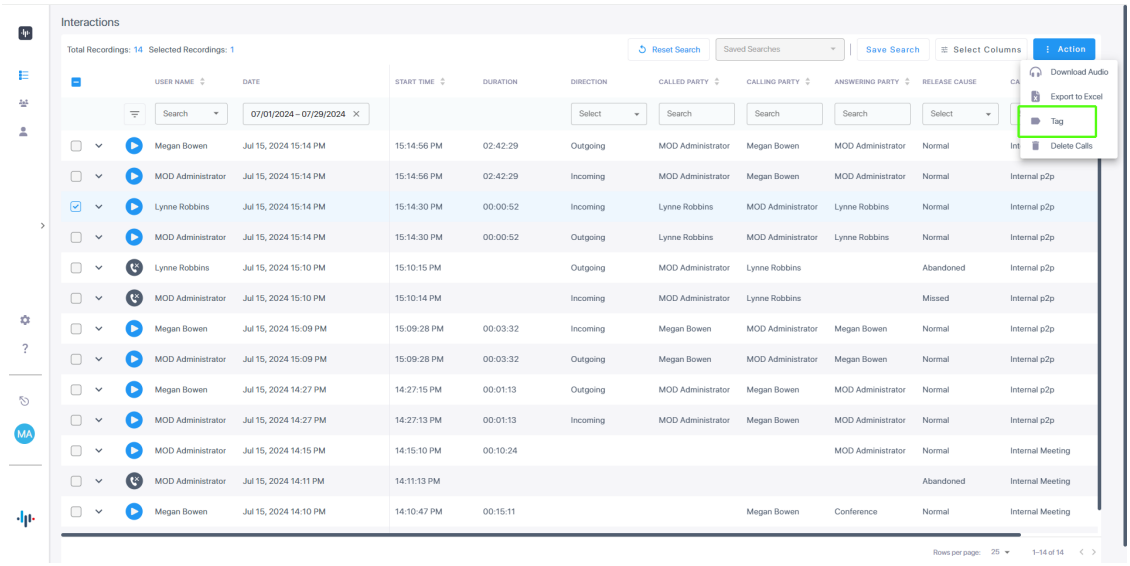
3. Slide the roller to the left adjacent to the column that you wish to hide.

Assigning Tags to Interactions

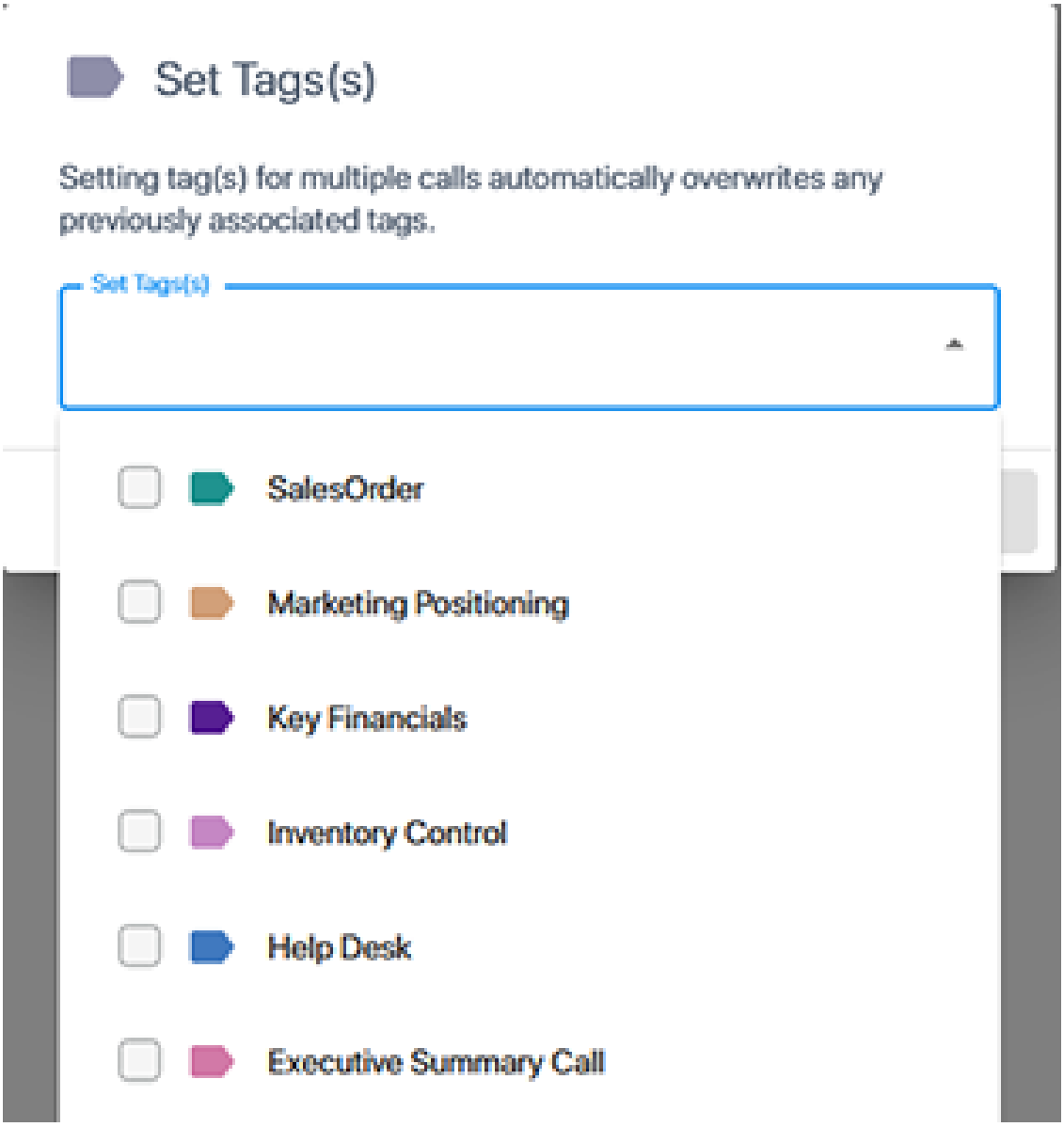
You can assign tags to Interactions, where the tag serves as a reminder or keyword that can be later used to retrieve the call details and for segmentation in interaction analysis.

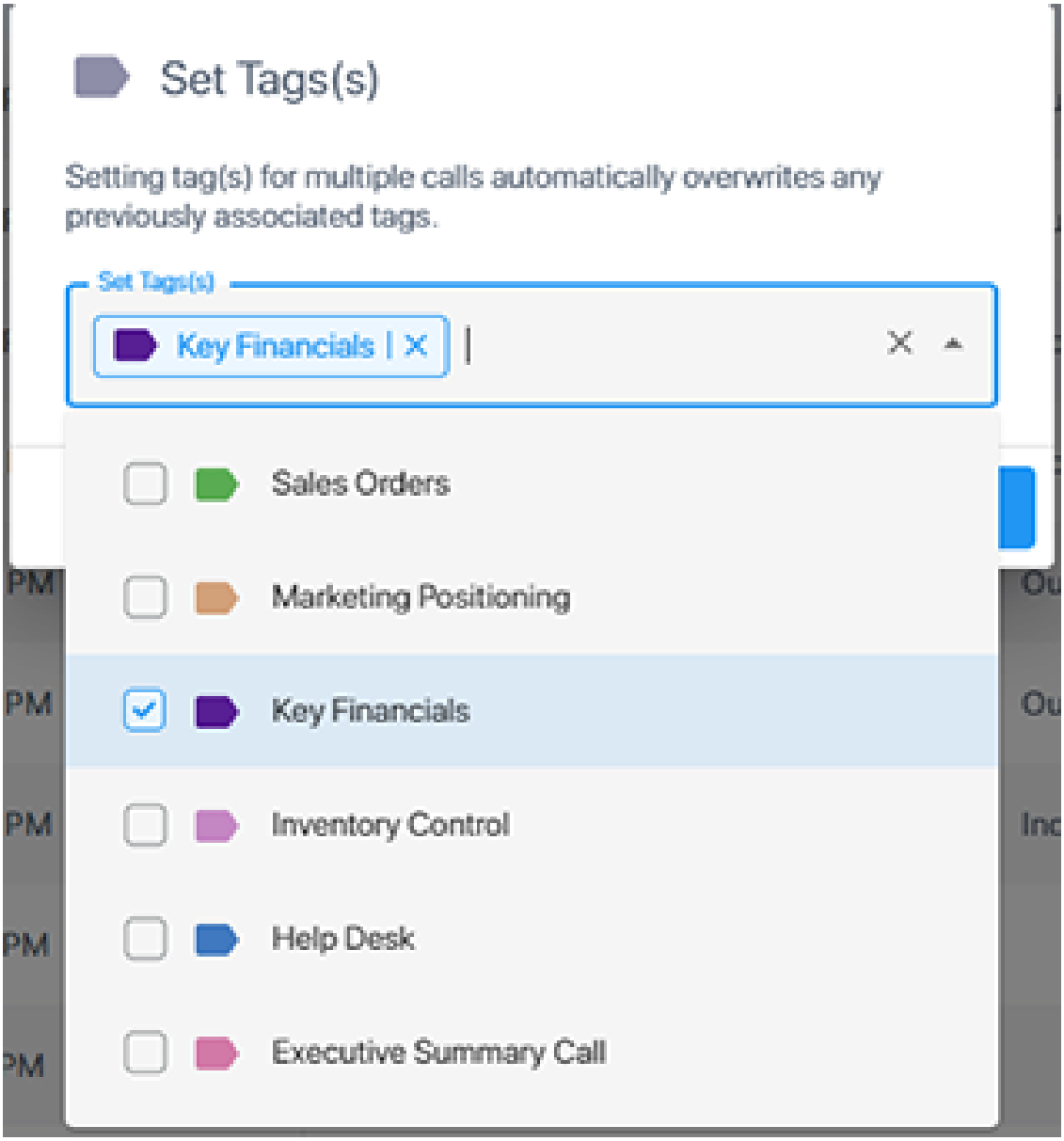
To assign tags:

1. In the Icon pane, click .
2. Select the check box adjacent to the interaction that you wish to tag.
3. From the Action drop-down list, choose **Tag**.

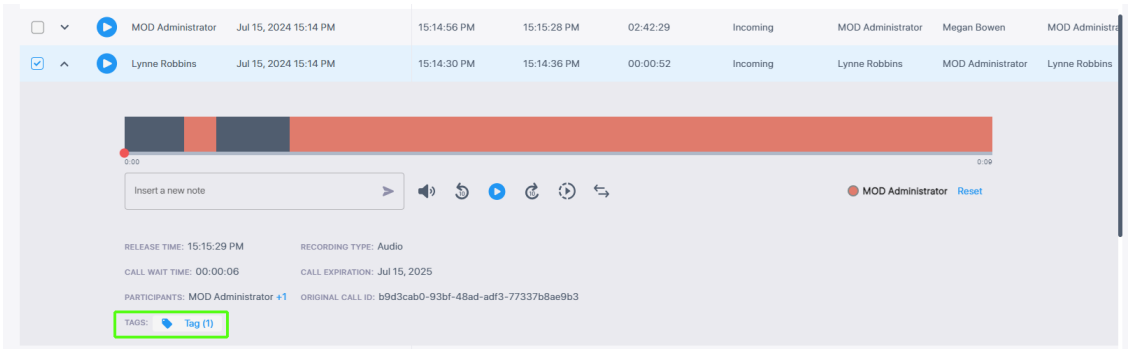


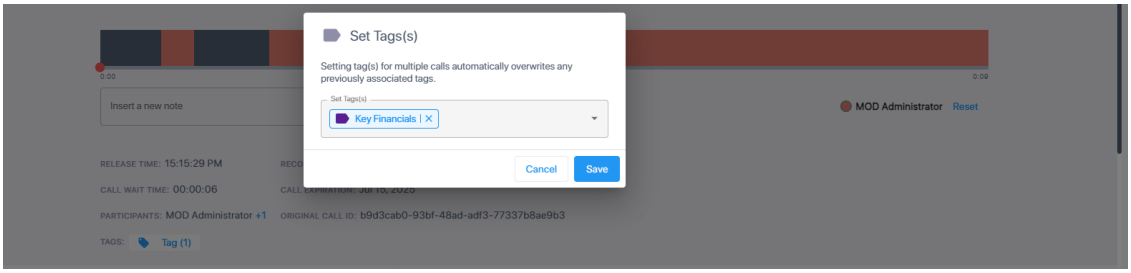
4. From the Set Tags drop-down list, select the check box adjacent to the tag that you wish set.


Set Tags(s)
Setting tag(s) for multiple calls automatically overwrites any previously associated tags.
Set Tags(s)
SalesOrder
Marketing Positioning
Key Financials
Inventory Control
Help Desk
Executive Summary Call



5. Click **Save**.
6. Open the Time line for the interaction. Notice the link to the tag that you just added.



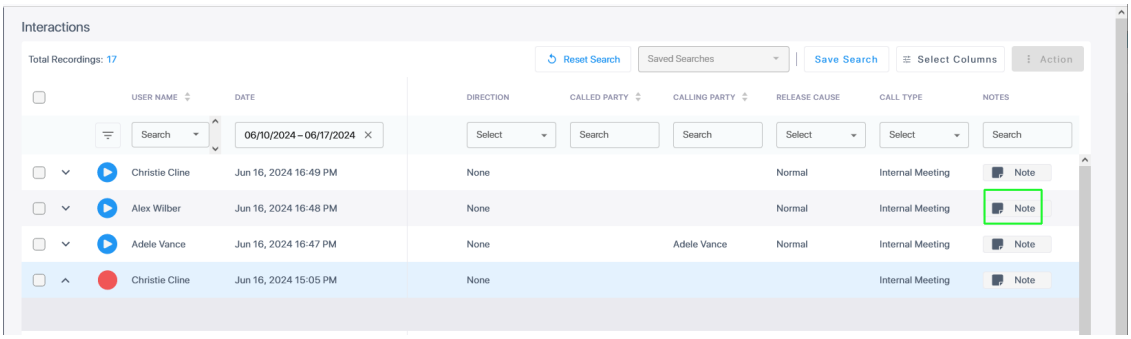


Adding Notes to Interactions

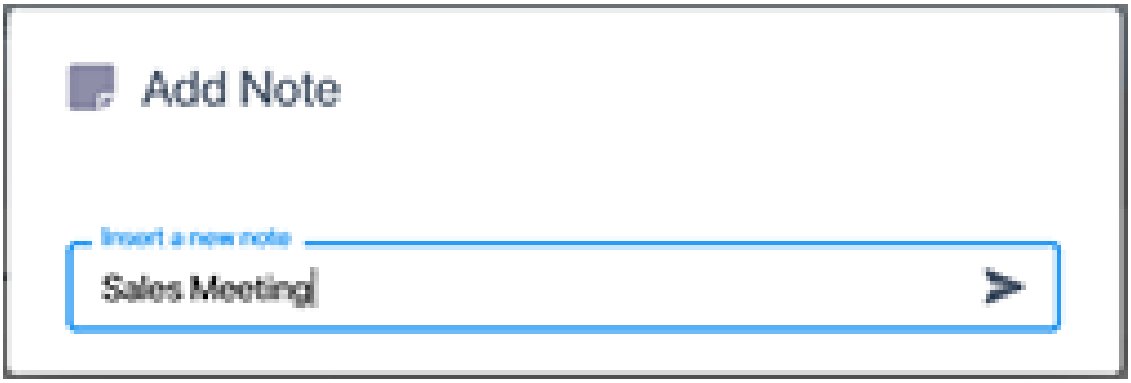
You can attach notes to Interactions containing any text or keywords that may later assist to identify the interaction when specifying search criteria (see Filtering Interactions and Active Calls Information on page 100).

➢ To add notes:

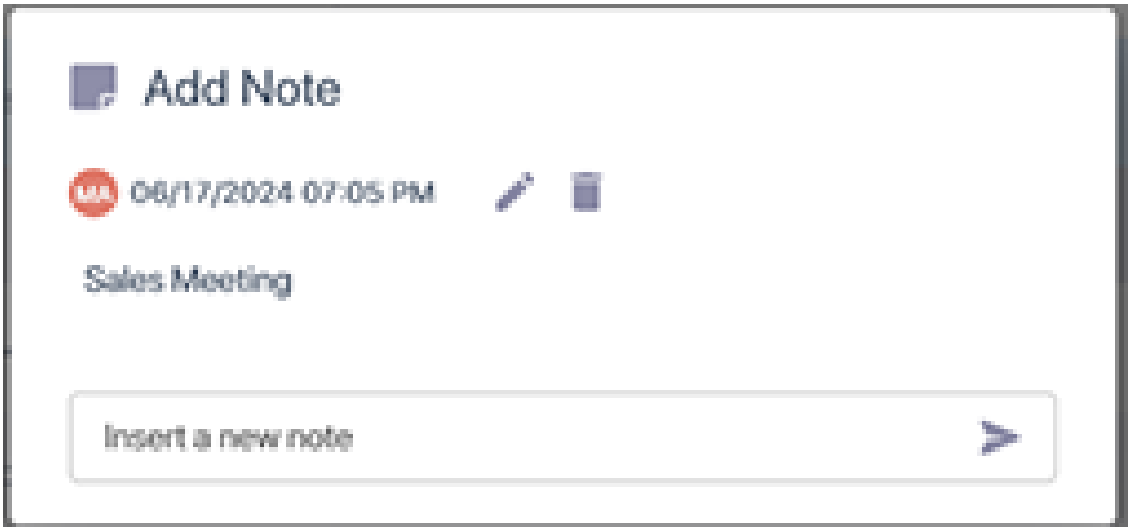
1. In the Icon pane, click , and then click the note icon adjacent to the interaction for which you wish to attach a note.



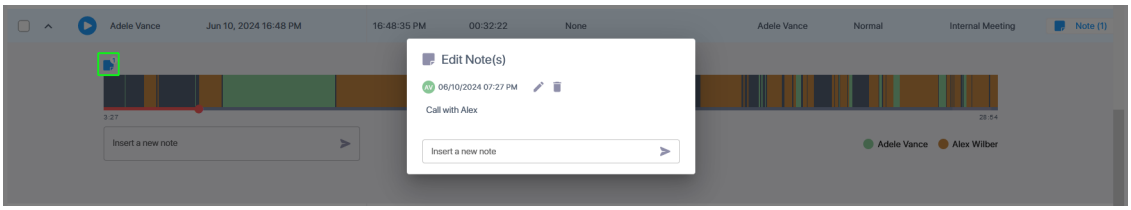
2. Click the arrow adjacent to the note text that you entered.



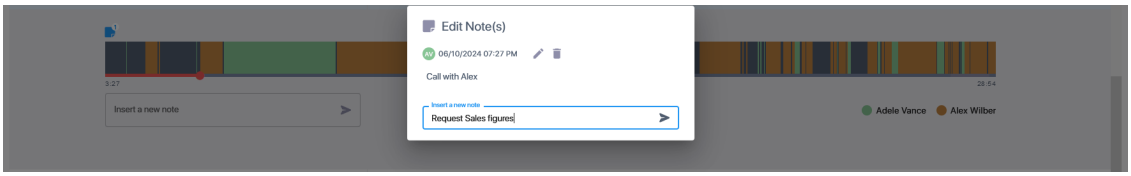
The new note is added.



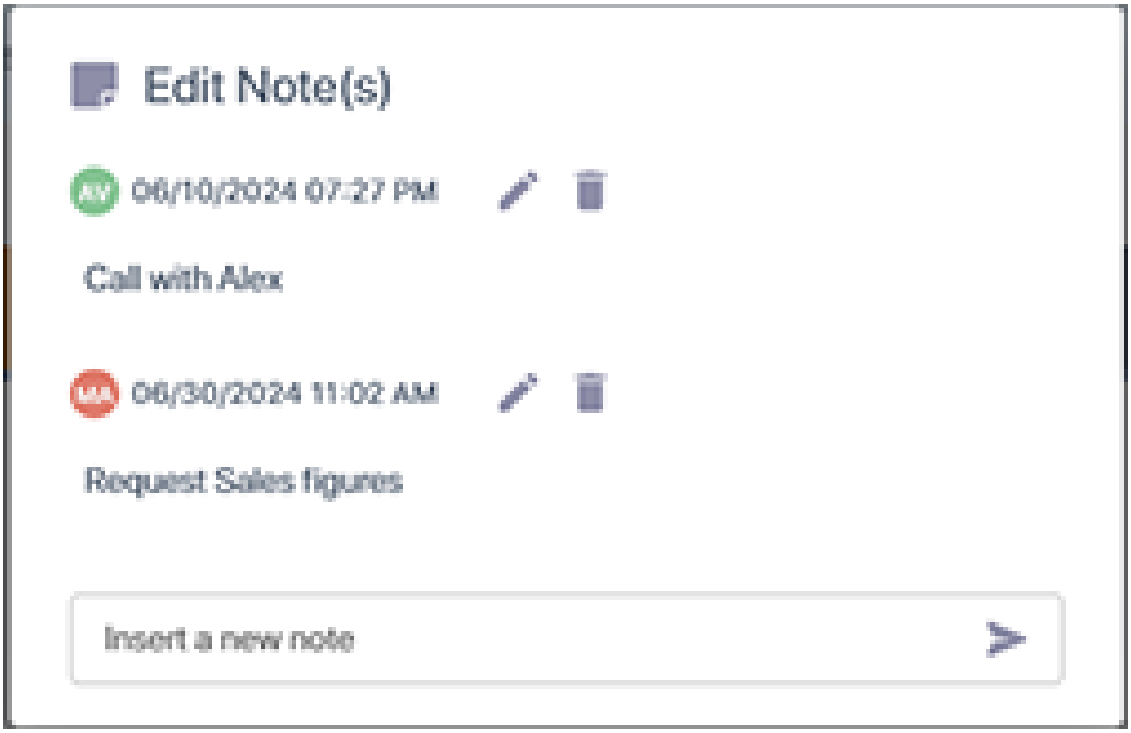
3. You can also add an a new note from an existing note inside the Media player. Click the note icon above the player.



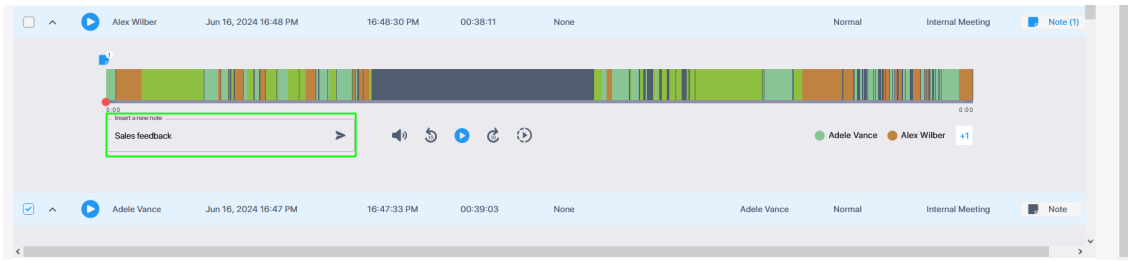
4. Enter the note text and then click the arrow.



The new note is added.



You can alternatively add notes below the Media player.



Managing Active Calls

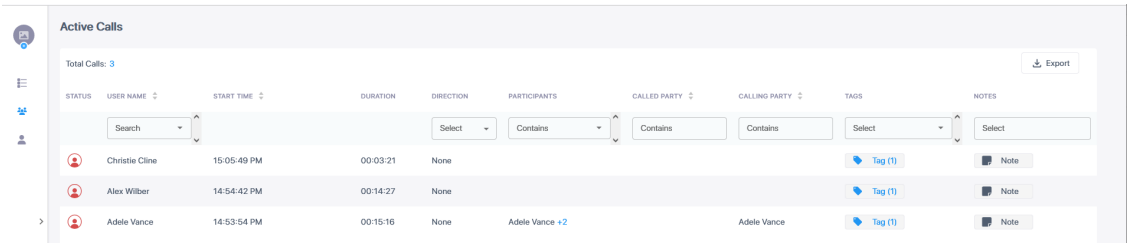
The Active Calls screen lets you view Active Calls of the targeted users of the customer tenant (users configured in recording profiles activated during the Onboarding or in Day Two (see Managing Recording Profiles on page 47). Global admin can view the Active calls for all tenant users. For the Calling party user, you can drill down to view the details of the other participants (Called Parties).

See also:

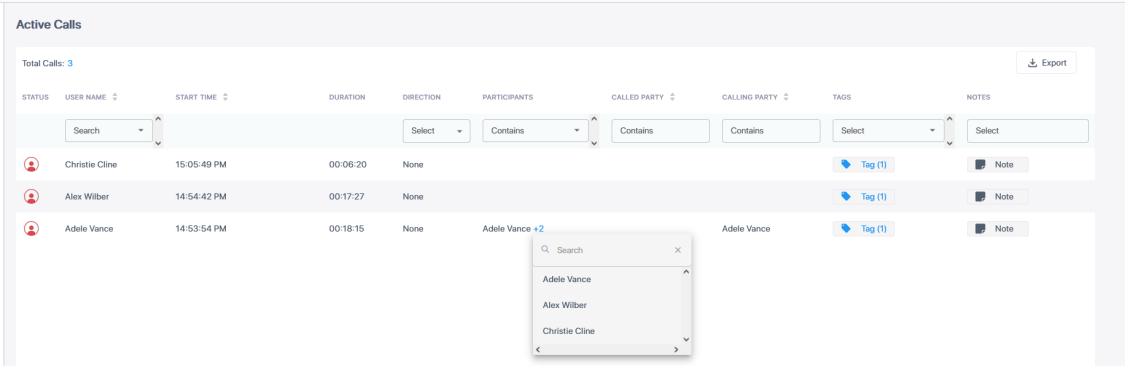
- Assigning Tags to Active Calls below
- Adding Notes to Active Calls on page 137
- My Active Call on page 143
- Exporting Active Calls on page 138

➢ To manage Active Calls:

1. In the Icon pane, click .



The figure below shows the Active Calls page of the Global Admin user, who can view the Active calls of all users. In the example, Adele Vance is the Caller and Christie Cline and Alex Wilber are the two other participants in the call.



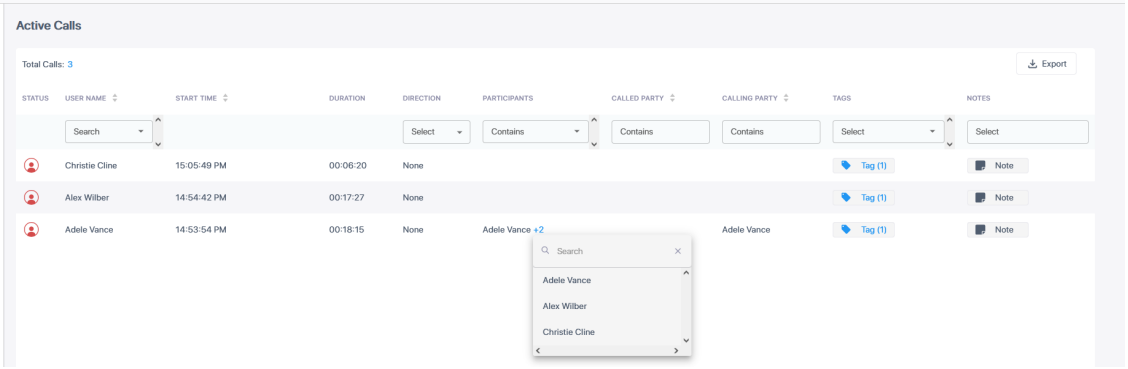
Assigning Tags to Active Calls

You can assign tags to Active Calls, where the tag serves as a reminder or keyword that can be later used to retrieve the call details and for segmentation in call analysis. In the example below, an Active Call is shown with three participants where a different tag is assigned to each participant in the call.

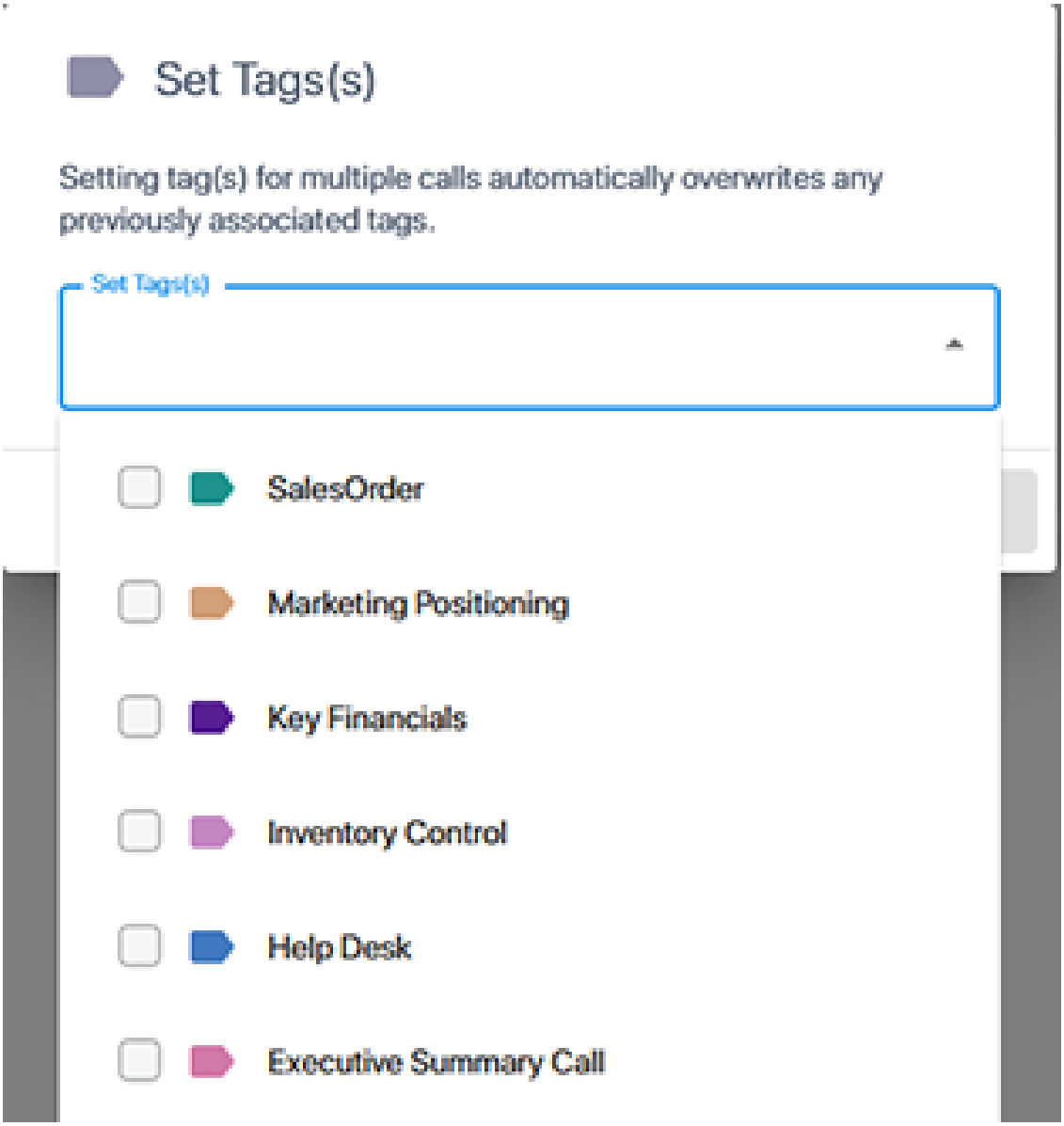
➢ To assign tags:

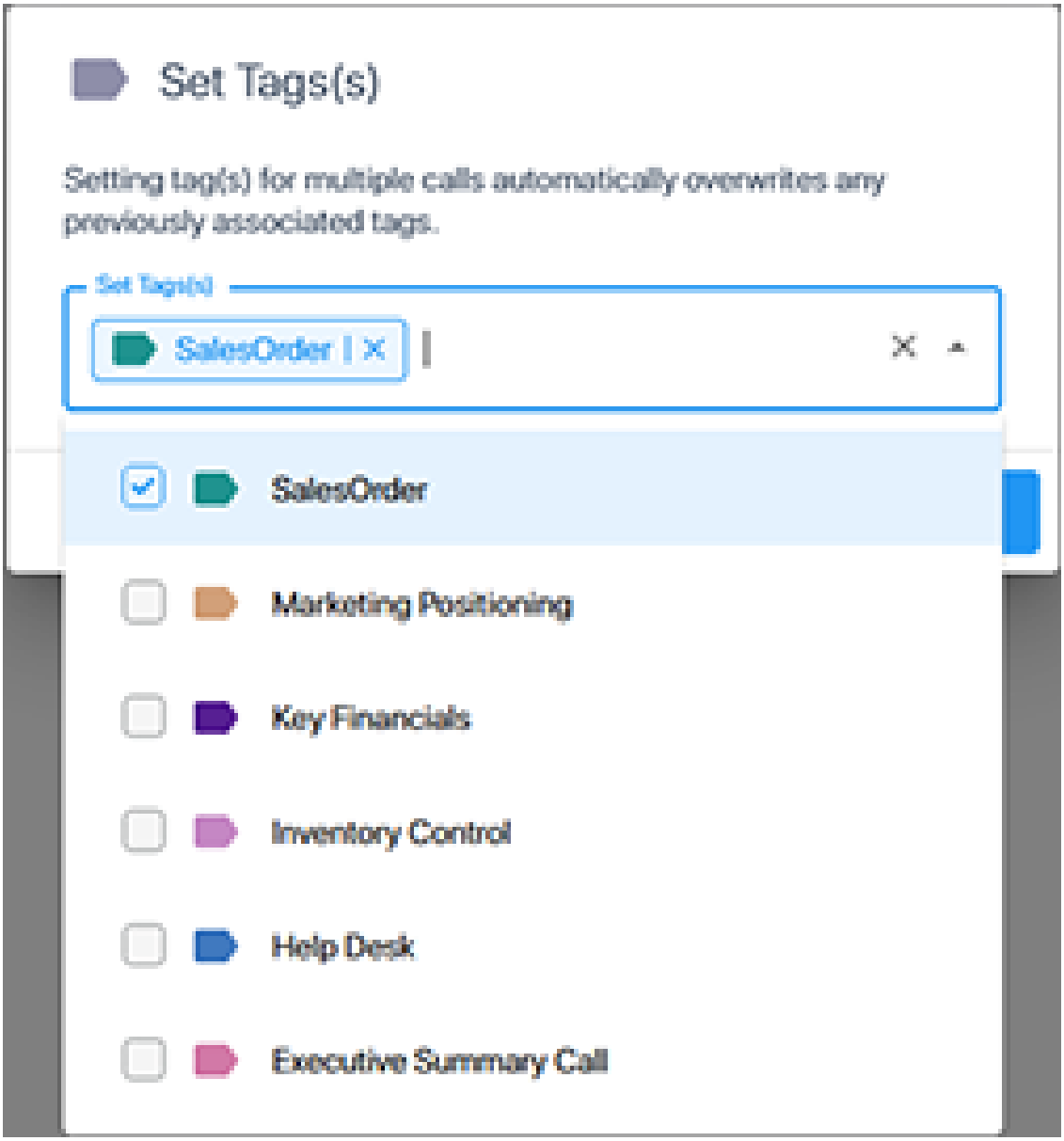
1. In the Icon pane, click .
2. Click the Tag icon adjacent to the call that you wish to tag.

   The figure below shows the Active Calls screen with Global admin permissions where each call participant is displayed a separate leg.



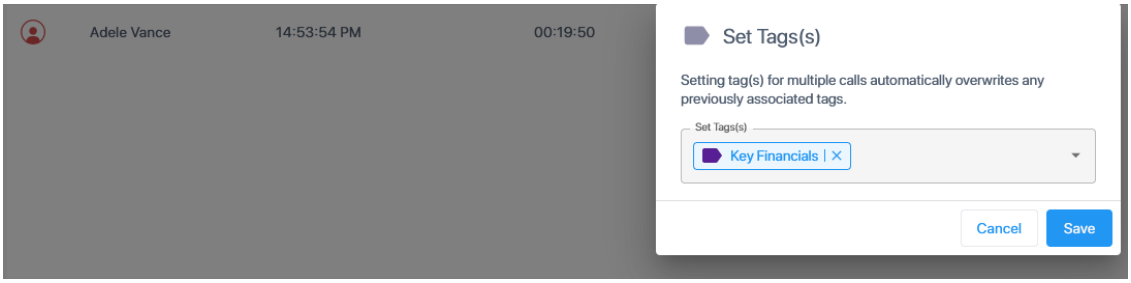
3. From the Set Tags drop-down list, select the check box adjacent to the tag that you wish set.

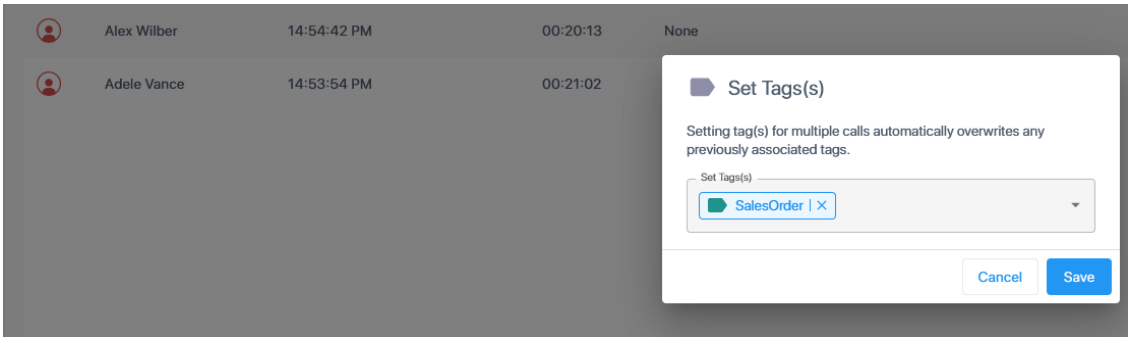

Set Tags(s)
Setting tag(s) for multiple calls automatically overwrites any previously associated tags.
Set Tags(s)
SalesOrder
Marketing Positioning
Key Financials
Inventory Control
Help Desk
Executive Summary Call

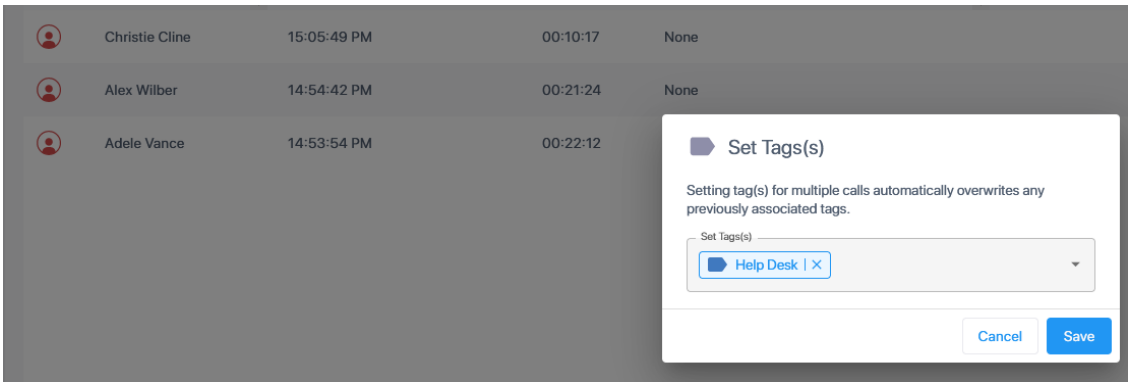


4. Click **Save**.

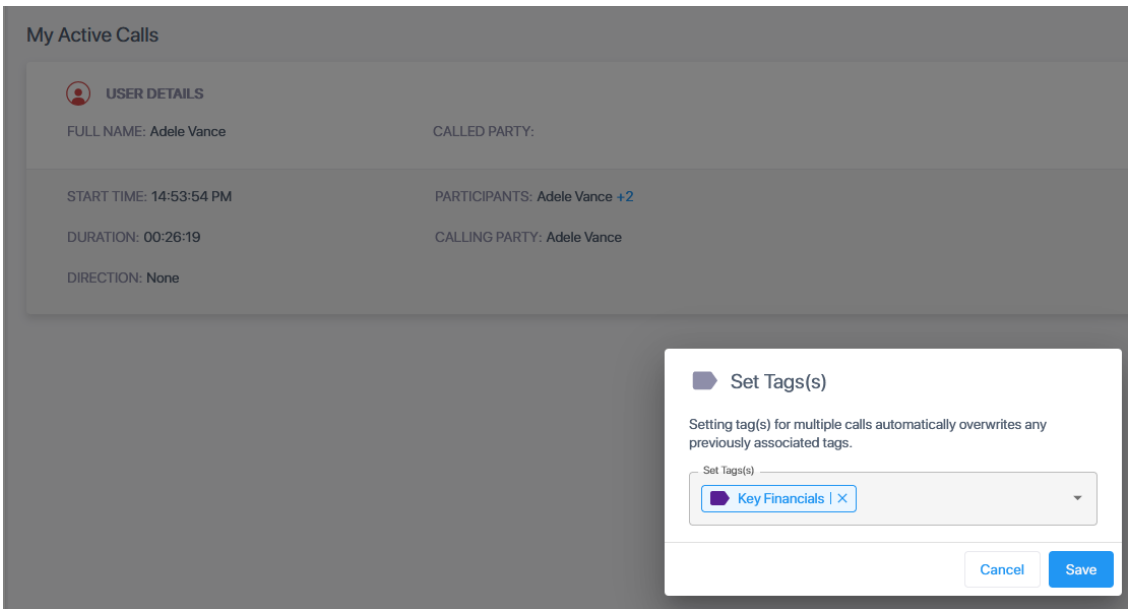
   The figures below show the separate tags that are assigned to each user participant in the Active call.

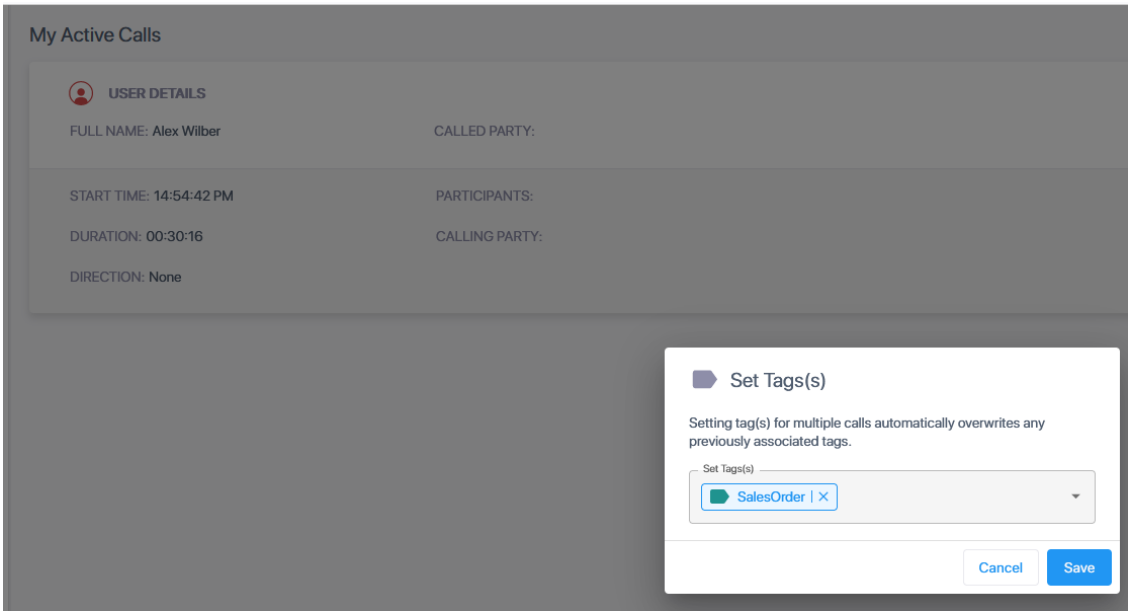


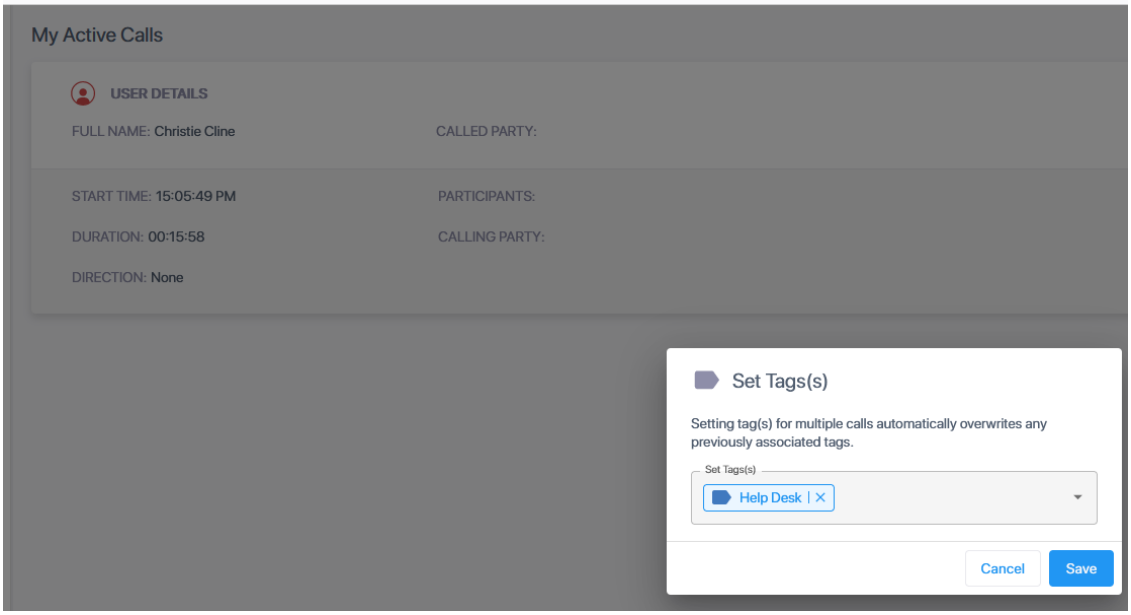




The examples below show the My Active Calls tab for each respective call participant where in each case the logged in user is the user shown in the screen.





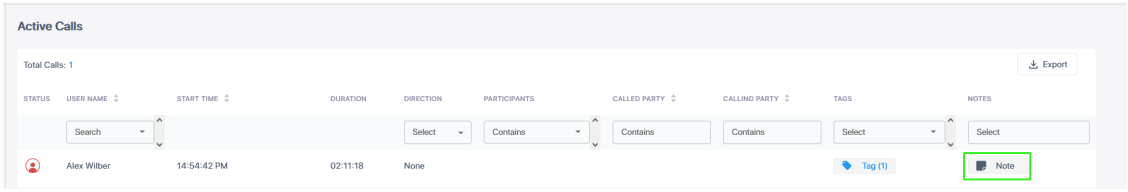


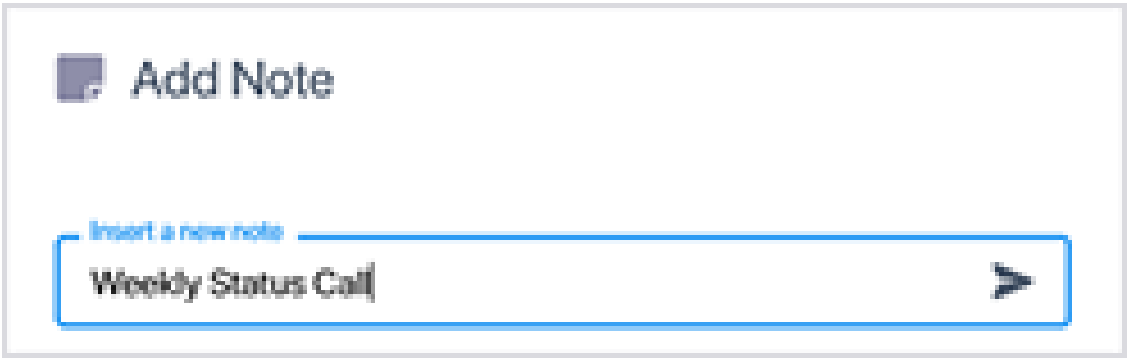
Adding Notes to Active Calls

You can attach notes to Active calls containing any text or keywords that may later assist to identify the call when specifying search criteria (see Filtering Interactions and Active Calls Information on page 100).

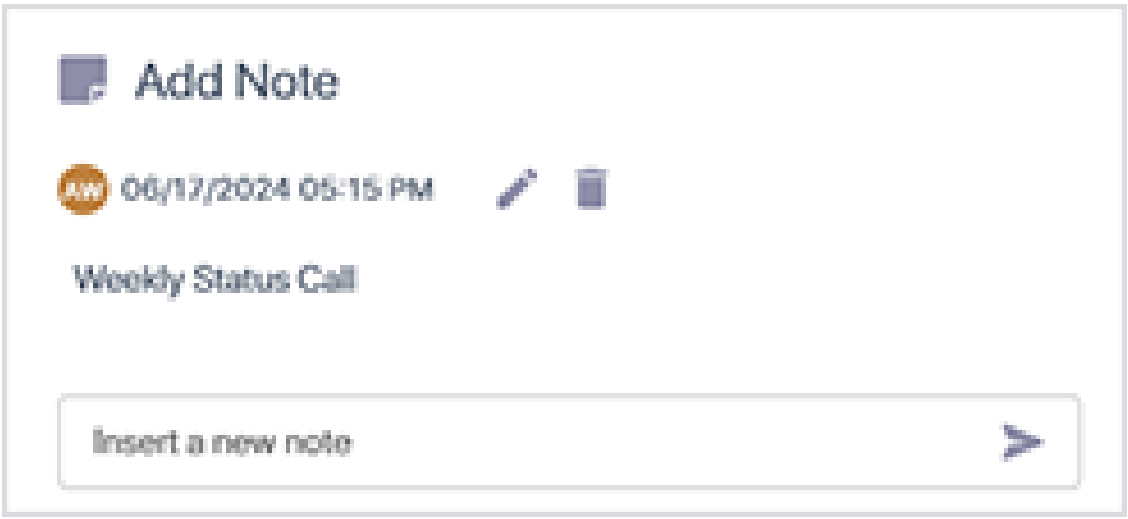
➢ **To attach notes:**

1. In the Icon pane, click or , and then click the note icon adjacent to the active call for which you wish to attach a note.





2. Click the arrow adjacent to the note text that you entered.

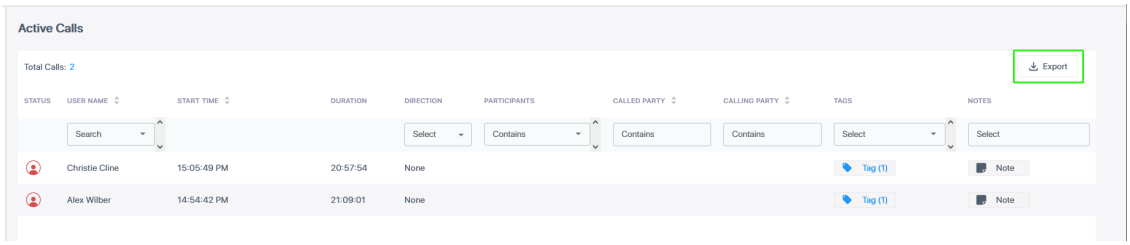


Exporting Active Calls

You can export the list of Active Calls to an Excel file. A separate entry is created for each currently Active call.

➢ To export a list of active calls:

1. In the Icon pane, click .



2. Click the **Export** button to export data. The following shows an example exported file.

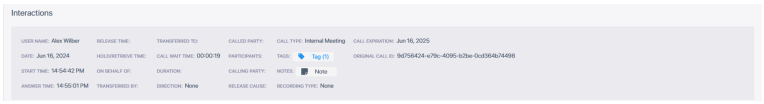
```
Report Header

Requested By    MOD Administrator

Created At    2024-06-17T09:07:55.322Z



Search Criteria



Call Id    Target Display Name    Target
Upn    OnBehalfOf    TransferredBy    TransferredTo    Called
Party    Calling Party    Answered By    Answered time    Start
Time    Release Time    SipCallId    SysCallId    Call Direction    Call
Type    Release Cause    Notes    Participants    Files    Media Audio
Status    Expiration    QueueName    DoubleRecordingType    PairedCall    T
ags    Call Link

666ed2822a44e64a82cda302    AlexW@M365x21689653.OnMicrosoft.com    AlexW@M3
65x21689653.OnMicrosoft.com                          Alex Wilber    2024-06-
16T11:55:01.621Z    2024-06-16T11:54:42.471Z        1-
8692352b214e4a418aaea352fd63fd35-2024061611544247    9d756424-e79c-4095-
b2be-0cd364b74498    None    Conference_
Internal                    Recording    2025-06-
16T11:54:42.471Z        Primary        SalesOrder    https://stngqa.ai-
logix.net/ui/interactions/666ed2822a44e64a82cda302

666ed51d2a44e64a82cda3cc    ChristieC@M365x21689653.OnMicrosoft.com    Chri
stieC@M365x21689653.OnMicrosoft.com                          Christie
Cline    2024-06-16T12:06:09.765Z    2024-06-16T12:05:49.196Z        1-
a4a790f99c6c40edb5100de2ce57c2cb-2024061612054919    9d756424-e79c-4095-
b2be-0cd364b74498    None    Conference_
Internal                    Recording    2025-06-
16T12:05:49.196Z        Primary        Help Desk    https://stngqa.ai-
logix.net/ui/interactions/666ed51d2a44e64a82cda3cc
```

The table below describes the fields in the exported data record.

Field	Description
Call Id	Unique call id

Field	Description
Target Display Name	The M365 username of the targeted user.
Target Upn	The M365 username of the targeted user.
OnBehalfOf	The name of the party for whom the call was transferred.
TransferredBy	The name of the party who transferred the call.
TransferredTo	The name of the party to whom the call was transferred.
Called Party	The M365 user receiving the call.
Calling Party	The M365 user initiating the call.
Answered By	The party who answered the call.
Answered time	The time that the call was answered.
Start Time	The time when voice recording commenced.
Release Time	The time the call was released.
SipCallId	The SIP CallId passed in the SIP Header.
SysCallId	Indicates the ID used to identify the call (also known as 'Original Call ID'). This value may be either the original call id or scenario id (Teams). For example, when recording a Teams call between user A and B the id of the call between A and B is displayed. This ID is also displayed in the Teams CDR.
Call Direction	Incoming or Outgoing
Call Type	Indicates the type of the call. One of the following values: ■ Internal Meeting ■ External Meeting ■ Internal Meeting with External Participants ■ Externalp2p ■ PSTN p2p
Release Cause	Indicates the reason why a call is disconnected. One of the following values: ■ Normal – the call was answered and then released. ■ Failure – the call or recording was stopped due to an error.

Field	Description
	■ Missed – the Targeted user didn’t answer an incoming call. ■ Abandoned – the Targeted user made an outgoing call and hanged up before the call was answered ■ Transferred – the call was transferred to another call.
Notes	Option to add notes to the Interaction record (see Adding Notes to Interactions on page 129).
Participants	The names of the call participants (I don't see this field filled ?)
Files	This field is currently not supported.
Media Audio Status	One of the following values: ■ Available: The interaction is available for playback. ■ Pending: The interaction is pending database synchronization. ■ Recording: The Interaction is currently being recorded. ■ Failed: The SmartTAP failed. ■ Unavailable: The recording is unavailable. ■ Deleted: The recording has been deleted.
Expiration	Indicates the date that the call recording is purged as defined in the Recording profile.
QueueName	Teams Queue Call Instance ID when configured in the Recording profile.
DoubleRecordingType	Indicates whether Essentials (Single Recording Audio License) or Pro (Double Recording Audio &Redundancy license) is configured for the service.
PairedCall	Indicates whether Geographical Redundancy Storage is enabled in a paired region for data disaster recovery (enabled by default when a Pro License is configured for the service).
Tags	Names of any tags assigned to the calls.
Call Link	Opens a summary of the call details with the Call Id in the URL . For example https://stngqa.ai-logix.net/ui/interactions/666ed2822a44e64a82cda302

Field	Description
	

My Active Call

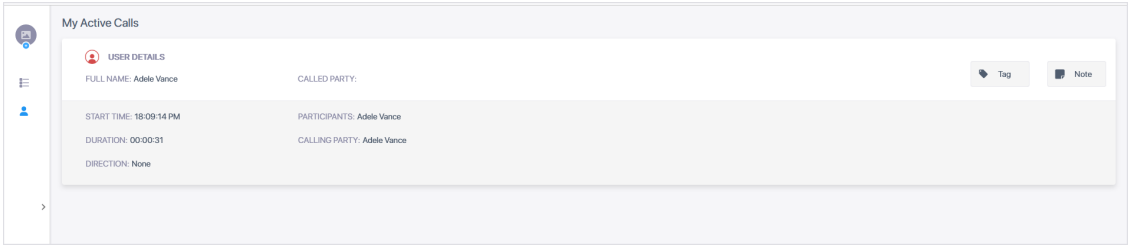
The My Active Calls screen displays the details of any Active calls in the targeted user's Teams client. The call details are displayed so long as the call remains active. The Duration field increments while the call remains active. Multiple Active calls can be displayed.

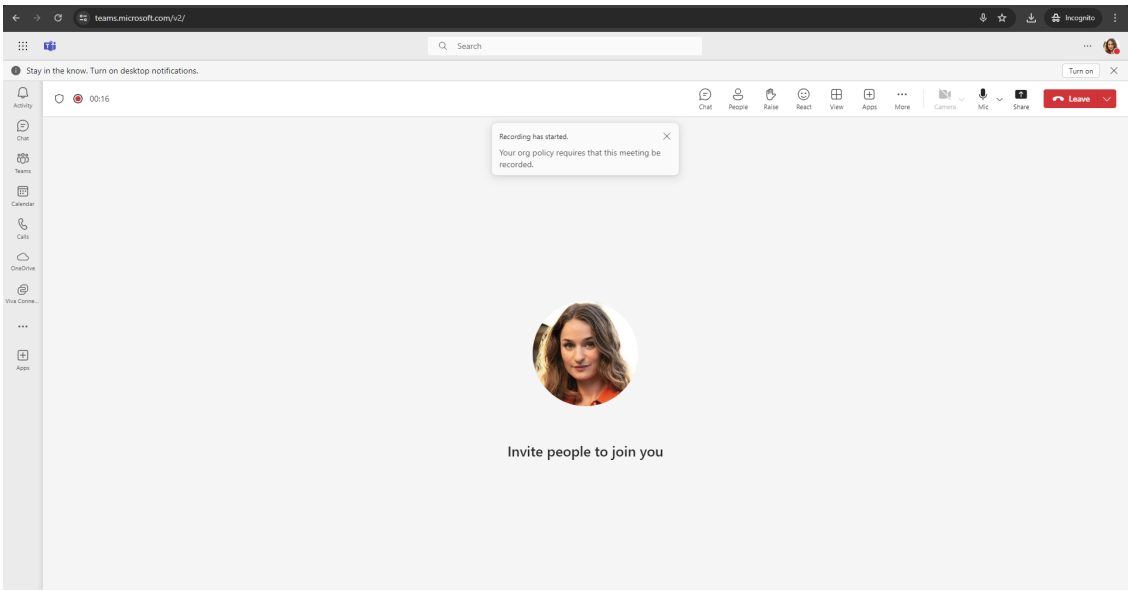
See also:

- Assigning Tags to Active Calls on page 132
- Adding Notes to Active Calls on page 137

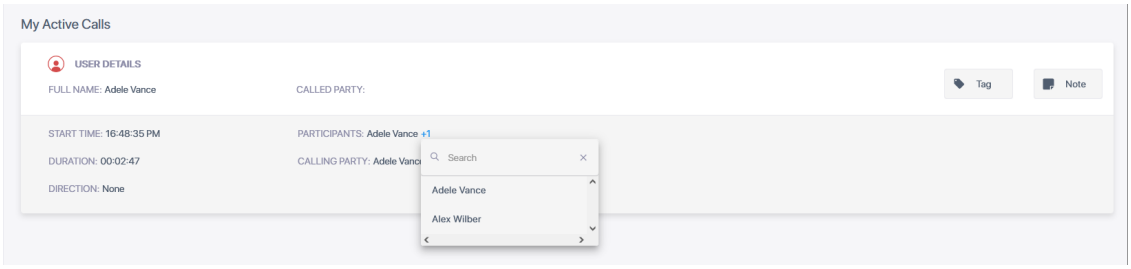
➢ **Do the following:**

1. In the Icon pane, click .

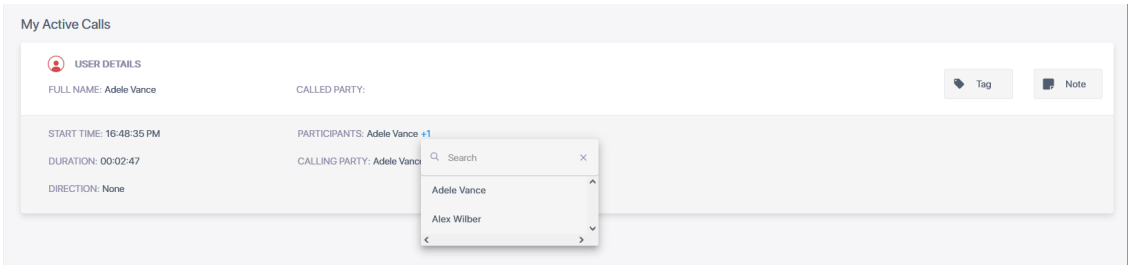


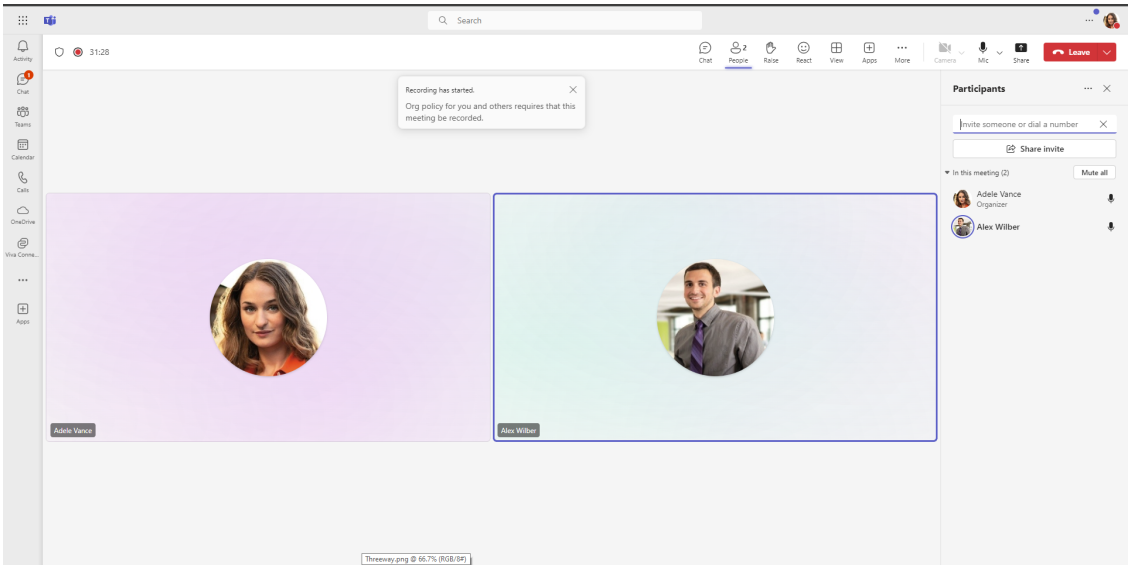


The following figure shows an example of an Active call between two participants.

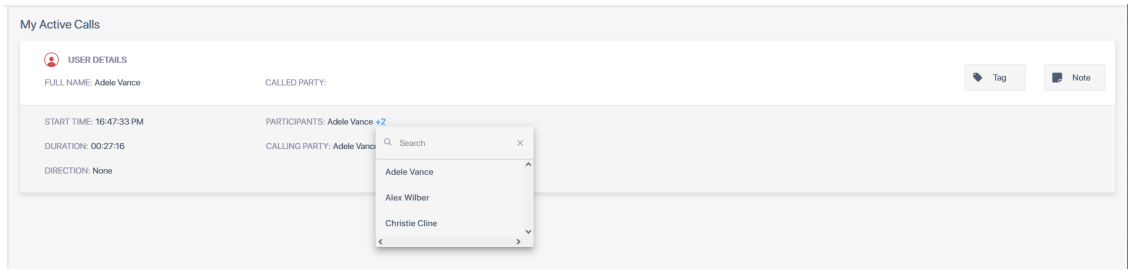


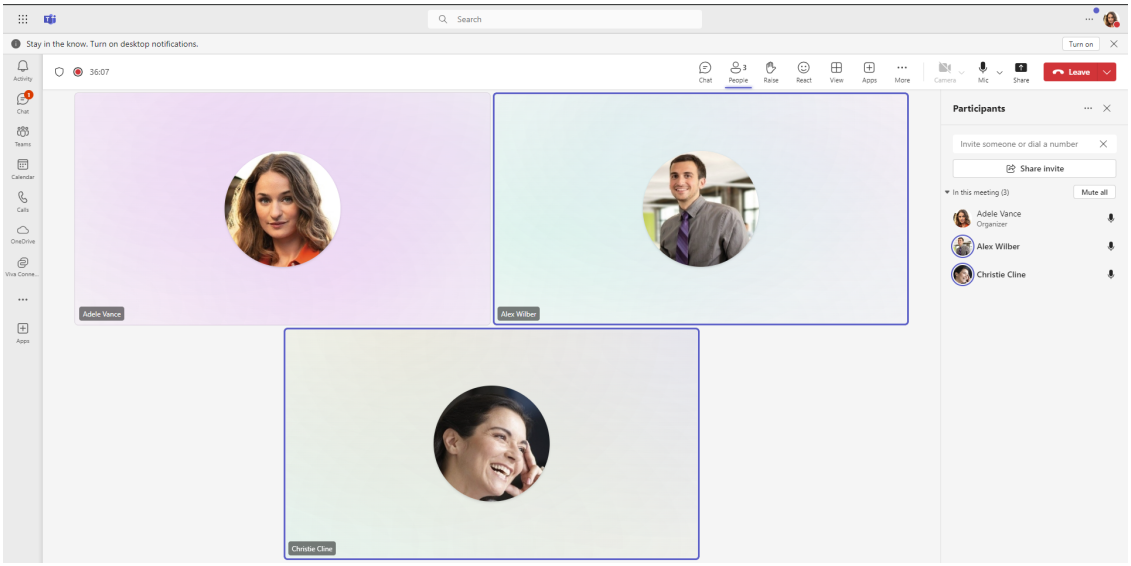
The number of participants is displayed for the Calling party only (the party initiating the call).



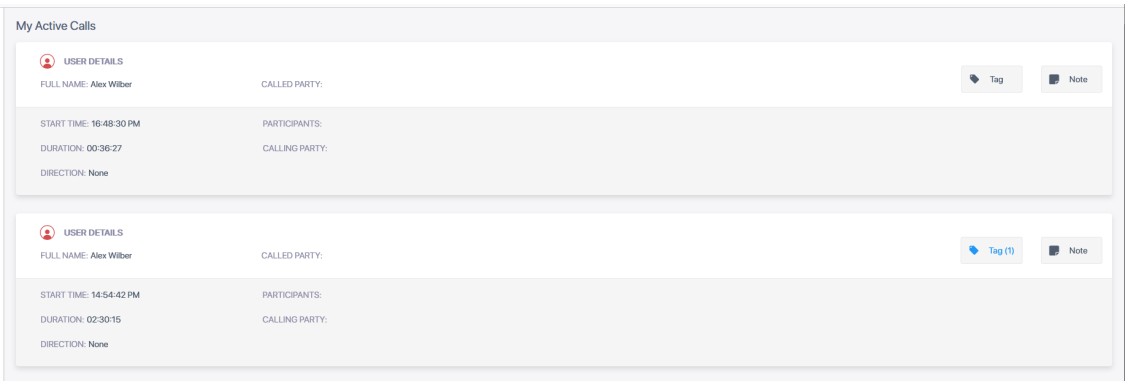


The following figure shows an example of an Active Call between three participants.





The following figure shows two Active calls for the user Alex Wilber.



System Settings

- Tools on page 148
- Bring-Your-Own-Storage on page 153
- Manage Tags on page 159
- Branding on page 161
- Licenses on page 163

Connect to M365

The M365 Settings screen lets you manage your connections to the M365 platform. You most likely provided consents during the Quick Start wizard (Quick Start on page 15). Upon consent an Enterprise application is created on your M365 tenant with the required permissions (see table below for details).

Global Admin privileges for the customer Azure tenant are required to provide consents.

The table below describes the required consents and the Enterprise applications that are created on your M365 tenant.

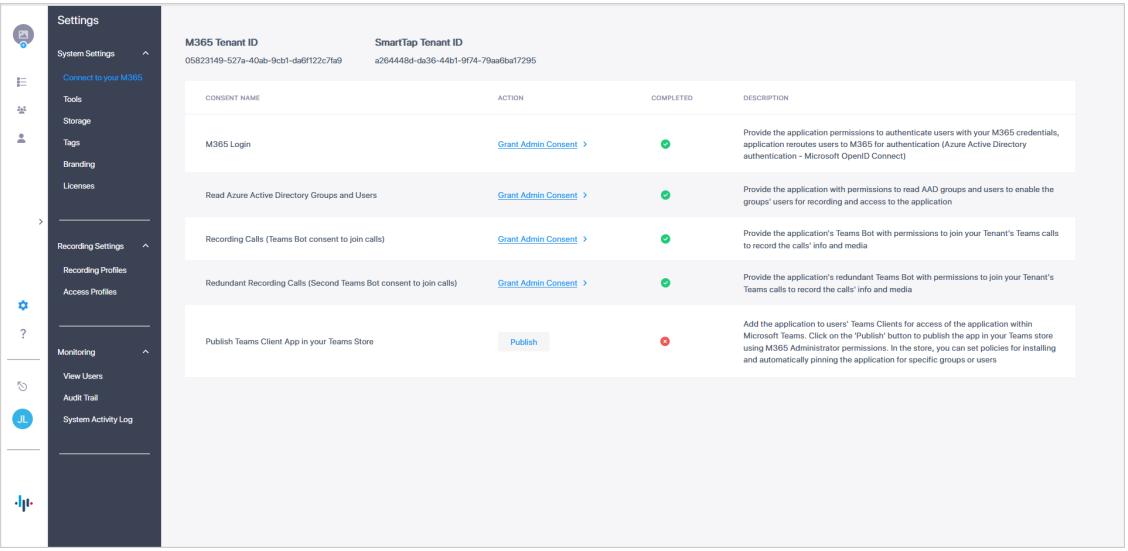
Consent	Description
M365 Login	Provide the application permissions to authenticate users with your M365 tenant credentials. The application reroutes users to M365 for authentication (Azure Active Directory authentication-Microsoft OpenID Connect-Oauth 2). The permissions are required for the SmarTAP application to authenticate users utilizing your tenant AAD authentication, and Microsoft Open ID Connect (Oauth 2) authentication. The permissions enable AudioCodes Live SmartTAP to reroute users accessing the AudioCodes Live SmartTAP application either from a browser or from the AudioCodes Live SmartTAP Teams application (see row below) to be authenticated according to your organizational M365 policy. The Deployment generates the Enterprise application <LivePlatformSer verName>-auth. Youconsent to the following permissions: ■ email – View users; email address (Delegated) ■ offline_access – Maintain access to data you have given it access to (Delegated) ■ openid – Sign users in (Delegated) ■ profile – View users' basic profile (Delegated)

Consent	Description
	■ User.Read – Sign in and read user profile (Delegated)
Publish Teams Client App in your Teams Store	Add the application to users Teams Clients for access of the application within Microsoft Teams. Click the publish button to access the app within your Teams store using M365 Administrator permissions. In the store, you can set policies for installing and automatically pinning the application for specific groups are users. This consent is part of the M365 Login application (shown above). In addition to the permissions shown above, the following are added: ■ AppCatalog.Submit – Submit application packages to the catalog and cancel pending submissions. ■ AppCatalog.ReadWrite.All – Read and write to all app catalogs Publishing the app makes it available for users in the tenant organization within Teams store. Each user needs to add the application from their Teams admin center in order to access it from Teams.
Read Azure Active Directory Users and Groups	Provide the application permissions to read AAD groups and users from your M365 tenant to enable the groups' targeted users for recording and access to the application. Deployment of AudioCodes Live SmartTAP generates the Enterprise application <LivePlatformServerName>-aad. Youconsent to the following permissions: ■ User.Read.All – Read all users' full profiles (Application) ■ GroupMember.Read.All – Read all group memberships (Application)
Recording Calls (Teams Bot consent to join calls)	Provide the application's Teams Bot with permissions to join your Tenant's Teams calls to record the calls' info and media. The calls-app permissions are required for the AudioCodes Live SmartTAP Bot application to join your Teams' tenant calls and to receive the media to be recorded. Deployment of AudioCodes Live SmartTAP generates the Enterprise application <LivePlatformServerName>-hue. Youconsent to the following permissions: ■ Calls.JoinGroupCall.All - Join group calls and meetings as an app (Application) ■ Calls.AccessMedia.All - Access media streams in a call as an app (Application)
Redundant Recording	Provide the application's Redundant Teams Bot with permissions to join your tenant's Teams calls to record the calls' info and media. The calls-app

Consent	Description
Calls (Second Teams Bot consent to join calls)	permissions are required for the AudioCodes Live SmartTAP Bot application to join your Teams' tenant calls and to receive the media to be recorded. Deployment of AudioCodes Live SmartTAP generates the Enterprise application <LivePlatformServerName>-hue-paired. Youconsent to the following permissions: ■ Calls.JoinGroupCall.All - Join group calls and meetings as an app (Application) ■ Calls.AccessMedia.All - Access media streams in a call as an app (Application) ⚠ This consent is required in the event where a Pro User license has been configured for the service.

➢ **Do the following:**

1. In the Icon pane, click ⚙, and then in the Navigation pane, select **System Settings** > **Connect to your M365**.



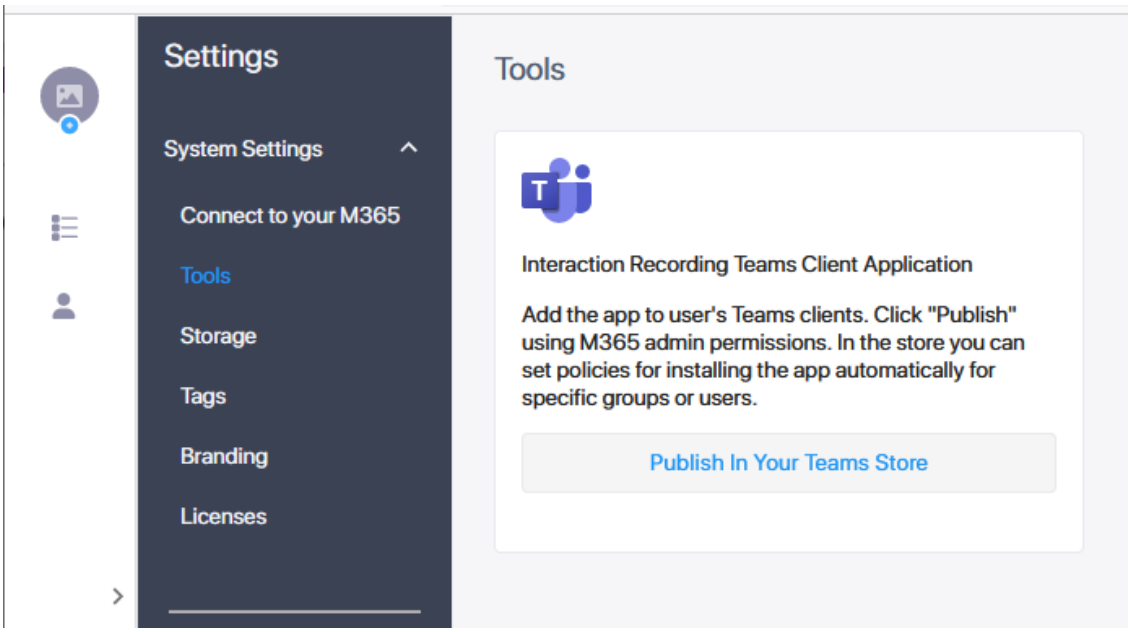
2. Click the **Grant Admin Consent** button adjacent to each Consent for which you wish to activate. A green tick is displayed once the consent process has completed successfully.

Tools

This option lets you publish the app to the admin user's Teams admin center. In the store you can also set policies for installing the app automatically for specific groups or users. This can also be performed in the Quick Start wizard (see Quick Start on page 15). Once you have published, open the Teams client for any of your tenant users and install the app in the Web client (see Deploy SmartTAP Teams App in Customer Teams client).

➢ **Do the following:**

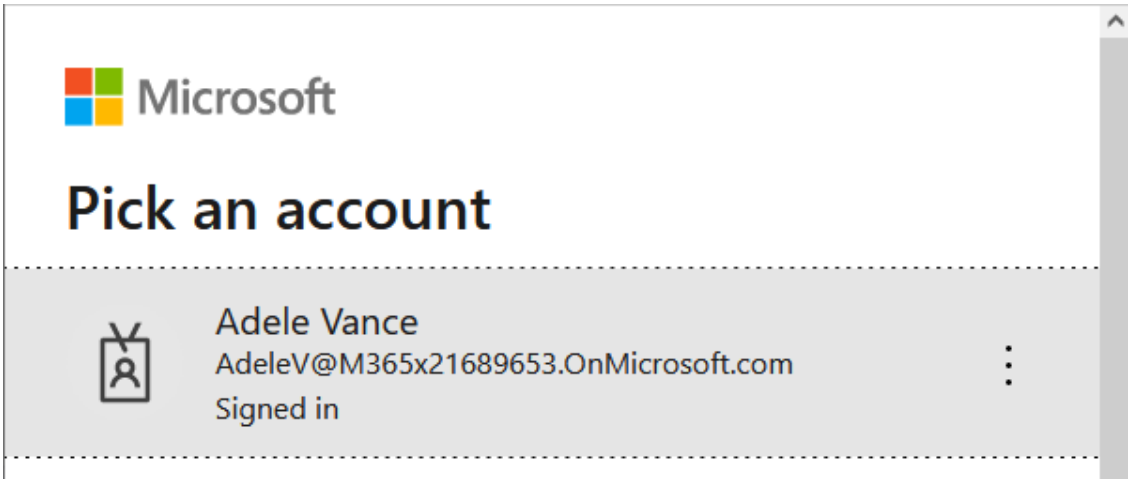
1. In the Icon pane, click , and then in the Navigation pane, select **System Settings > Tools**.



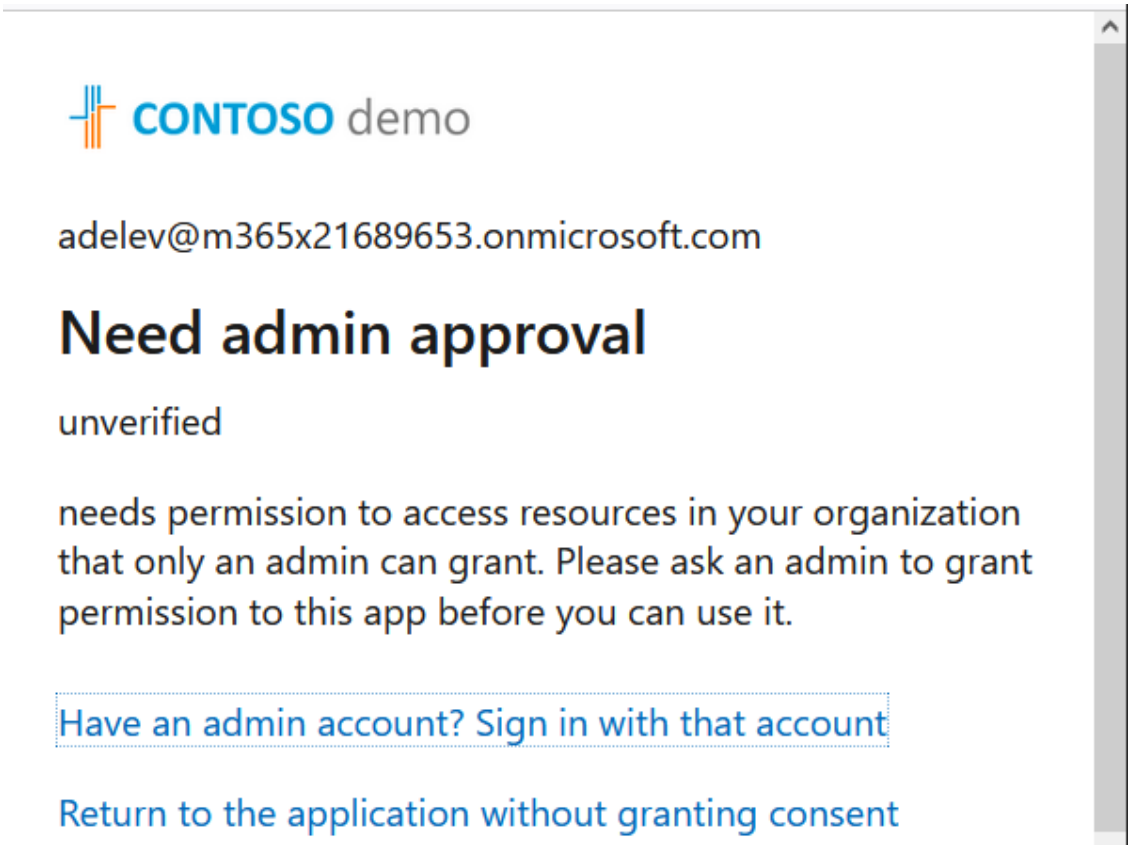
2. Click **Publish in Your Teams Store** to publish the app to the logged in users' Teams client.

> Publishing the app makes it available for users in the tenant organization within Teams store. Each user needs to add the application from their Teams admin center in order to access it from Teams.

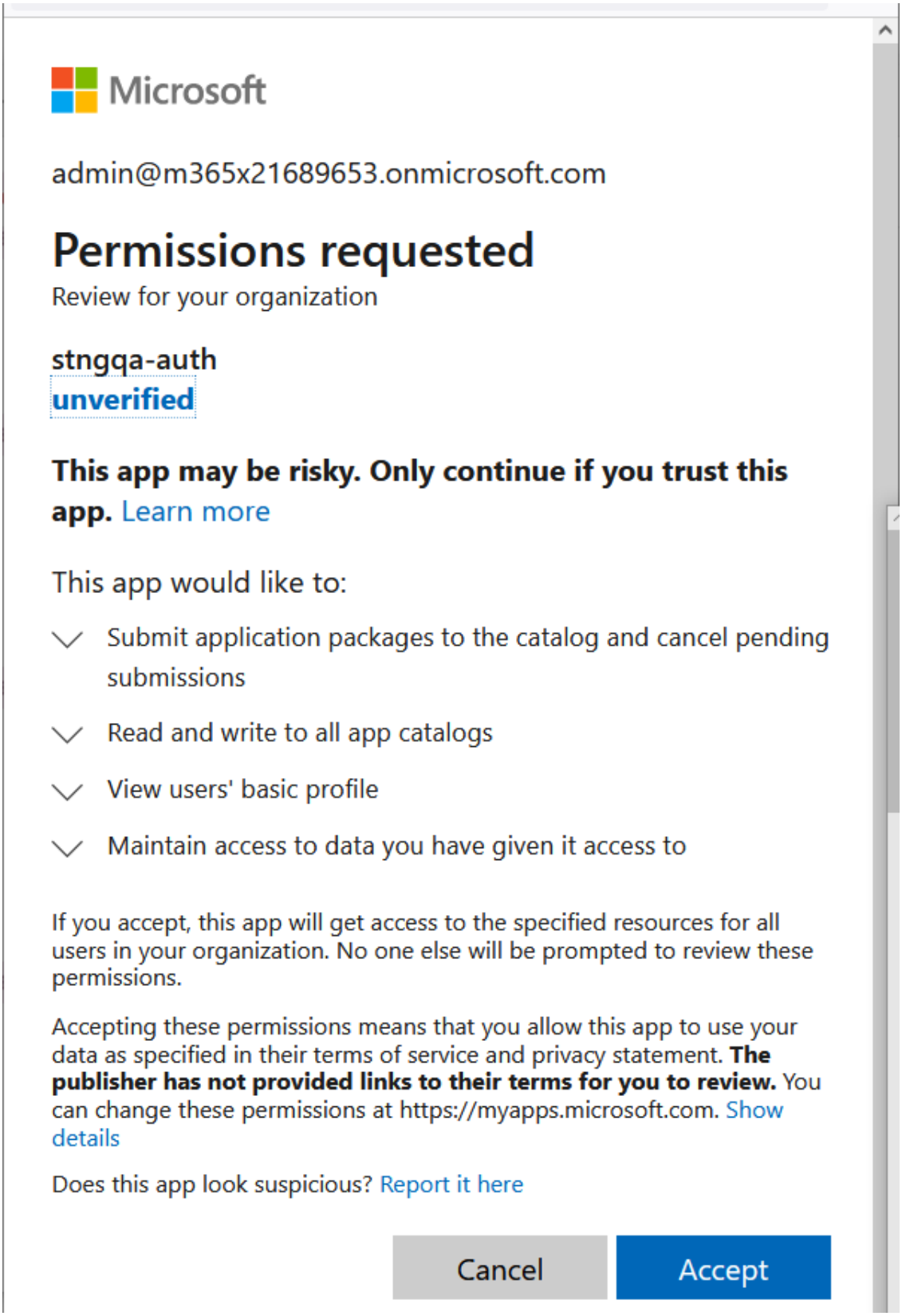
3. Select the user account for which you wish to publish.



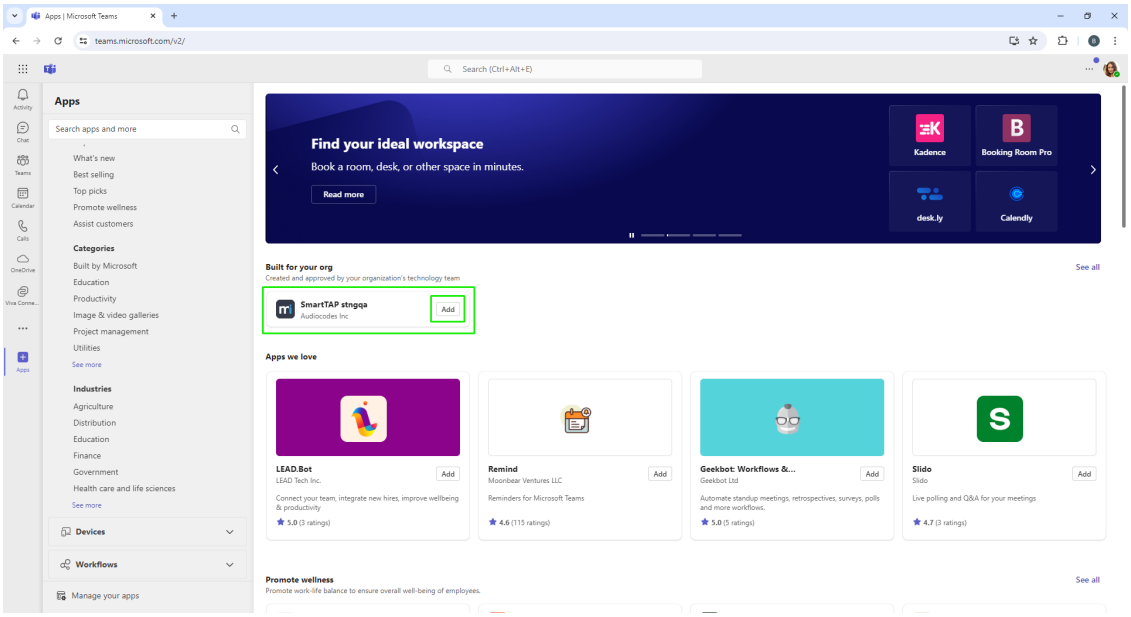
4. Click the **Have an admin account? Sign in with that account** link



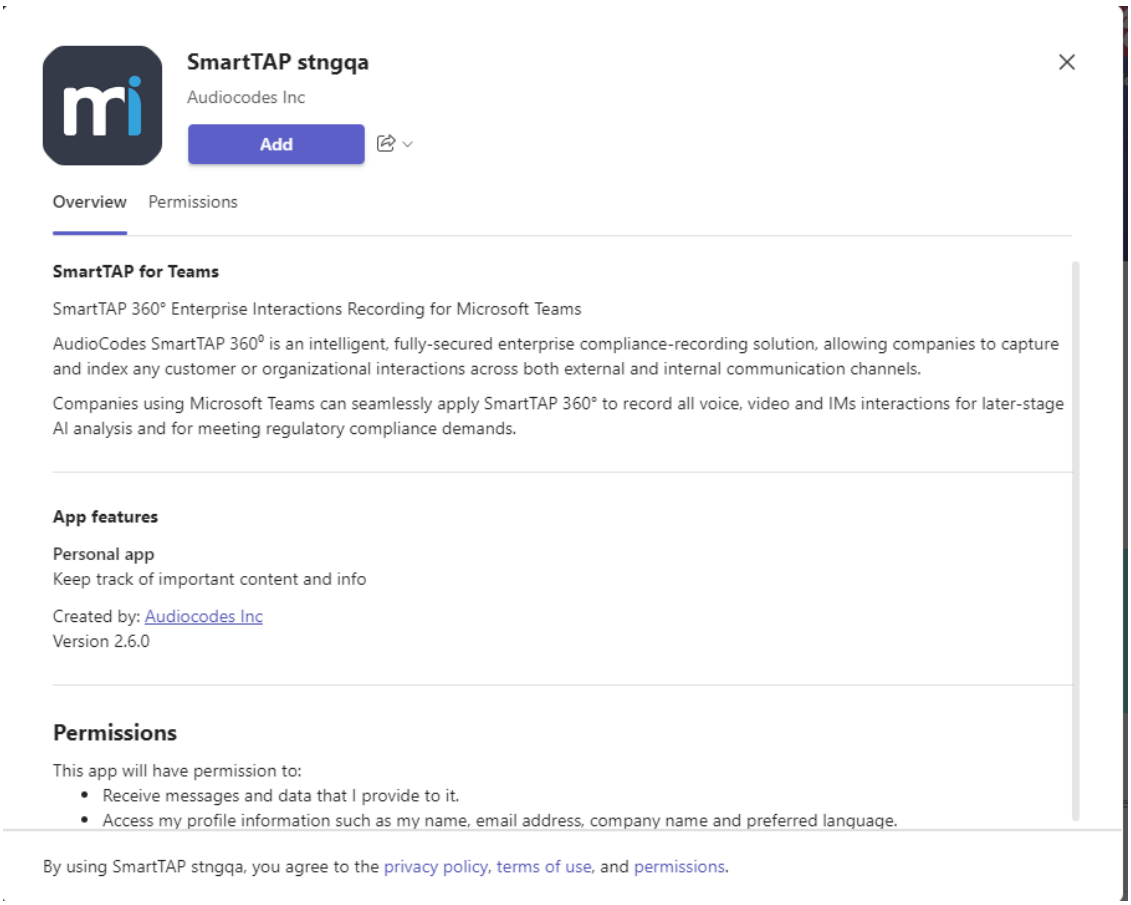
5. Click **Accept.**



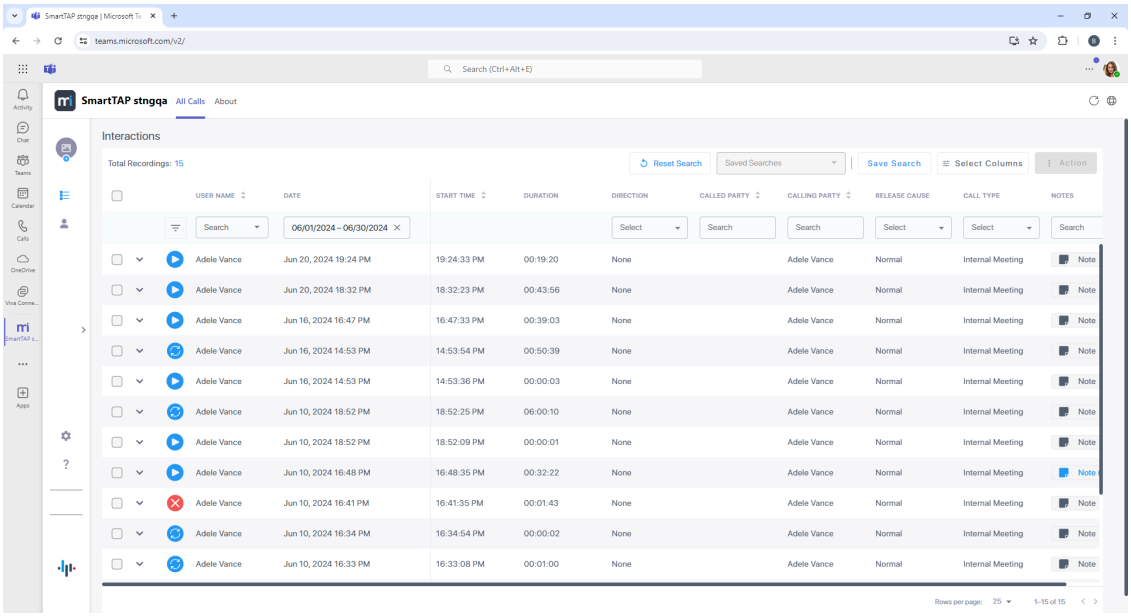
6. Open the Microsoft Teams, open the Apps page, and search for the SmartTAP app.



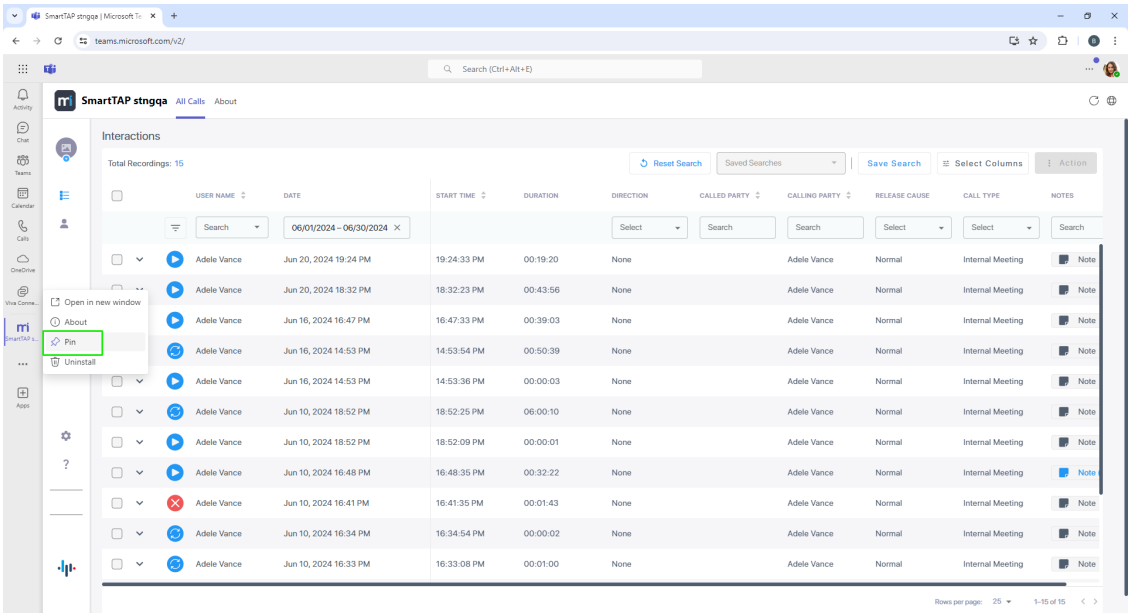
7. Click **Add**.



8. Click **Add**. The app opens inside the users' Teams client.



9. Right-click the app icon, and then choose **Pin**.



Bring-Your-Own-Storage

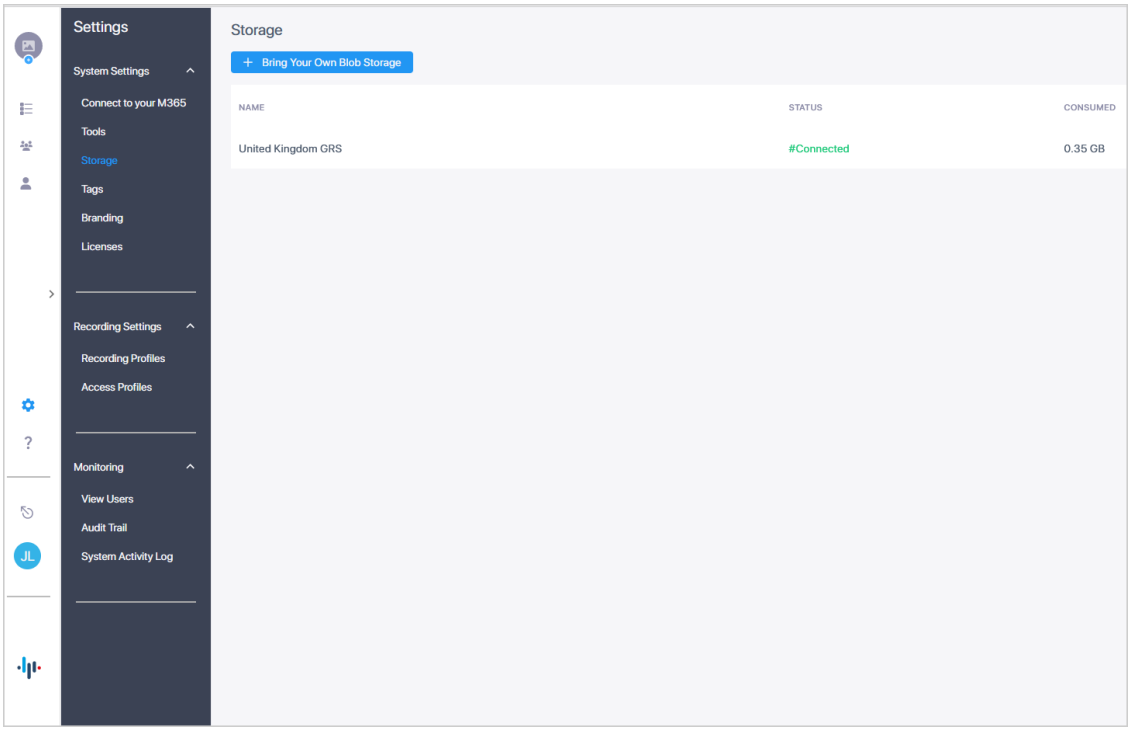
This option lets you manage your Blob Storage accounts. The Quick Start process added the Service Provider Azure Blob System Storage account for your region. You can add additional Azure Blob accounts for different locations. For each location, you can monitor the status of the connection and Consumption in GB for the storage utilization. Once you add BYOS locations, they can be associated to Recording profiles.

- The ability to add Blob storage accounts requires the BYOS feature key. Contact AudioCodes support for details.
- Ensure that you have added your BYOC accounts on your M365 tenant.
- Performance latency may be affected if the storage location is geographically remote to the SmartTAP server deployment instance.
- Data consumption is only displayed for GRS (Geo Recording Storage) storage accounts.

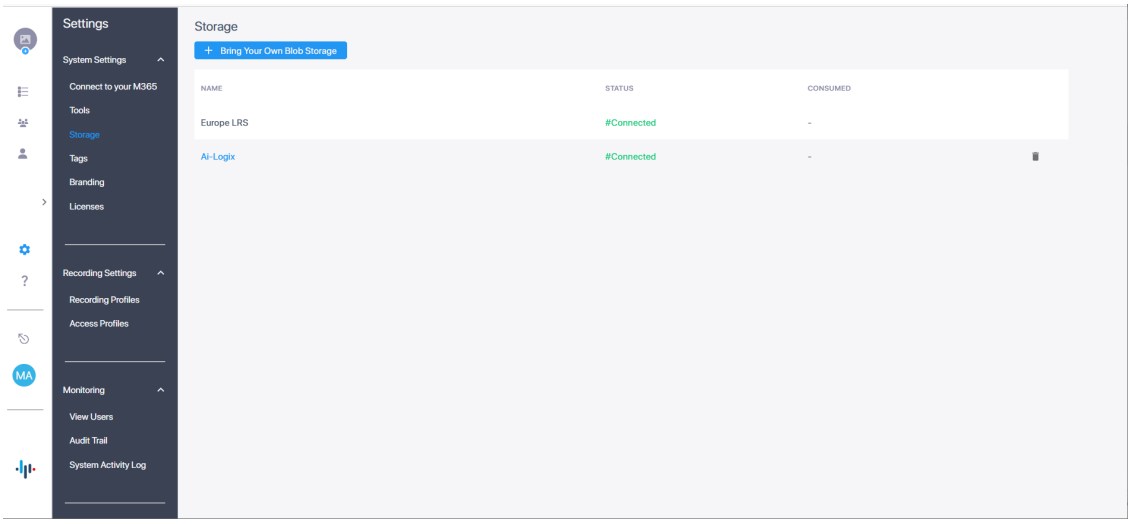
➢ **Do the following:**

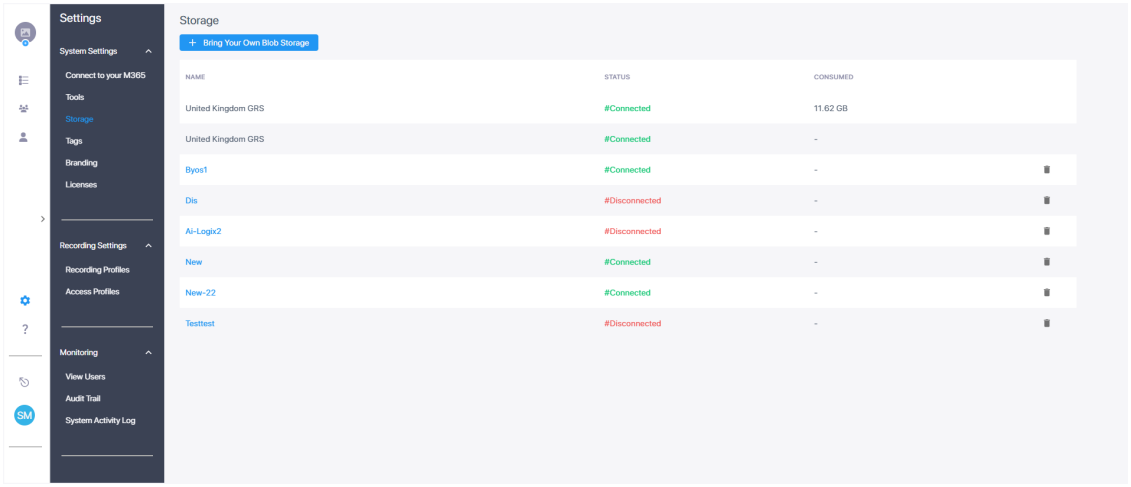
1. In the Icon pane, click , and then in the Navigation pane, select **System Settings** > **Storage**.

   In the figure below, the default System storage account is 'United Kingdom GRS'. The storage utilization is 0.35 GB. If your service was onboarded with an Essentials user license with Single Recording server instance, then the default system storage location name is <RegionName> LRS (Local Recording Storage). If your service was onboarded with a Pro user license with Redundancy Recording server instance, then the name is <Region Nane> GRS (Geo Recording Storage).

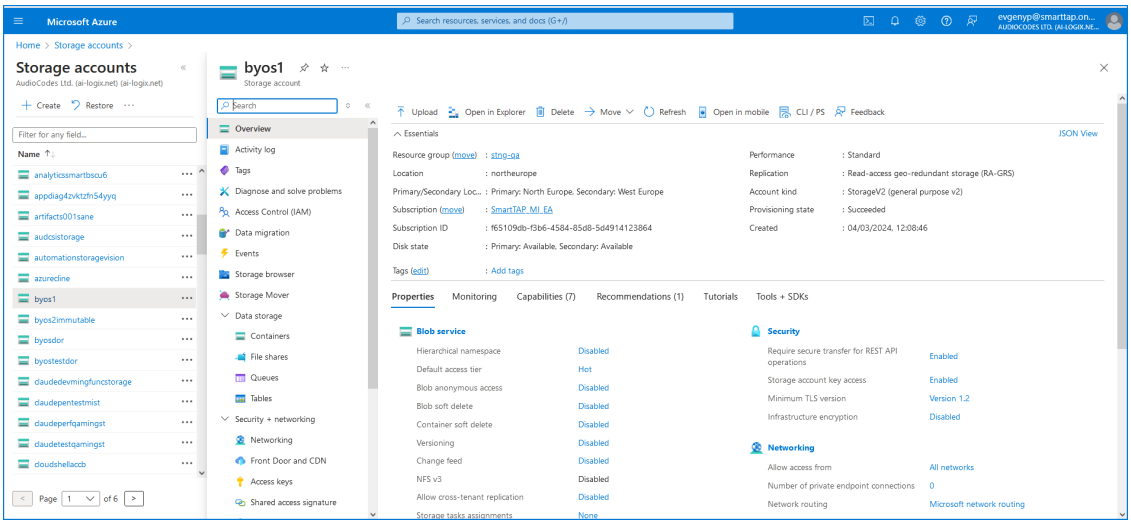


   The figure below shows added BYOS storage accounts. Once added, accounts can be later removed.

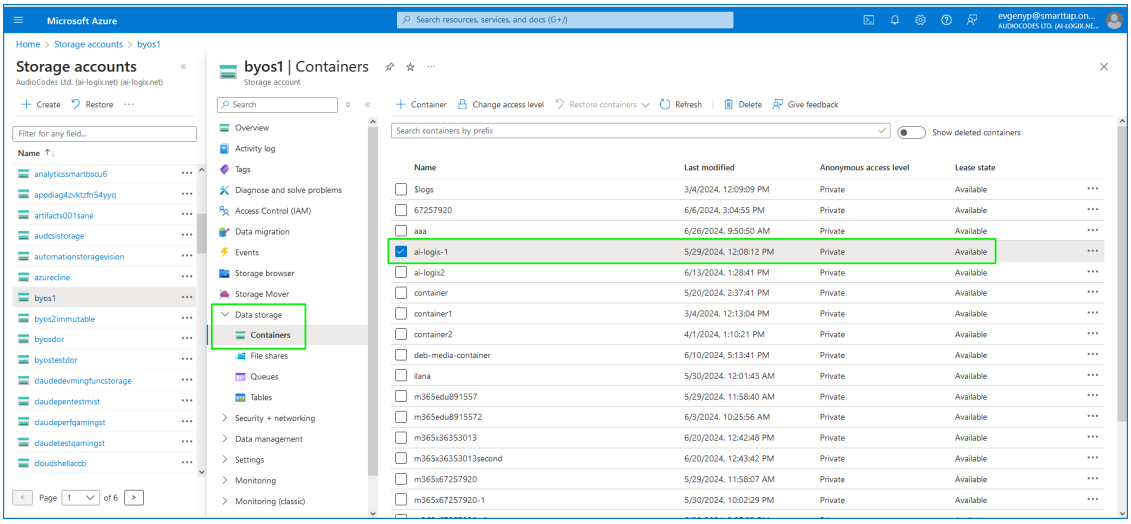




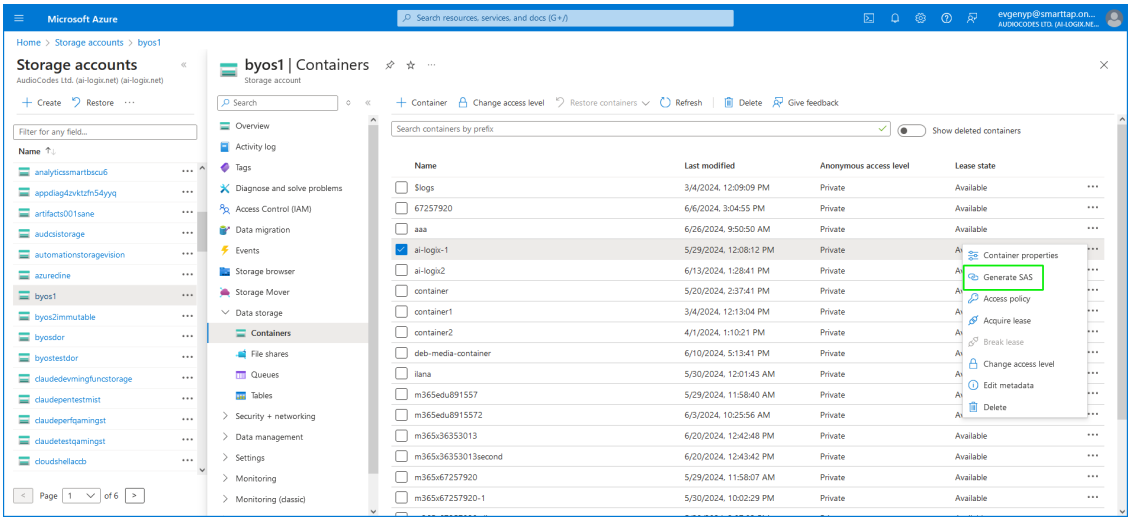
2. Login to the Microsoft Azure customer tenant, and open the relevant Blob Storage account.

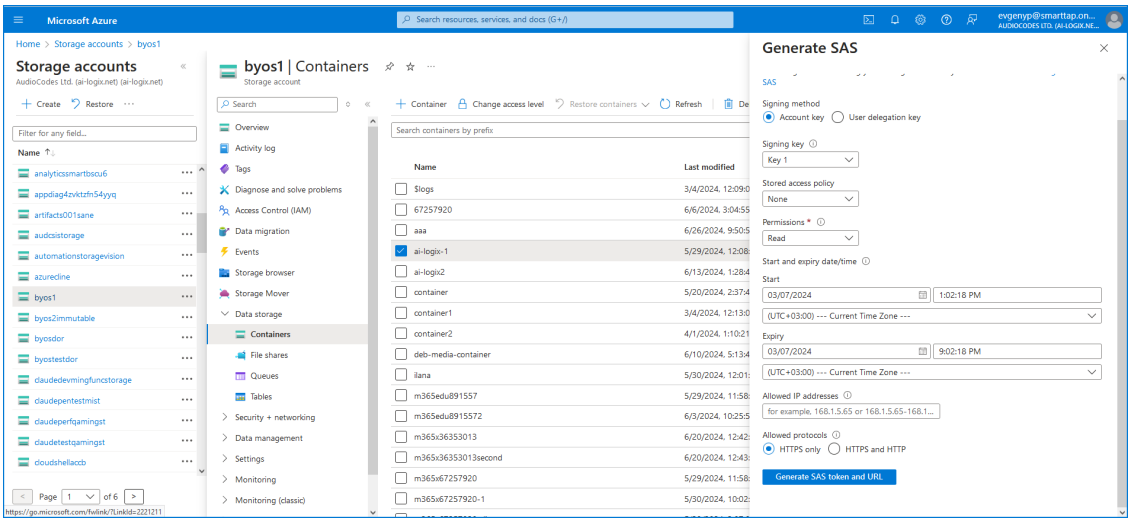


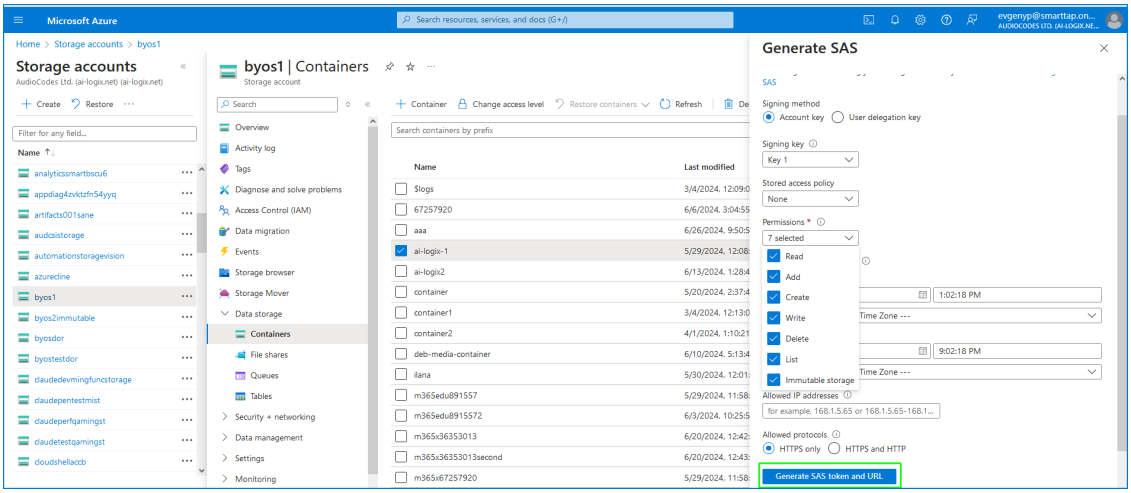
3. In Navigation pane, select **Data storage** > **Containers**, and then select the relevant container in which you wish to store media.



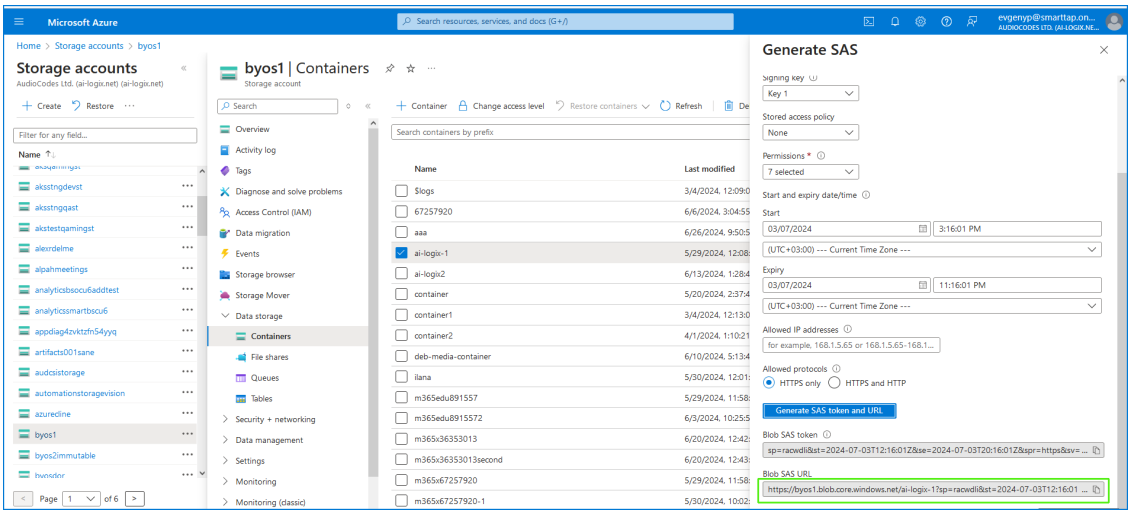
4. Select the entry and then from the .....right-click menu, choose **Generate SAS**.



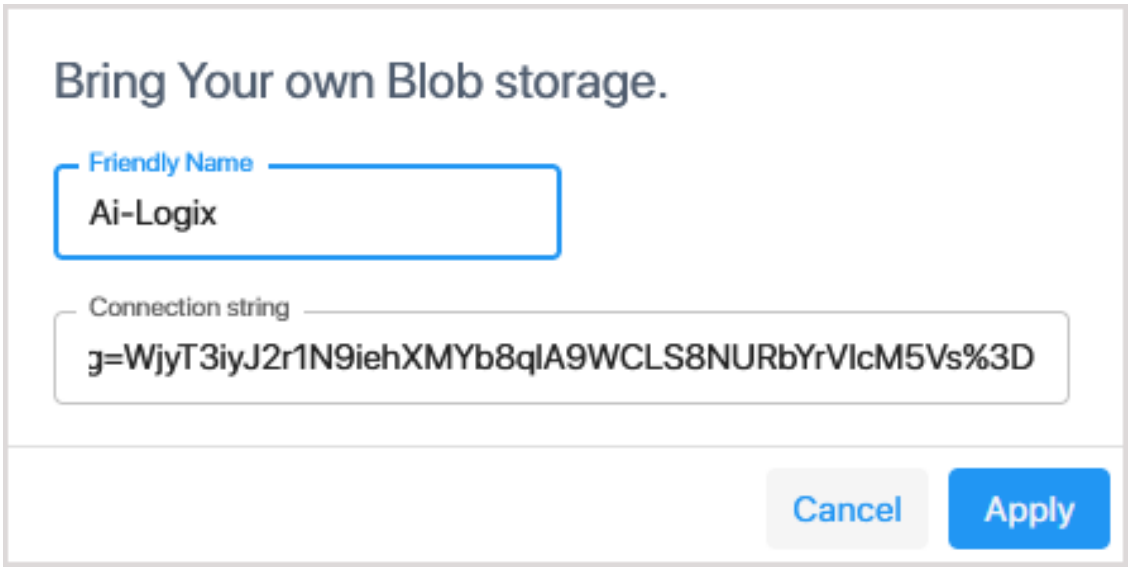




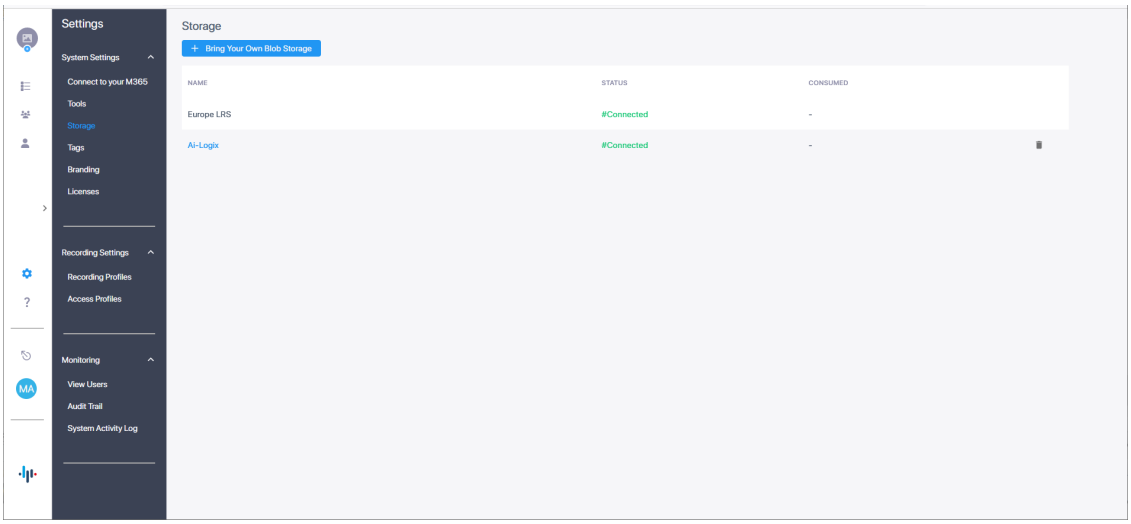
5. Configure as follows:
   a. Select the Account key check box.
   b. Signing key **Key 1**
   c. Shared access policy
   d. Select all permission check boxes.
   e. Allowed protocols **HTTPS only**.
6. Click **Generate SAS token and URL**.
7. Copy the Blob SAS URL value to notepad.



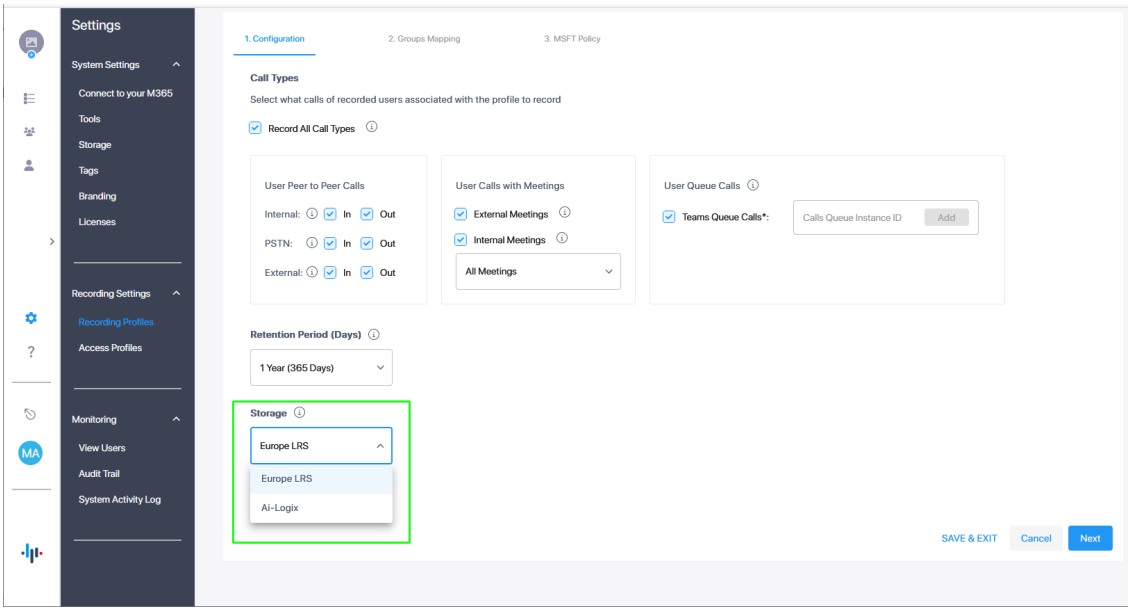
8. Return to the Storage page in the AudioCodes Live SmartTAP interface.
9. Click **Bring Your Own Blob Storage**.
10. Enter the name of the Blob storage container.
11. Paste the Blob SAS URL that you copied above to the Connection string field.



12. Click **Apply**. The new BYOS account is added.



13. You can now associate the Storage account to a Recording Profile (see Modifying Recording Profiles on page 66).



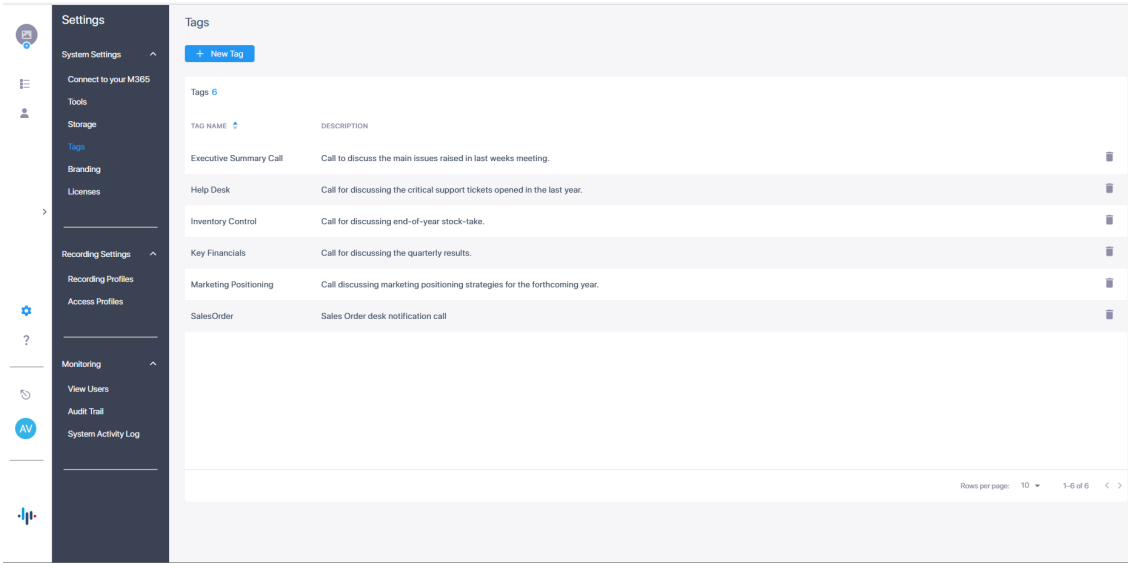
Manage Tags

Call Tags can be created by the network administrator defining tags' allowing users to enter data manually on their screen during the course of a call, or via a third-party application. A tag is a user definable label i.e. word or phrase that identifies a specific context associated to a call. The tags can then be applied to filters for quick and easy retrieval of the related context. For example, define a tag for Quarterly financial review for all calls related to the financial results reported for the quarter. Call Tagging provides the following benefits:

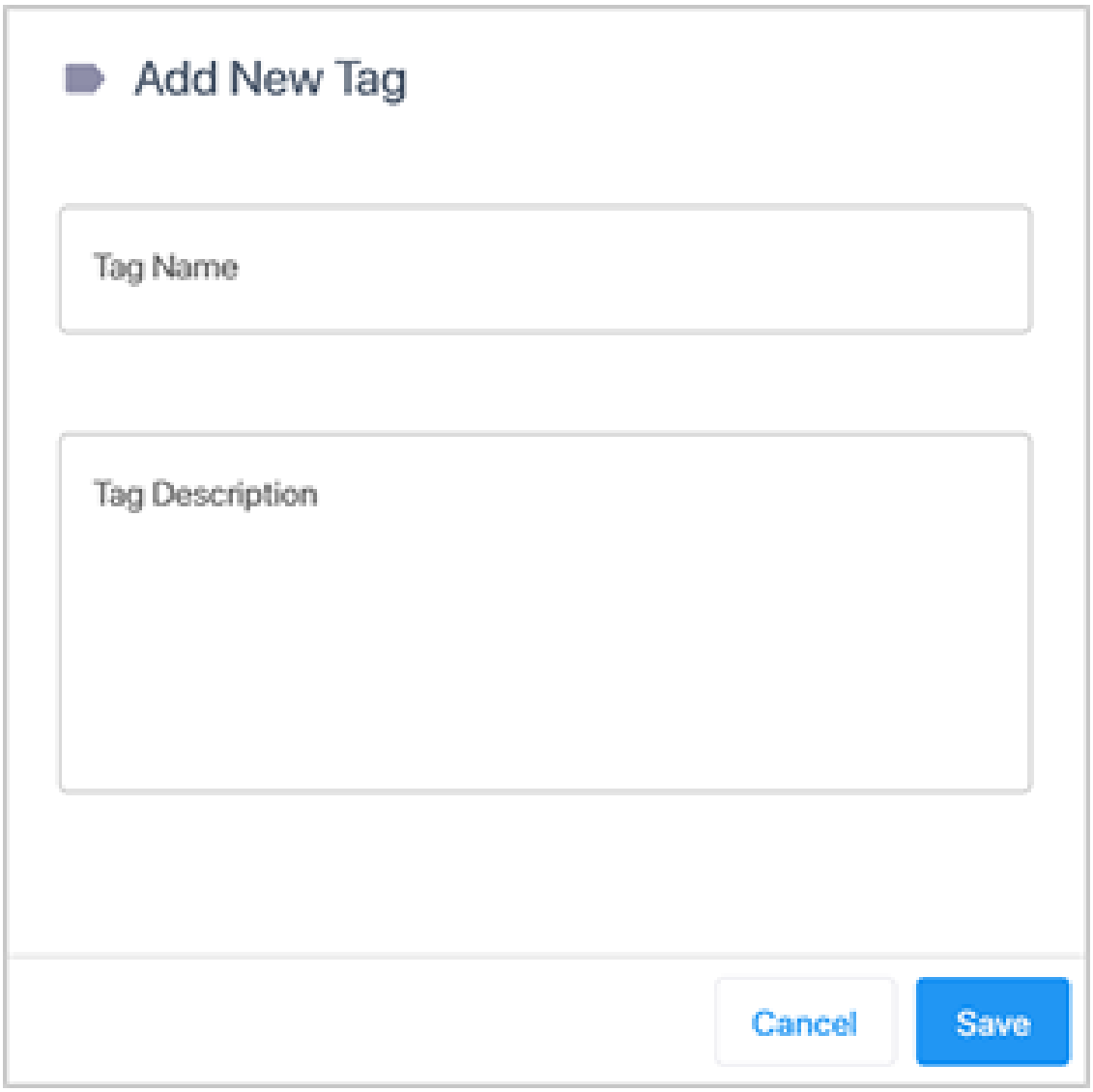
- Categorizes calls by type or outcome, making searches easy (i.e., Malicious, Account ID, etc.). By default, the Notes tag is already defined within the system.
- Saves money by dramatically reducing the time to find individual recorded calls.
- Improves internal processes by using the call tags as searchable data fields for other applications.

➢ **Do the following:**

1. In the Icon pane, click , and then select **System Settings** > **Tags**.



2. Click **New Tag** to add a new tag.

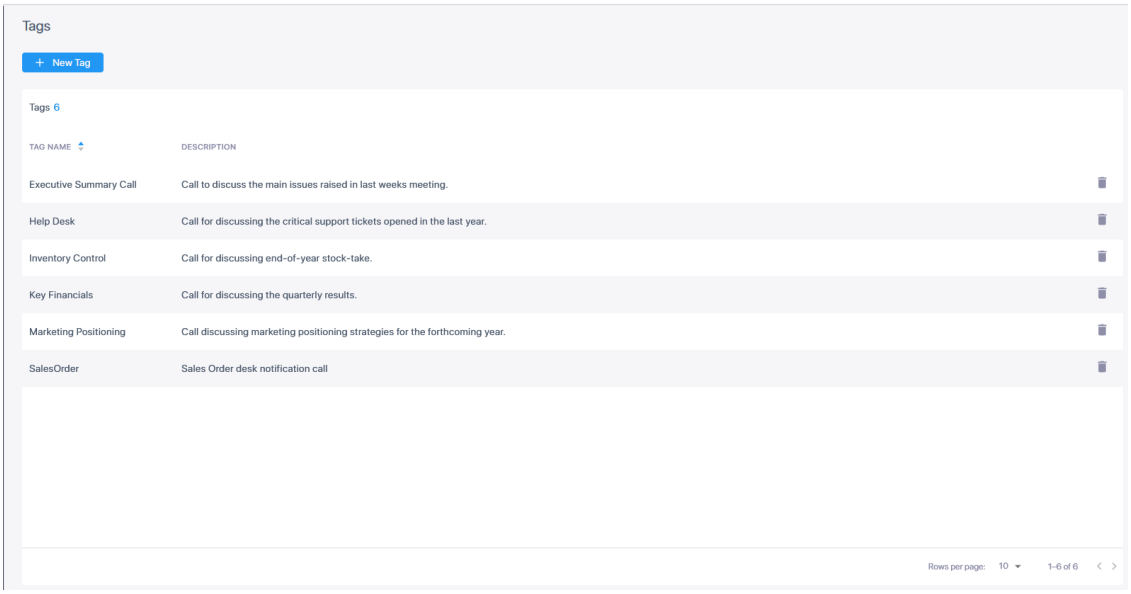


3. Enter the Tag Name and description and then click **Save**.

Table 8-1: Call Tagging Fields

Field	Description
Tag Name	Enter the tag name to the filter list.
Tag Description	Enter description of the purpose of the tag that can later be used as keyword text in search filter queries.

4. Enter the Tag name and description, and then click **Save**.

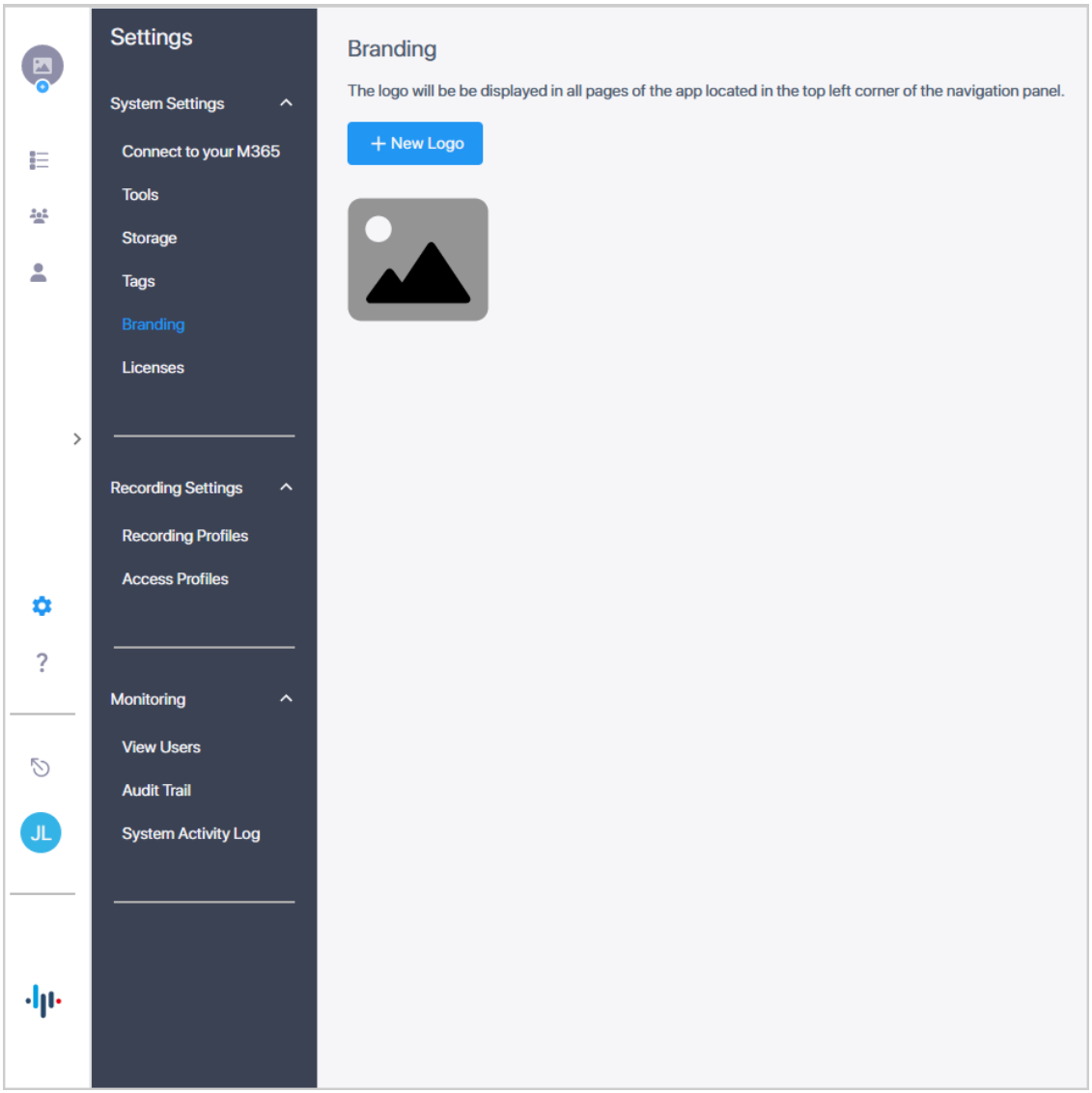


Branding

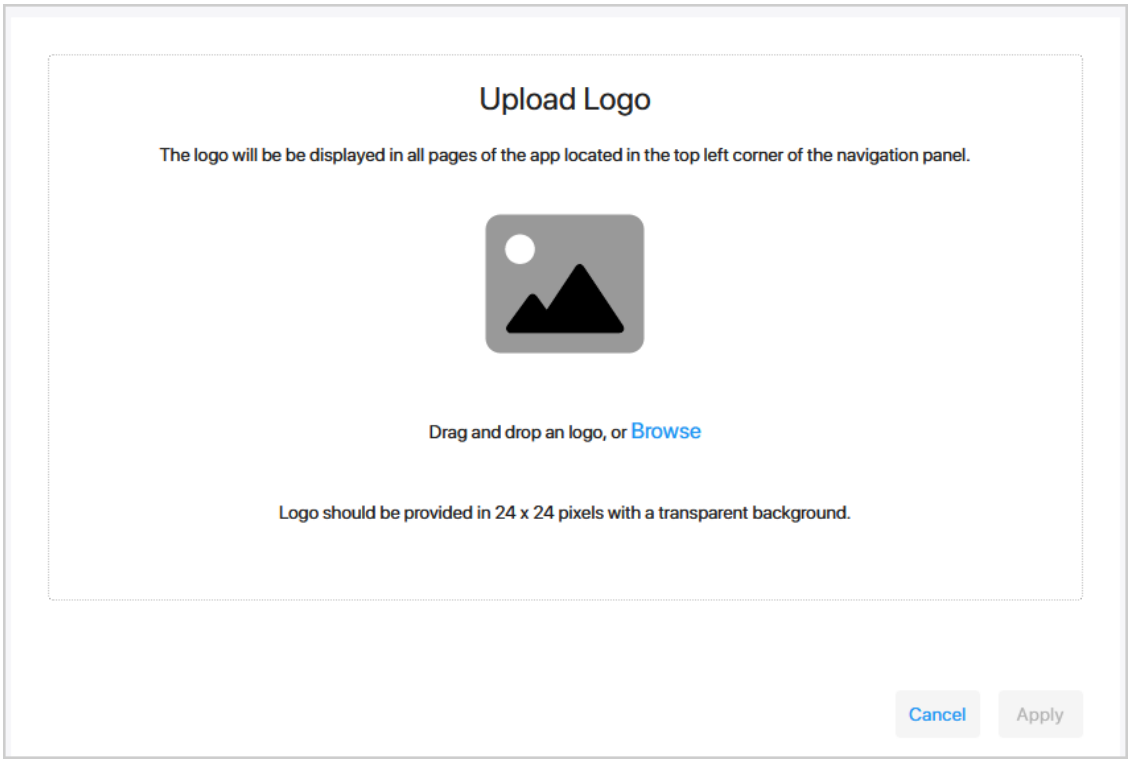
This option lets you load your Corporate logo to the application Web page. Once loaded, it is displayed in the top left corner of the interface.

➢ **Do the following:**

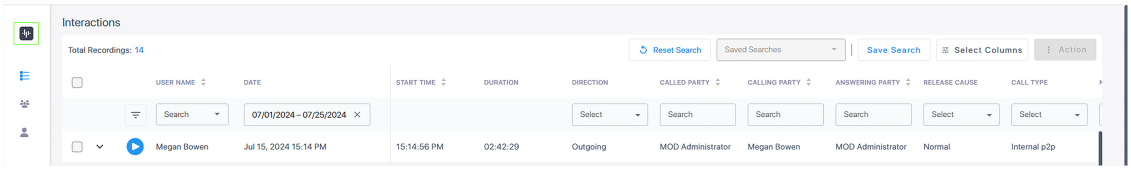
1. In the Icon pane, click , and then in the Navigation pane, select **System Settings > Branding.**



2. Click the **New Logo** button to add a new logo to the interface.



3. Drag or drop a logo or click Browse and then click **Apply**.



Licenses

This option lets you monitor the recordings licenses and Auto Sync with AAD. The page displays the number of licenses that were initially configured in the Quick Start wizard, the number of Targeted users belonging to Azure groups that are attached to Recording profiles, and the number of remaining licenses. In the figure below, 100 licenses were configured in the wizard, there are 21 licensed users belonging to attached Azure groups, and therefore the remaining number of users is 79 (100-21). When AAD groups are updated or associations with Recording Profiles are changed, the License utilization data displayed is synchronized.

- You can exceed the number of purchased licenses with pay-as-you-go option. For example, if you purchase 100 recording user licenses (minimum), you are allowed to exceed the number with a pay-as-you-go option for the average at the same price as the 100 recording user licenses.
- The customer is charged for 100 user licenses per month regardless if the licenses are in use.
- When an additional user recording license is added and at least one day has elapsed, you are charged for the entire month.

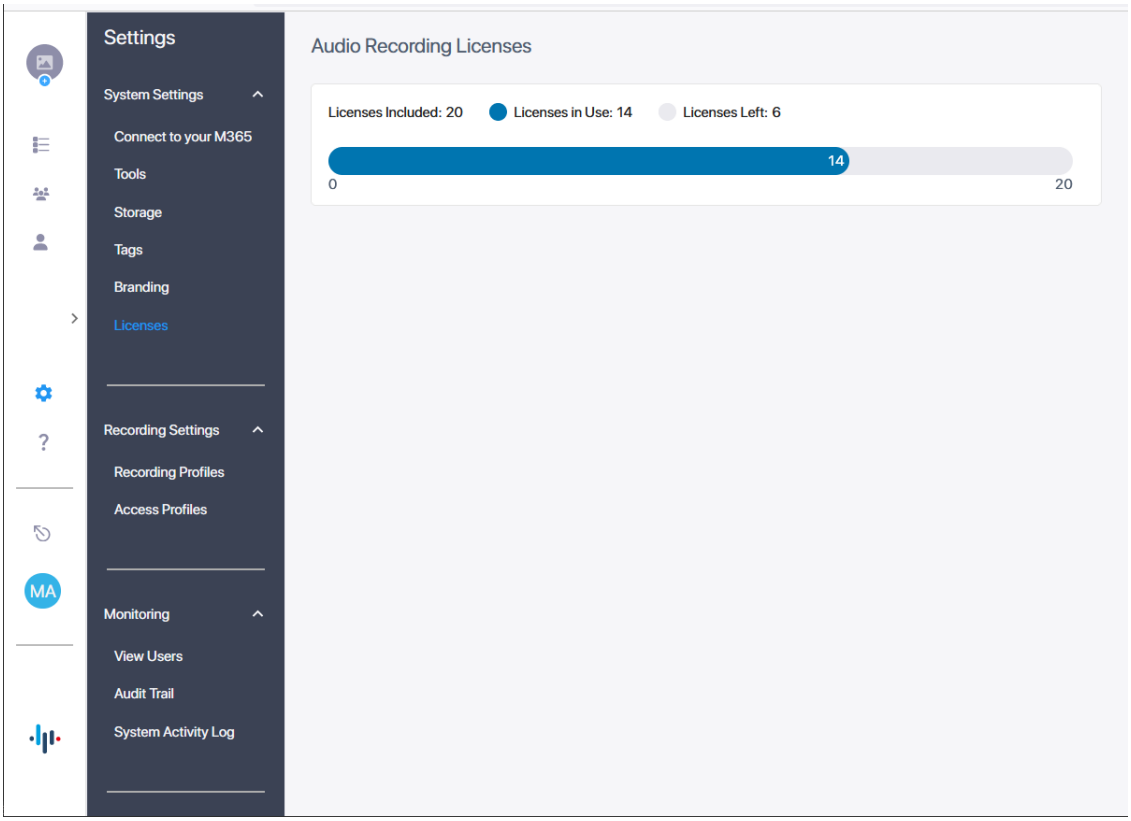
- The customer may choose Automatic or Manual license and user management (sync with AAD).

> If you add or remove users from AAD groups or add or remove AAD groups from Recording profiles, you must perform AAD Group Sync (see Synchronizing Recording Profiles on page 71) to update license data.

- **Automatic:** Automatic user license assignment and management is available for customers who are allowed to exceed the number of included user licenses. Default.
- **Manual:** Customers don't have an option to exceed the included user licenses or for customers that do have the option to exceed however they opt out from the automatic management. The assignment of the users with license is performed when you add users to a recording profile. If the customer adds users directly in AAD groups that are attached to Recording profiles, you must perform synchronization, see Synchronizing Recording Profiles on page 71.

➢ **Do the following:**

1. In the Icon pane, click , and then in the Navigation pane, select **System Settings** > **Licenses**.



The following license data is displayed.

License Parameter	Description
Licenses Included	Total number of user licenses allocated to the tenant.
Licenses in Use	Total number of active user licenses.
Licenses Left	Total number of remaining user licenses.

Monitoring

- Managing Users below
- Viewing and Searching an Audit Trail on page 172
- System Activity Log on page 175

Managing Users

This page displays users belonging to M365 groups assigned to Recording or Access profiles or who were previously assigned and have been unmapped for whatever reason. You can search and sort users according to their associated profiles and groups and place users on Legal Hold.

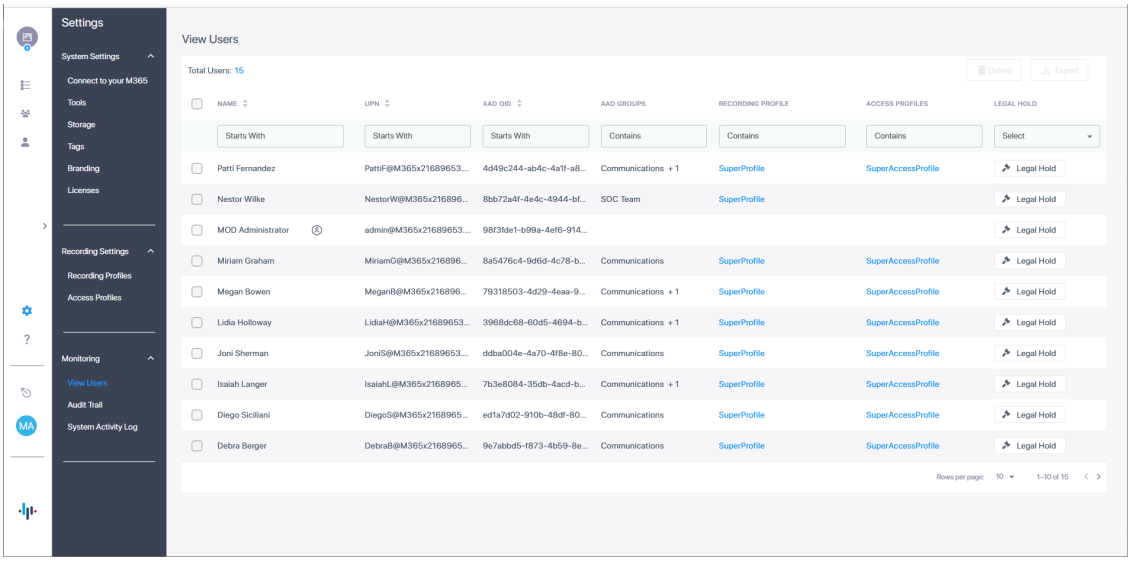
- Users cannot be deleted if they are mapped to a Recording profile, until their associated recordings are deleted, or the Retention period for the recordings expires or they are placed on Legal Hold.
- When a user is placed on Legal Hold, all of their associated calls are also placed on Legal Hold and cannot be deleted.

See also:

- Exporting Users on the next page
- Deleting Users on page 169
- Placing a User on Legal Hold on page 170

➢ **Do the following:**

1. In the Icon pane, click , and then in the Navigation pane, select **Monitoring** > **View Users.**



2. Click adjacent to the user that you wish to modify.

3. Configure fields according to the table below.
4. Click to apply changes.

Field	Description	Filters
Name	The name of the M365 tenant user.	This field can be sorted in ascending or descending order by clicking header up or down arrows. If defined, the field entry displays only matching entries.
UPN	The email address of the M365 tenant user.	This field can be sorted in ascending or descending order by clicking header up or down arrows. If defined, the field entry displays only matching entries.
AAD OID	Object ID of the user in the Azure Active Directory of the M365 customer tenant	This field can be sorted in ascending or descending order by clicking header up or down arrows respectively. If defined, the field entry displays only matching entries.
AAD Groups	Indicates the M365 tenant groups that are assigned to the user.	Start typing the text of the desired Group name in the search field.
Recording Profile	Indicates the Recording profile that is assigned to the user.	Start typing the text of the desired Recording Profile in the search field.
Access Profile	Indicates the Access profile that is assigned to the user.	Start typing the text of the desired Access Profile in the search field.
Legal Hold	Indicates whether the Legal Hold is enabled for the user. Click the button adjacent to the user that you wish to place under Legal Hold.	From the Select drop-down list, select whether to display calls on Legal Hold or not.

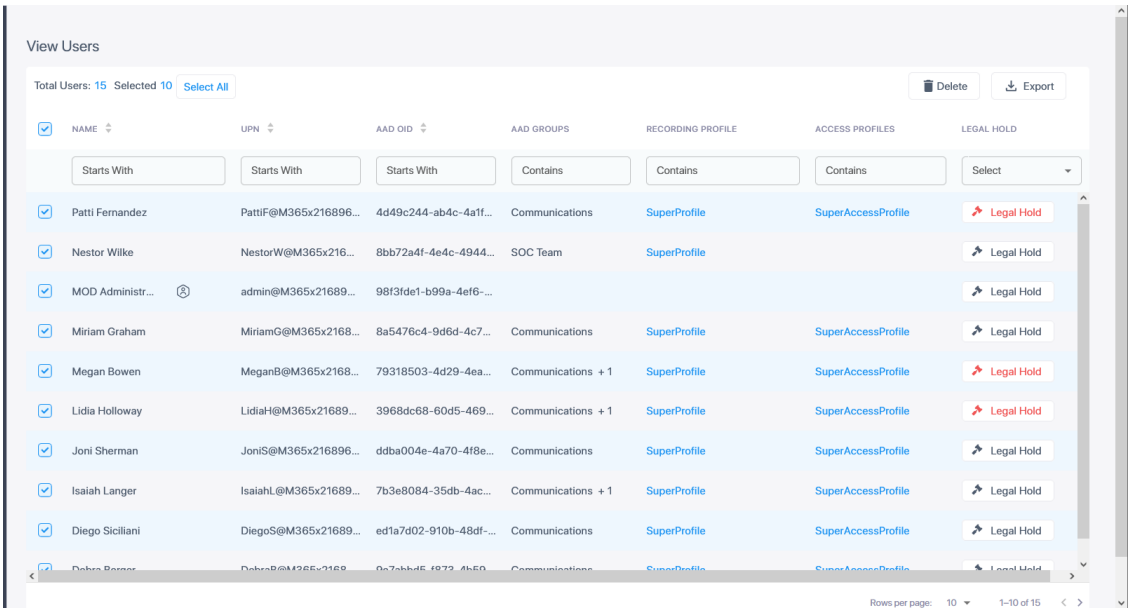
Exporting Users

You can export a list of users to an Excel or PDF file.

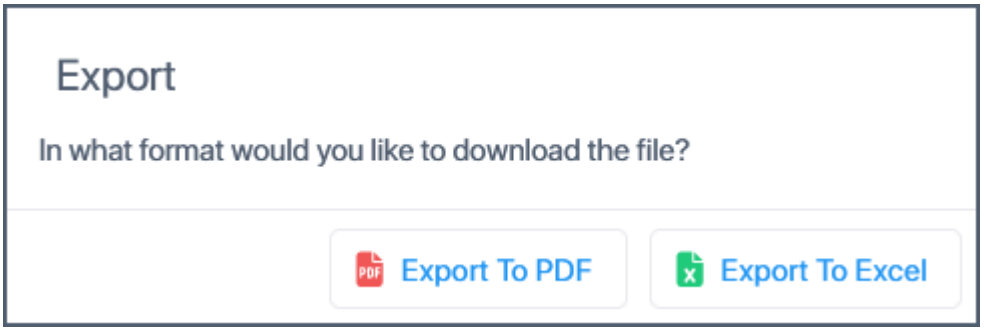
➢ **To export users:**

1. In the Icon pane, click , and then in the Navigation pane, select **Monitoring** > **View Users.**

2. Select the check box adjacent to the users that you wish to export or select the Name check box.



You are prompted whether you wish to **Export to PDF** or **Export to Excel**.



3. Choose one of the options.

The file is exported. See example of the exported data below.

```
Name    AAD OID    UPN    Recording Profile    Access Profiles    AAD
Groups    Admin    Legal Hold

MOD Administrator    98f3fde1-b99a-4ef6-914d-
03464f7ccfad    admin@M365x21689653.onmicrosoft.com                TRUE
FALSE

Diego Siciliani    ed1a7d02-910b-48df-809b-
941456b22702    DiegoS@M365x21689653.OnMicrosoft.com    SuperProfile    Sup
erAccessProfile    Communications    FALSE    FALSE

Megan Bowen    79318503-4d29-4eaa-9a22-
a516fce884bc    MeganB@M365x21689653.OnMicrosoft.com    SuperProfile    Sup
erAccessProfile    Communications,SOC Team    FALSE    TRUE
```

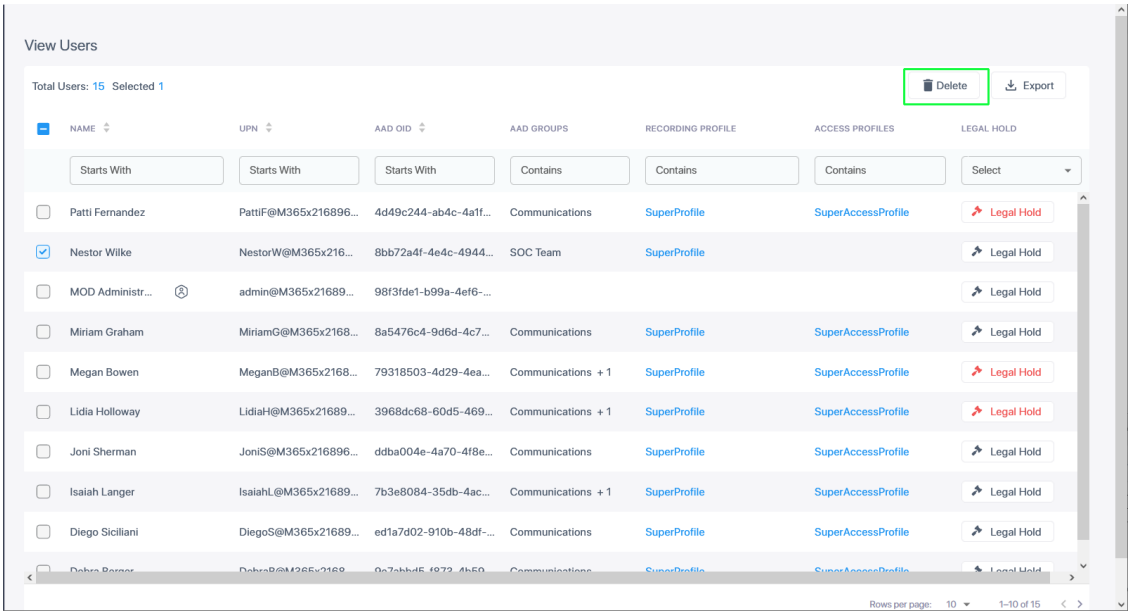
```
Patti Fernandez    4d49c244-ab4c-4a1f-a8d3-
dbe6fb758a91    PattiF@M365x21689653.OnMicrosoft.com    SuperProfile    Sup
erAccessProfile    Communications    FALSE    TRUE

Joni Sherman    ddba004e-4a70-4f8e-80c7-
ac2f2f4a2968    JoniS@M365x21689653.OnMicrosoft.com    SuperProfile    Supe
rAccessProfile    Communications    FALSE    FALSE

Lidia Holloway    3968dc68-60d5-4694-b205-
a9778571e7af    LidiaH@M365x21689653.OnMicrosoft.com    SuperProfile    Sup
erAccessProfile    Communications,SOC Team    FALSE    TRUE

Isaiah Langer    7b3e8084-35db-4acd-bbec-
f040563cf9d0    IsaiahL@M365x21689653.OnMicrosoft.com    SuperProfile    Su
perAccessProfile    Communications,SOC Team    FALSE    FALSE

Miriam Graham    8a5476c4-9d6d-4c78-baf1-
7bf5889a251e    MiriamG@M365x21689653.OnMicrosoft.com    SuperProfile    Su
perAccessProfile    Communications    FALSE    FALSE

Debra Berger    9e7abbd5-f873-4b59-8ec8-
1bc21528654f    DebraB@M365x21689653.OnMicrosoft.com    SuperProfile    Sup
erAccessProfile    Communications    FALSE    FALSE

Nestor Wilke    8bb72a4f-4e4c-4944-bfe2-
cce2c48b685e    NestorW@M365x21689653.OnMicrosoft.com    SuperProfile
  SOC Team    FALSE    FALSE
```

Deleting Users

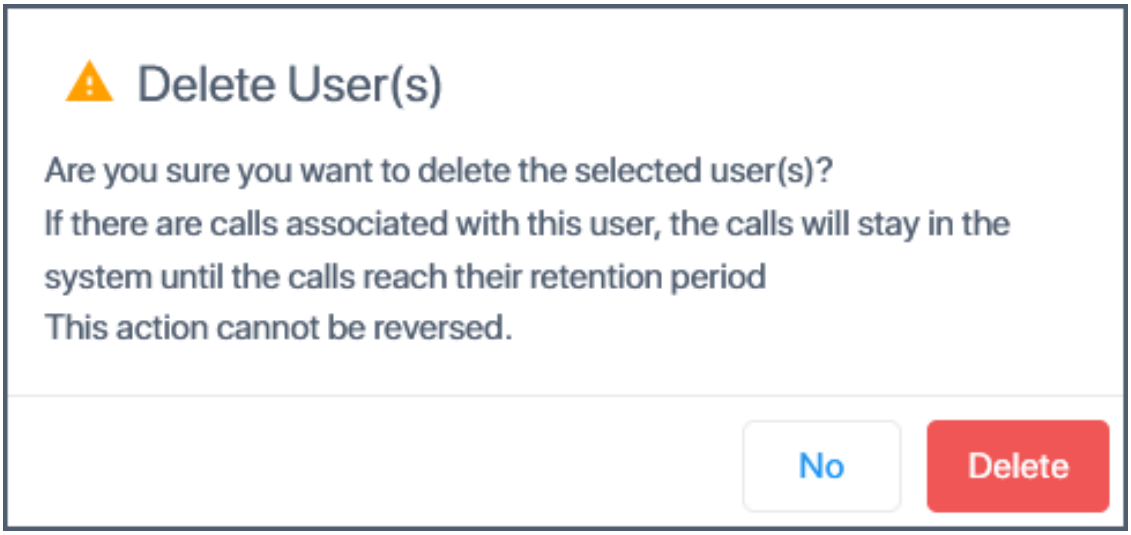
You can delete tenant users. When deleting users, any calls associated with the users remain in the database until their Retention expiration period expires.

➢ **To delete users:**

1. In the Icon pane, click , and then in the Navigation pane, select **Monitoring** > **View Users.**
2. Select the check box adjacent to the users that you wish to delete.



3. Click **Delete**.



4. Click **Delete** to confirm.

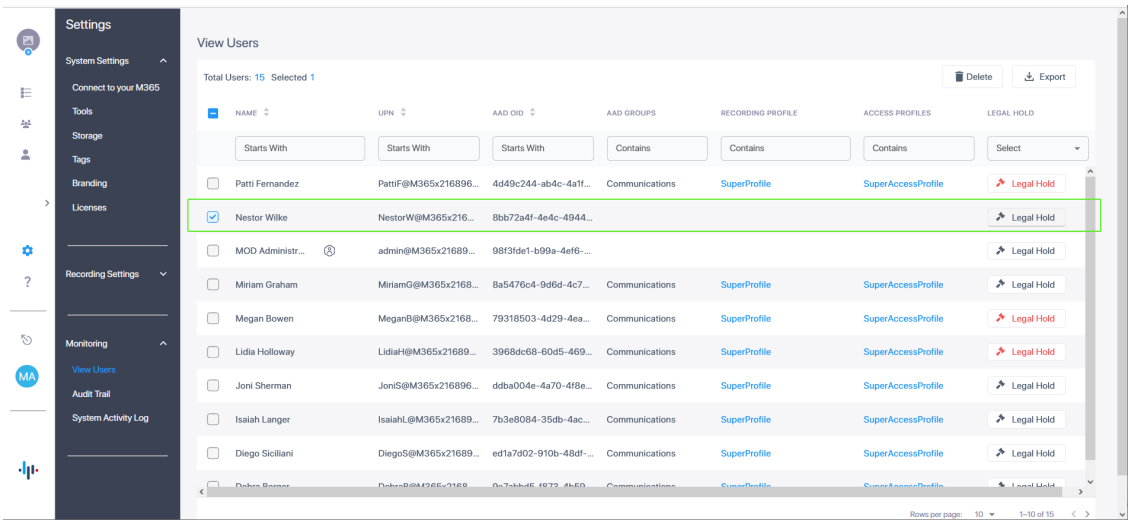
Placing a User on Legal Hold

You can place a user on Legal Hold to disable the user from making or receiving calls. During the Legal Hold period, the user cannot be deleted and their calls are not deleted even if their retention period expires. Once a user is released from legal hold, their calls are purged according to the Cleanup scheduling. For example, if the Retention period is 3 Months (90 Days), the users' calls are placed on Legal Hold on June 1 2024, and then released on August 1 2024, then their calls are retained until September 1 2024.

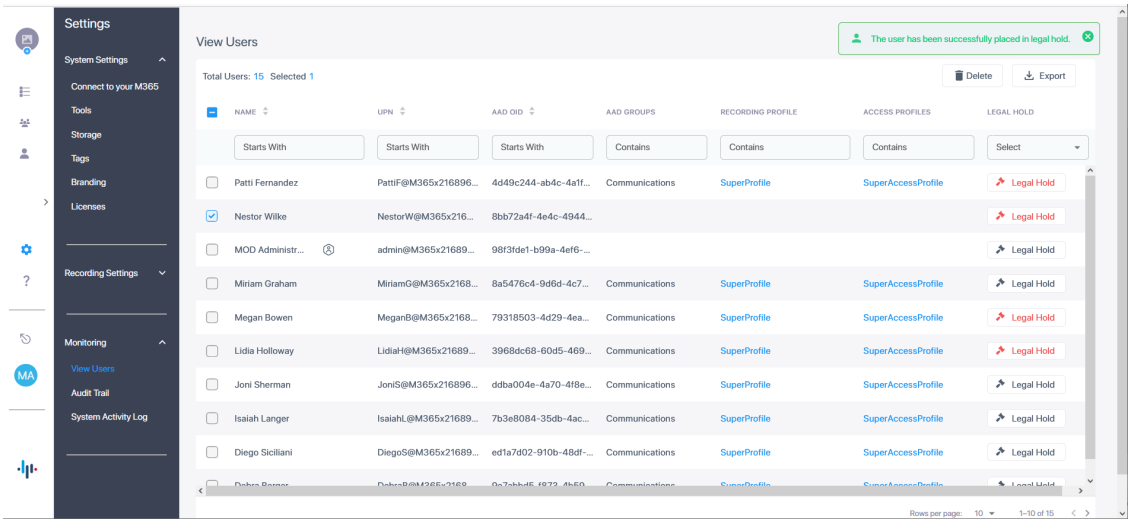
➢ To place a user on legal hold:

1. In the Icon pane, click , and then in the Navigation pane, select **Monitoring** > **View Users.**

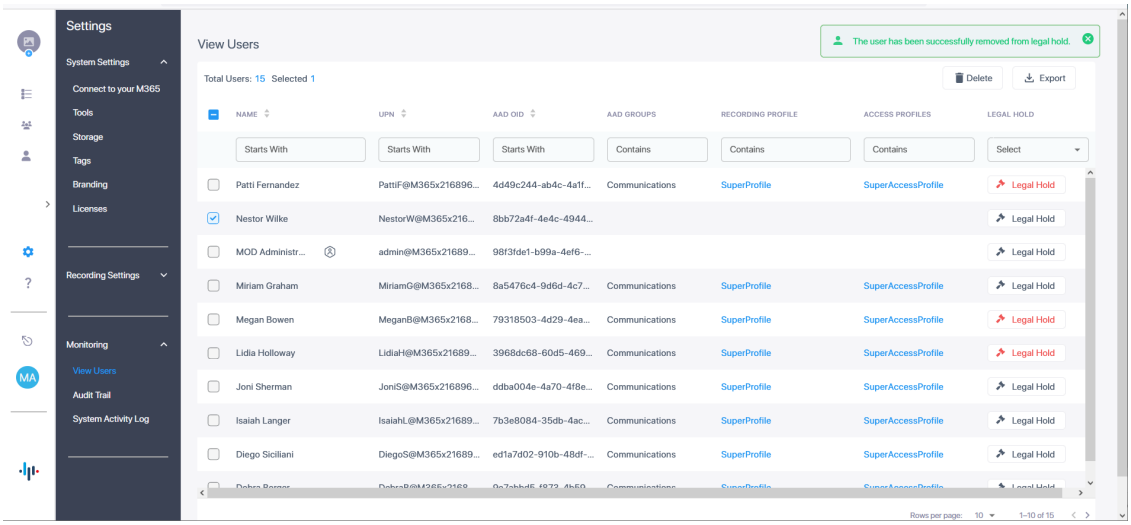
2. Select the check box adjacent to the user that you wish to place on Legal Hold, and then click the **Legal Hold** button.



A confirmation message is displayed.



3. Click again to remove the user from Legal Hold. A confirmation message is displayed.

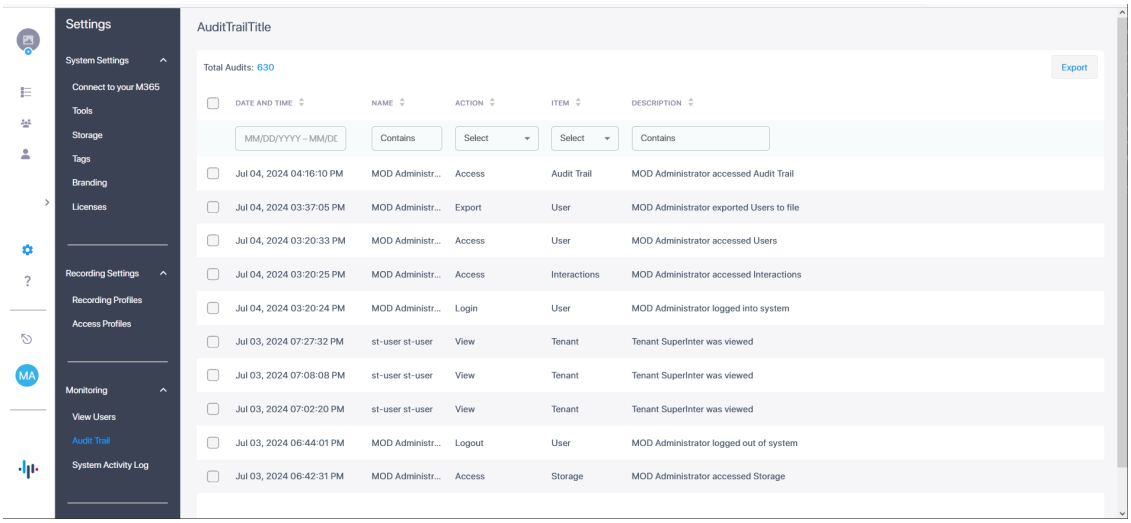


Viewing and Searching an Audit Trail

The Audit Trail feature allows the administrator to search the history of all user activity on AudioCodes Live SmartTAP. The Audit Trail is searchable but cannot be edited or deleted. You can view and search the user changes made to the AudioCodes Live SmartTAP database.

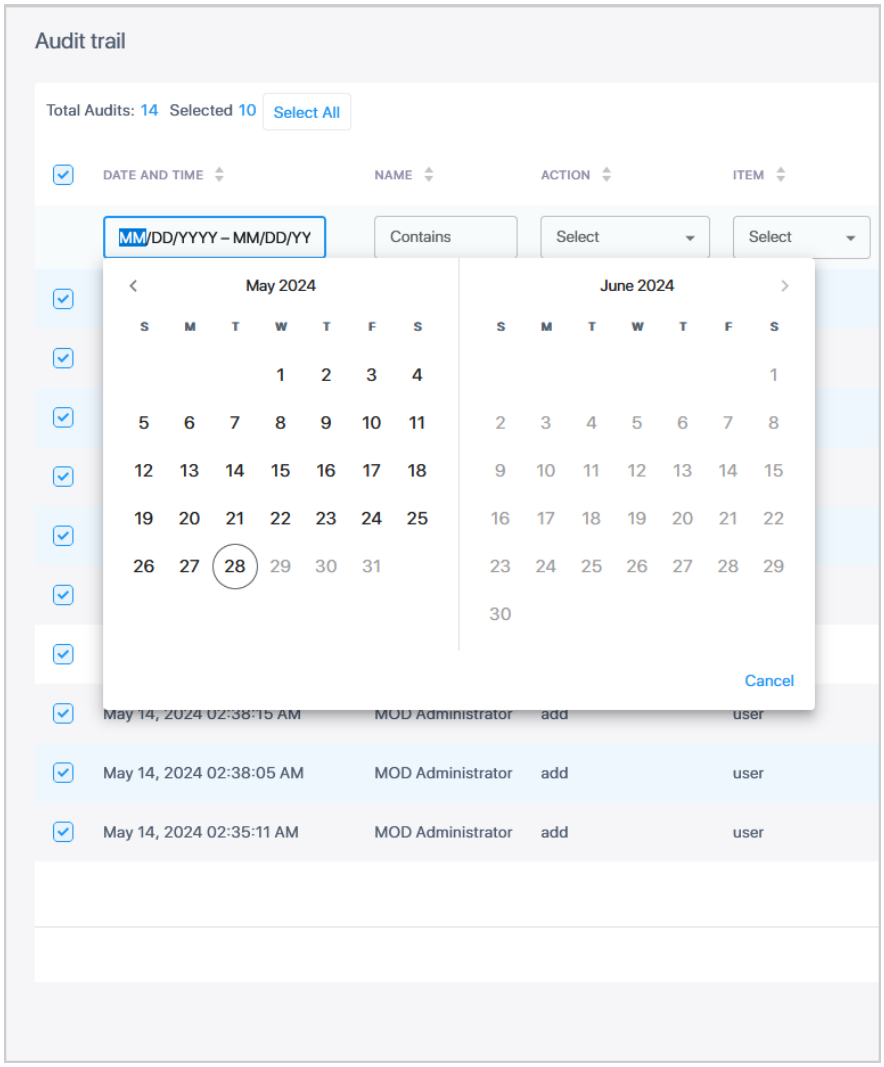
➢ **Do the following:**

1. In the Icon pane, click , and then in the Navigation pane, select **Monitoring** > **Audit Trail.**



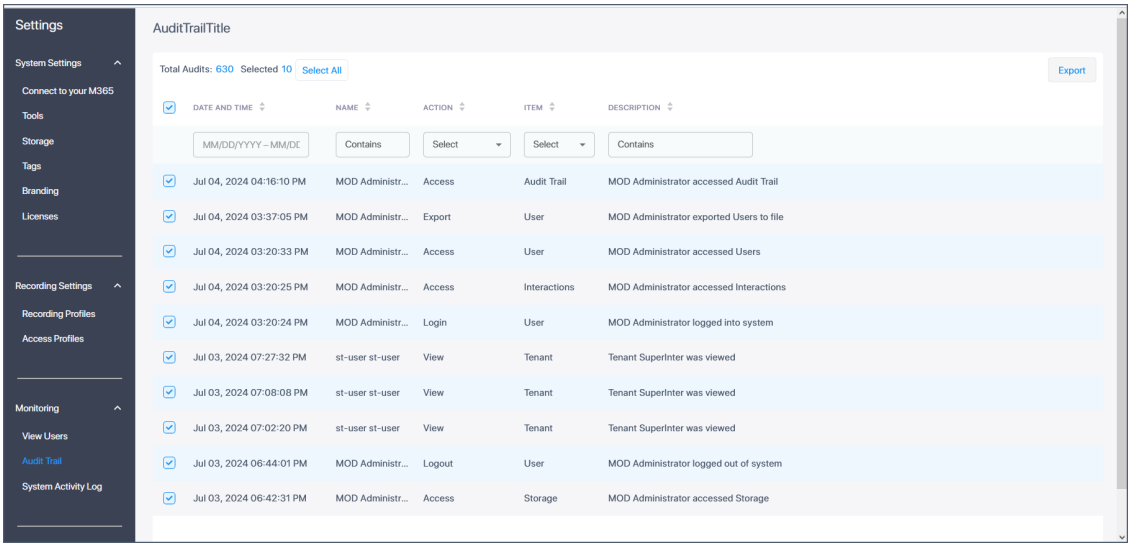
2. Set the search filter criteria according to the table below.

Parameter	Description
Date and Time	Select the **Date and Time** check box, and then from the calendar set the desired date range.

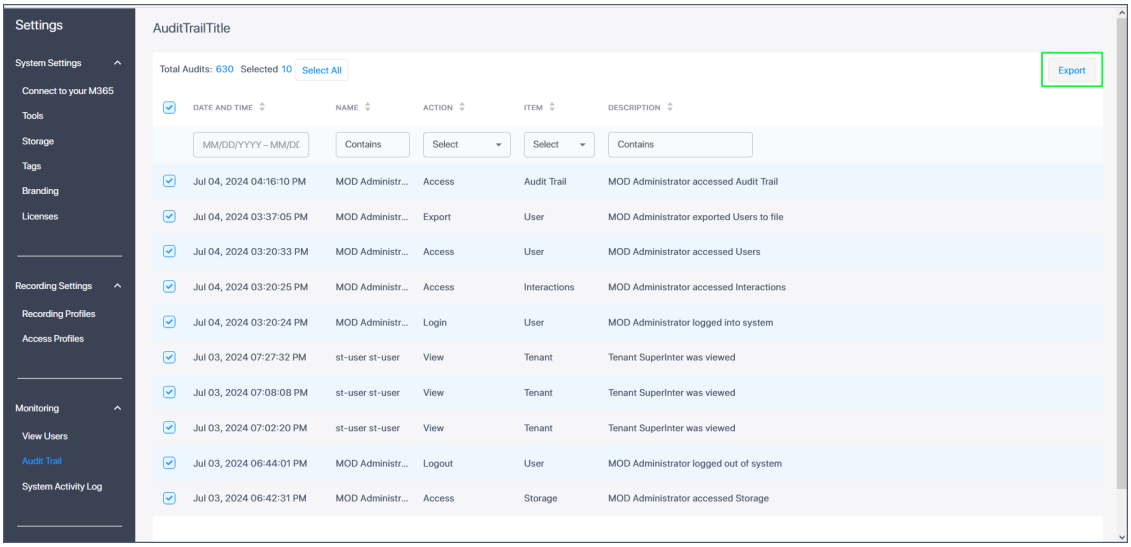
Parameter	Description
	
Name	M365 Tenant user performing the action. For example Alex Wilber. Hover over the name to display the UPN e.g. AlexW@M365x21689653.OnMicrosoft.com
Action	From the drop-down list, choose one of the following actions: ■ Login- – user logged in the system ■ Logout-user logged out of the system ■ Add-an item(s) was added ■ Modify-an item(s) was modified ■ View-an item was viewed ■ Delete-an item(s) was deleted ■ Export-an item was exported

Parameter	Description
	■ Play-an item was played ■ Send Mail (currently not supported) ■ Disabled-an item was disabled.
Item	From the Drop-down list choose one of the following entities upon which one of the above actions was performed: ■ Recording Profile ■ Access Profile ■ Group ■ User ■ Call ■ Tag ■ Note ■ Tenant ■ Legal Hold ■ Auto Sync with AAD
Description	Enter free text to search in descriptions.

3. To export the Audit Trail for accountability purposes, select the entries that you wish to export or select the check box adjacent to the Date and Time search field.

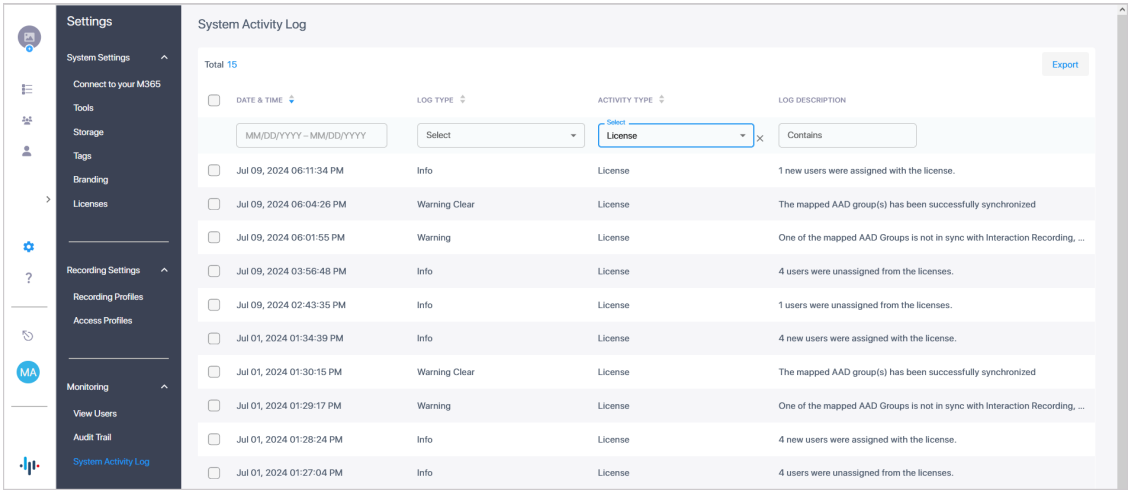


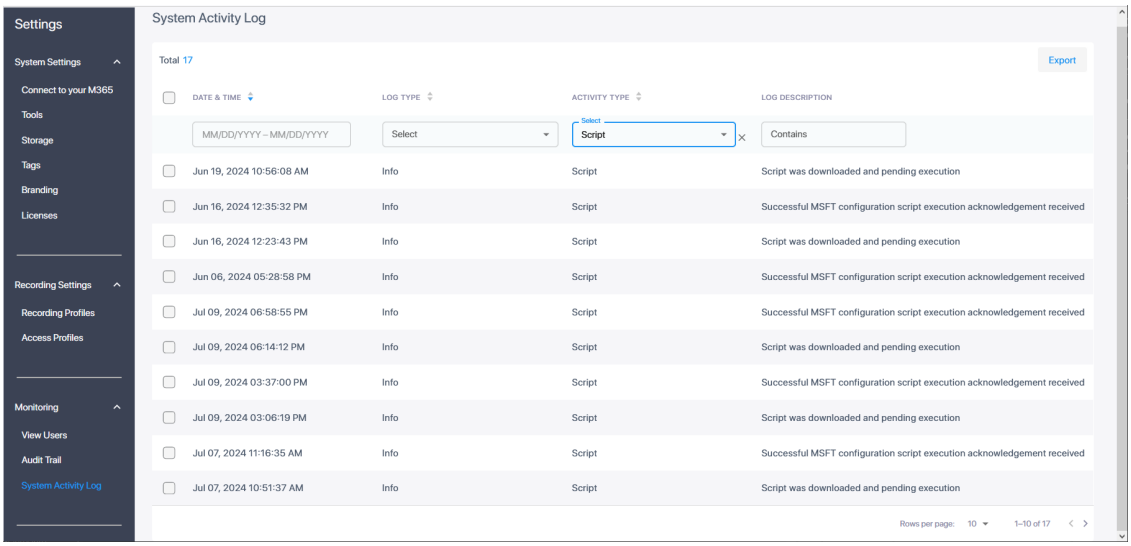
4. Click **Export**.



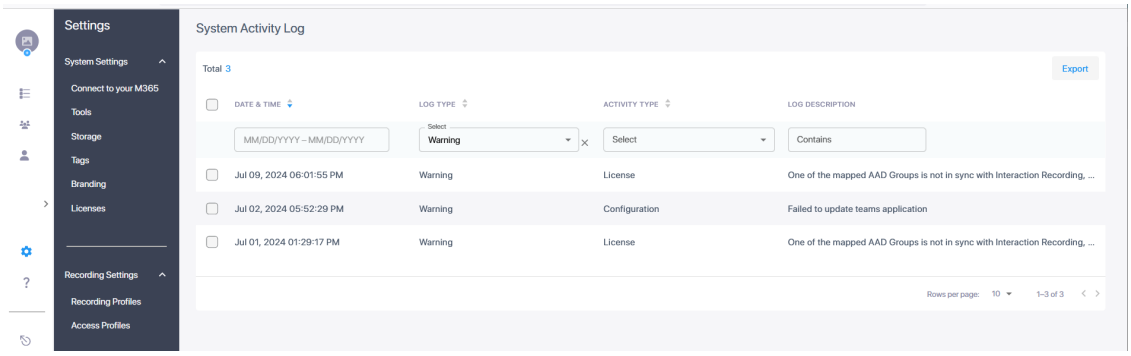
System Activity Log

The System Activity Log lets you monitor system tasks for activities of the system. The figures below display filtered views for the License and Script logs.



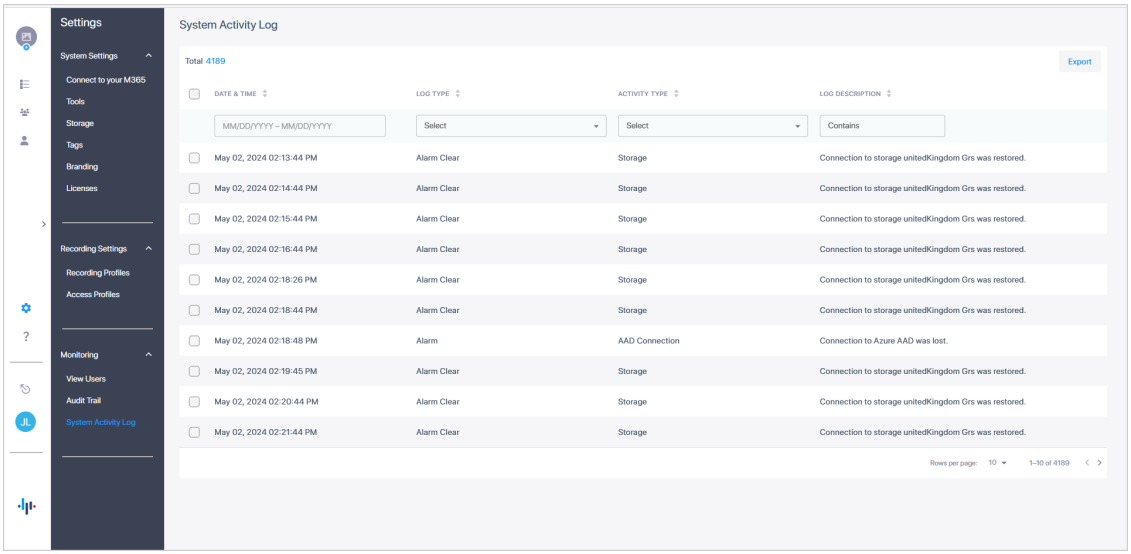


The following figure displays a Filtered view for Warning messages.



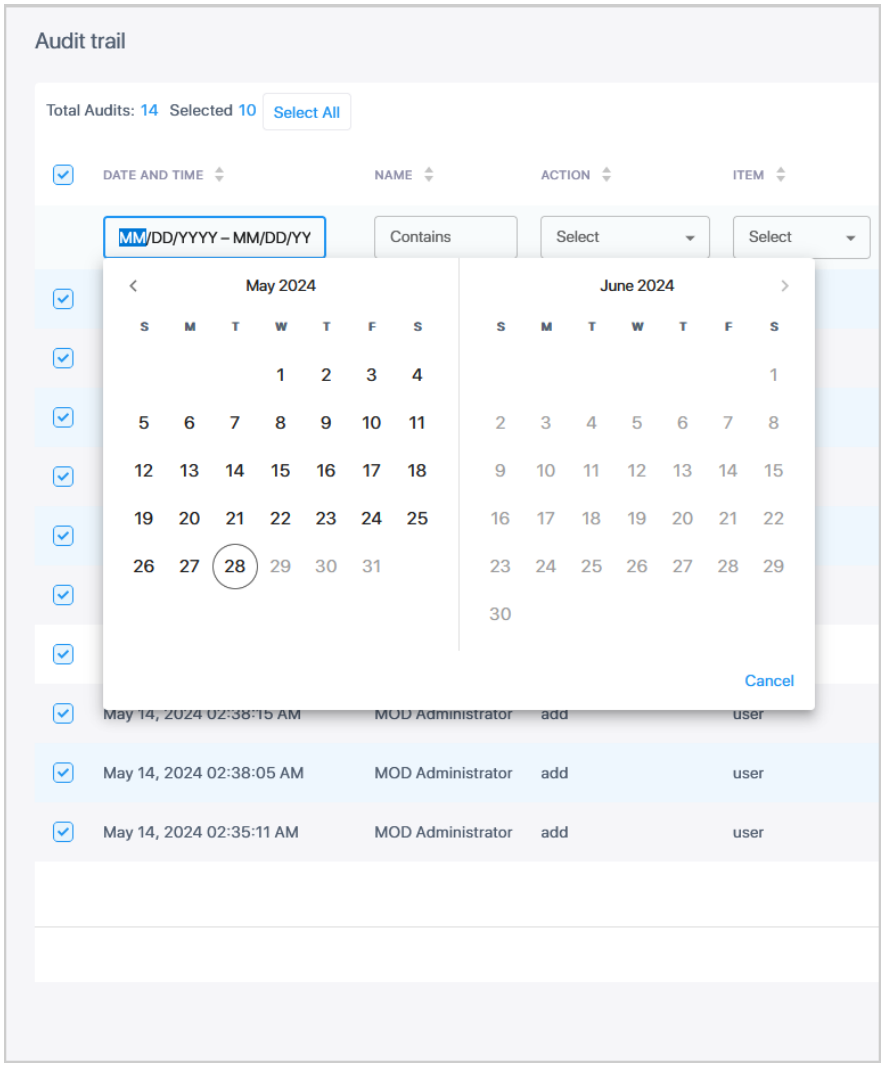
➢ Do the following:

1. In the Icon pane, click , and then in the Navigation pane, select **Monitoring** > **System Activity Log**.



2. Set the Search criteria according to the table below.

Parameter	Description
Date and Time	Select the **Date and Time** check box, and then from the calendar set the desired date range.

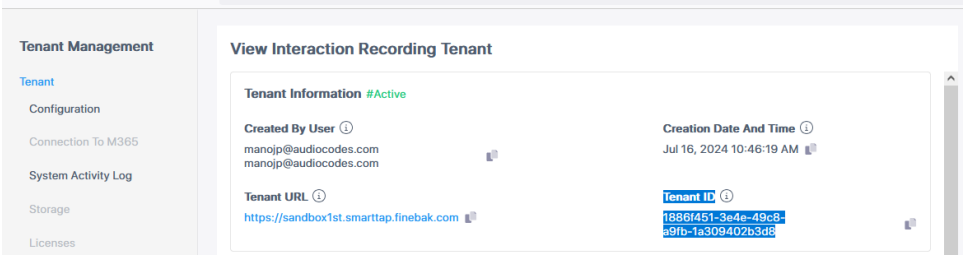
Parameter	Description
	
Log Type	From the drop-down list, choose one of the following values: ■ Info ■ alarm ■ alarm Clear ■ warning ■ warning Clear ■ error ■ errorClear
Activity Type	From the drop-down list, choose one of the following values: ■ License: Monitors user license assignments.

Parameter	Description
	■ Storage: Monitors status of connection to storage accounts. ■ Configuration: Monitors consent actions (see Connect to M365 on page 146) ■ AAD Connection: Monitors connection with your M365 platform. ■ AAD Sync: Monitors status of AAD synchronization (see Synchronizing Recording Profiles on page 71) ■ Script: Monitors status of Microsoft script download and execution (see Download and Run Microsoft Script on page 73)
Log Description	Description of the log event. Enter text in the search field to search for a word or phrase matching an event description.

Alarms

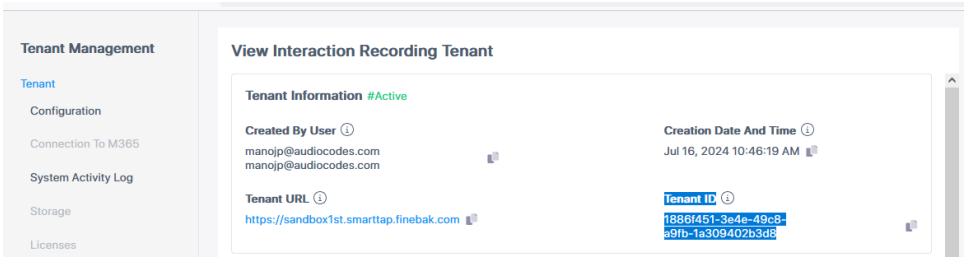
This section describes the alarms that are raised on the SmartTAP server and sent to the OVOC interface.

Recording Resource Unavailable

Alarm Field	Description		
Description	This alarm is sent when Bot fails to record a call due to Graph API error.		
SNMP Alarm	RecordingResourceUnavailable		
SNMP OID	.1.3.6.1.4.1.5003.9.40.3.2.0.100		
Alarm Source	<Unique Service Id>/Bot Where unique service Id is the Tenant Id for the service. View the service to match the Id. 		
Alarm Title	Recording Resource Unavailable		
Alarm Type	Other		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Critical	Bot receives Graph Api error when trying to join call and access media stream.	<Graph API error that was returned>	Grant consent for the Teams Bot to record calls (in the SmartTAP Web interface go to either the Quick Start wizard or the Connect to your M365 Platform page). Try to record a call.

Alarm Field	Description		
Cleared	Bot is able to join call and record media for this tenant.		

Connection Failed

Alarm Field	Description		
Description	This alarm is generated when the application fails to connect to customer Entra ID (AAD) or to customer provided storage account (BYOS).		
SNMP Alarm	ConnectionFailed		
SNMP OID	.1.3.6.1.4.1.5003.9.40.3.2.0.101		
Alarm Source	■ <Unique Services Id>/Sync ■ <Unique Services Id>/<StorageFriendlyName>-SystemConfiguration 		
Alarm Title	Connection Failed		
Alarm Type	Communications Alarm		
Probable Cause	Other		
Additional Info			
Alarm Severity	Condition	<text>	Corrective Action
Critical	■ Service has been successfully added on Live Platform; however the customer has not yet provided consent for connecting to their M365 platform. ■ Sync service communication to customer AAD has failed.	Connection to AAD failed, please provide ensure to consent for the application to read AAD groups and users.	■ Complete the Quick Start wizard, providing all consents and run the Microsoft Quick Start script (see Quick Start on page 15). ■ Perform Sync Groups to AAD action in SmartTAP Web interface Access Profiles page.
Critical	SystemConfiguration failed to connect to customer provided storage account	Connection To Storage <StorageFriendlyName > Lost	■ Check that the Blob SAS URL has been configured correctly in the IR Web Storage screen. In addition, check its' Expiry period. Regenerate and update in Storage screen if necessary. ■ Check that access to the storage account is not blocked by firewall.
Cleared	■ Sync service communication to customer AAD succeeded ■ SystemConfiguration service successfully connected to customer provided storage	-	-

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-27608