Microsoft Teams

Overview

If your organization already has meeting recordings in Microsoft Teams, you can import them into Alchemer Voice for analysis. Alchemer Voice reviews the calendars of team members who are Alchemer Voice users, identifies recorded meetings that include participants from outside your company, and imports those meetings into your catalogue.

This article explains how to give Alchemer Voice access to retrieve those recordings.

How it works

Alchemer Voice uses the Microsoft Graph to access meeting transcripts and attendance data on behalf of your users. Setting up the connection has two parts:

1. Grant access from the **Connect** button on the Connections page under Admin in Alchemer Voice.
2. Configure an **application access policy** in Microsoft Teams using PowerShell.

Before you begin

- You must be a **Teams administrator** in your Microsoft 365 tenant.
- Install the Microsoft Teams PowerShell module if you have not already, or use the embedded terminal in the Azure portal.

Create the application access policy

1. Connect to Microsoft Teams PowerShell

```
Connect-MicrosoftTeams
```

2. Create the policy

```
New-CsApplicationAccessPolicy -Identity AlchemerVoice -AppIds "d4a8379f-7ee7-4c71-a02b-931b36dbe0fc"
```

This creates a policy named "AlchemerVoice" that authorizes the Alchemer Voice application to access Teams meeting data. The App ID identifies the Alchemer Voice application for Microsoft Teams. You can choose a different policy name if you prefer; use the same name in the next step.

3. Grant the policy globally

```
Grant-CsApplicationAccessPolicy -PolicyName AlchemerVoice -Global
```

This applies the policy to all users in your tenant, allowing Alchemer Voice to access meeting transcripts and attendance reports for any user.

Note: Changes to application access policies can take up to 30 minutes to take effect.

Verify the connection

After waiting up to 30 minutes, open the Connections page under Admin in Alchemer Voice and check the Microsoft Teams status. The status should change from "Authentication failed" to "Connected".

Reference

For more detail on application access policies, see Microsoft's documentation: Configure application access policy.

Related Articles