


Teams integration

Last Modified on 08/30/2024 2:46 pm IDT

 This article is designated for administrators.

About

Experience the seamless integration between Microsoft Teams and Kaltura! Our Teams integration enables you to effortlessly upload and archive your Teams recordings, ensuring everything stays neatly organized in one centralized location. As the owner and host, you'll retain full control and enjoy easy collaboration with co-hosts. Dive in now to discover how to effortlessly manage all your Teams content with Kaltura.

 Note: Only recordings of sessions defined as Teams "meetings" can be uploaded to Kaltura using this integration. Teams "calls" are not covered by Microsoft's meetings API used for this integration.

Prerequisites

Teams prerequisites:

- A paid Teams account

Kaltura prerequisites:

- KMC account and access
- Teams integration service must be enabled in Kaltura (paid service)

Notes on administrator setup

- Each Teams account is linked to a specific Kaltura account for recording transfers.

Set up Azure account

Step 1 - Request permissions

1. Navigate to the [Microsoft Azure portal](#) and sign in with your Azure account credentials.
2. In the Azure Portal's left-hand menu, click **Azure Active Directory**.
3. Under **Manage**, click **App registrations**.
4. Click **+New Registration**.

The **Register an application** page displays.

5. In the **Name** field, type in a name, for example, '*Kaltura Teams Integration*'.

Microsoft Azure Search resources, services, and docs (G+)

Home > App registrations >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

 ✓

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Kaltura only - Single tenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

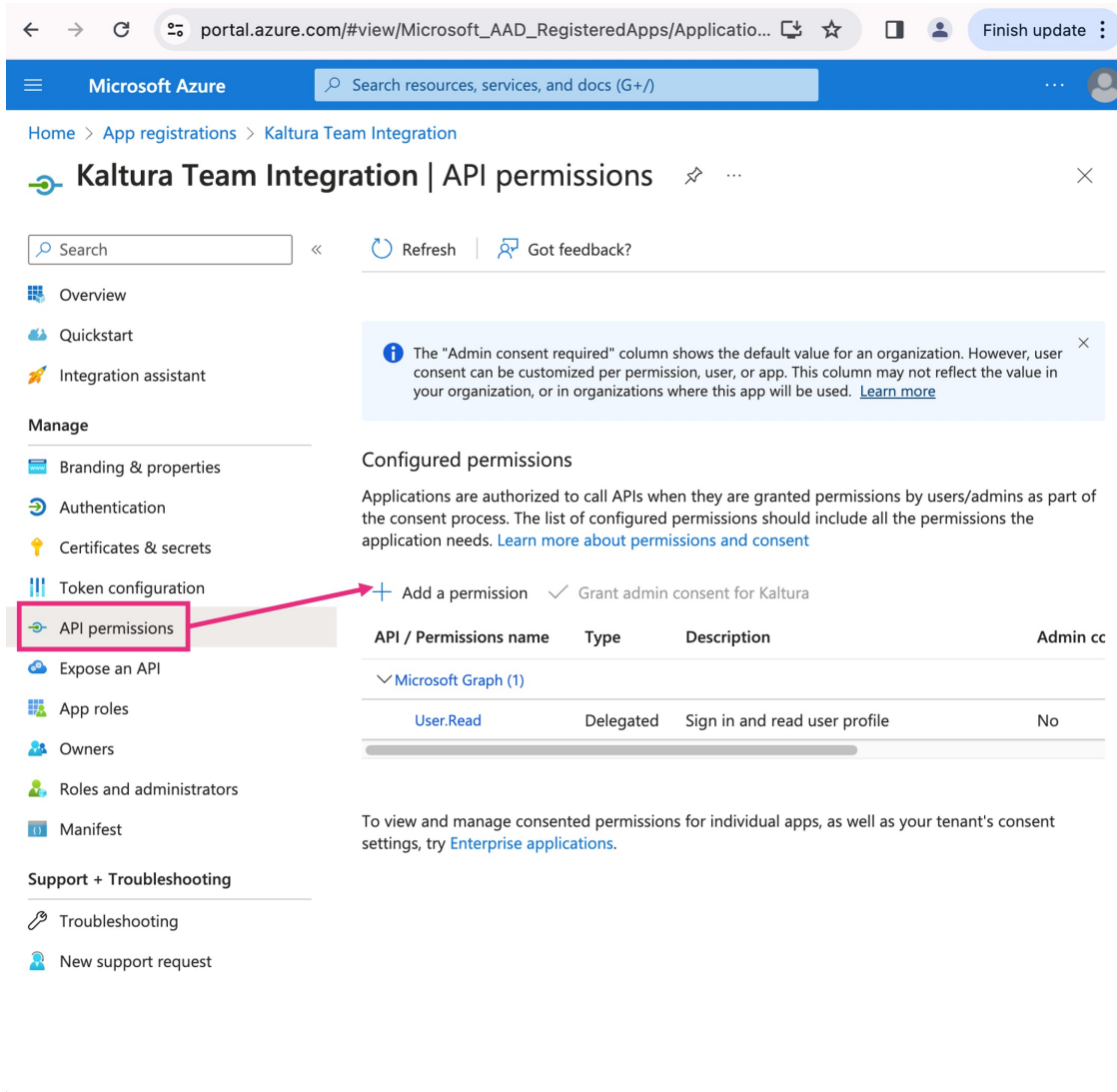
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

- At the bottom of the page, click **Register**.
The settings page displays.
- Under **Manage**, click **API permissions**.
- In the API permissions page, click **+Add a permission**.



portal.azure.com/#view/Microsoft_AAD_RegisteredApps/Applicatio... Finish update

Microsoft Azure Search resources, services, and docs (G+)

Home > App registrations > Kaltura Team Integration

Kaltura Team Integration | API permissions

Search Refresh Got feedback?

Overview
Quickstart
Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

API / Permissions name **Type** **Description** **Admin cc**

Microsoft Graph (1)

API / Permissions name	Type	Description	Admin cc
User.Read	Delegated	Sign in and read user profile	No

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

The **Request API permissions** page displays.

9. Under the **Microsoft APIs** tab, click **Microsoft Graph**.


Request API permissions




Select an API

Microsoft APIs APIs my organization uses My APIs


Commonly used Microsoft APIs

**Microsoft Graph**


Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Microsoft Entra ID, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

**Azure Communication Services**


Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams

**Azure Rights Management Services**


Allow validated users to read and write protected content

**Azure Service Management**


Programmatic access to much of the functionality available through the Azure portal

**Data Export Service for Microsoft Dynamics 365**


Export data from Microsoft Dynamics CRM organization to an external destination

**Dynamics 365 Business Central**


Programmatic access to data and functionality in Dynamics 365 Business Central

**Dynamics CRM**


Access the capabilities of CRM business software and ERP systems

**Intune**

Programmatic access to Intune data

**Microsoft Purview**

Unified data governance service that helps you manage and govern your on-premises, multi-cloud, and software-as-a-service (SaaS) data

**Office 365 Management APIs**

Retrieve information about user, admin, system, and policy actions and events from Office 365 and Microsoft Entra ID activity logs

10. Under the **Microsoft Graph** tab, click **Application permissions**.
11. Under **Select permissions**, check the checkbox for each of the following permissions:
 - a. OnlineMeetingRecording.Read.All
 - b. OnlineMeetings.Read.All
 - c. OnlineMeetingTranscript.Read.All
 - d. User.ReadBasic.All

Request API permissions

[← All APIs](#)

Microsoft Graph
<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

Permission	Admin consent required
> AccessReview	
> Acronym	
> AdministrativeUnit	
> AgreementAcceptance	
> Agreement	
> APIConnectors	

Add permissions
Discard

12. Finally, at the bottom of the page, click **Add permissions**

13. The configured permissions display with the status *Not granted for [your company name]*. Permissions require the administrator's consent. Once granted, status will display as *Granted for [your company name]*.

Home > [App registrations](#) > [Kaltura Team Integration](#)

[Company Team Integration](#) | API permissions ✕

« Refresh | [Got feedback?](#)

Overview

- [Quickstart](#)
- [Integration assistant](#)

Manage

- [Branding & properties](#)
- [Authentication](#)
- [Certificates & secrets](#)
- [Token configuration](#)
- [API permissions](#)
- [Expose an API](#)
- [App roles](#)
- [Owners](#)
- [Roles and administrators](#)
- [Manifest](#)

Support + Troubleshooting

- [Troubleshooting](#)
- [New support request](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

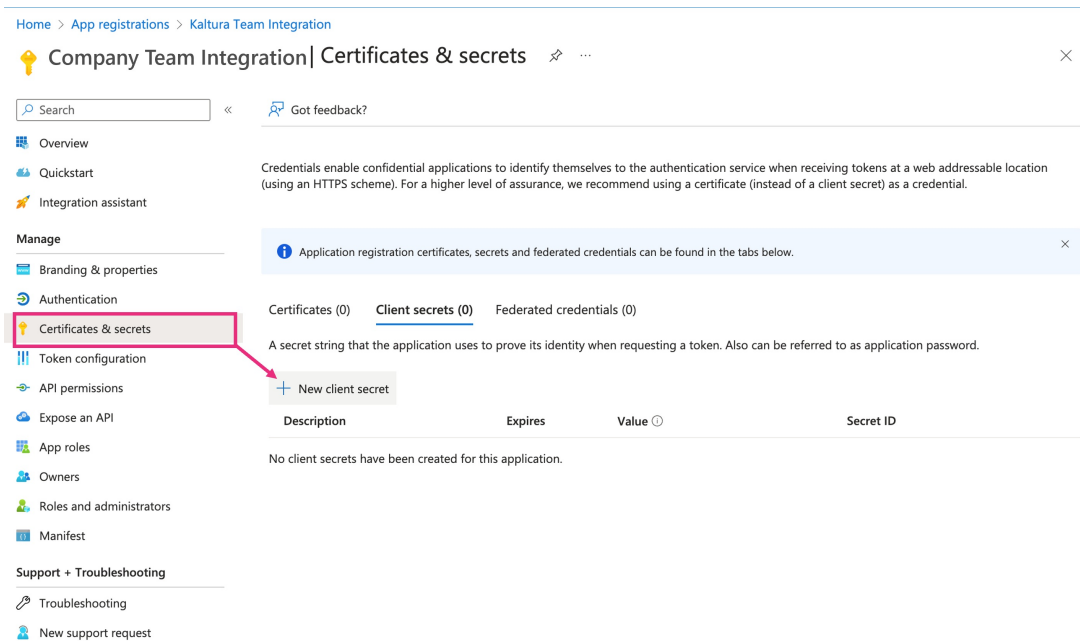
[+ Add a permission](#) ✓ Grant admin consent for Kaltura

API / Permissions name	Type	Description	Admin consent req...	Status
▼ Microsoft Graph (5)				
OnlineMeetingRecording	Application	Read all recordings of online meetings.	Yes	✔ Granted for Company
OnlineMeetings.Read.All	Application	Read online meeting details	Yes	✔ Granted for Company
OnlineMeetingTranscript	Application	Read all transcripts of online meetings.	Yes	✔ Granted for Company
User.Read	Delegated	Sign in and read user profile	No	✔ Granted for Company
User.ReadBasic.All	Application	Read all users' basic profiles	Yes	✔ Granted for Company

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Step 2 - Create a client secret

1. In the left-hand menu under **Manage**, click **Certificates and Secrets**.
2. Click **+New client secret**.



Home > App registrations > Kaltura Team Integration

Company Team Integration | Certificates & secrets

Search << Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (0)** Federated credentials (0)


A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
No client secrets have been created for this application.			

The **Add a client secret** window displays.

3. In the **Description** field, type in a description.
4. In the **Expires** field, choose a time period from the drop-down menu.

 Please note that while updating the secret in Kaltura isn't available at the moment, it's planned for the near future. In the meantime, we recommend selecting a longer expiry date.

5. Click **Add** to create the client secret.

Home > App registrations > Kaltura Team Integration

Company Team Integration | Certificates & secrets

Search << Got feedback?

- Overview
- Quickstart
- Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Application registration certificates, secrets and federated credentials

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates (0) **Client secrets (0)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires
No client secrets have been created for this application.	

Add a client secret [X]

Description:

Expires:

After adding the client secret, Azure will generate a new client secret value.

Important: Copy the client secret **value** and save it securely. You won't be able to see this value again after leaving this page.

Home > App registrations > Kaltura Team Integration

Company Team Integration | Certificates & secrets

Search << Got feedback?

- Overview
- Quickstart
- Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Got a second to give us some feedback? →

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
Default secret	4/4/2026	12L9G~7rBIVCerdS.PhrdMsew	081kkr5s~44ba~59g3~fh9t~3f

6. Click on the **Overview** tab to view your credentials which you will need for the configuration in KMC.

Home > App registrations > **Kaltura Teams Integration** ✨ ...

Search << Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request


Essentials

Display name Kaltura Teams Integration	Client credentials 0 certificate, 1 secret
Application (client) ID [blurred]	Redirect URIs Add a Redirect URI
Object ID [blurred]	Application ID URI Add an Application ID URI
Directory (tenant) ID [blurred]	Managed application in local directory Kaltura Teams Integration
Supported account types My organization only	

[Get Started](#) Documentation

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)



Step 3 - Configure an application access policy

To configure an application access policy and allow applications to access online meetings with application permissions, please follow the instructions provided in [Configure application access policy](#).

You'll need to follow steps 1, 2, and 3, then skip step 4 and proceed to step 5. Below are example commands:

Connect to Microsoft Teams PowerShell

```
Connect-MicrosoftTeams
```

Create Application Access Policy

```
New-CsApplicationAccessPolicy -Identity Teams-policy -AppIds "REPLACE_WITH_APP_ID" -Description "Upload Teams recordings to Kaltura"
```

Grant the policy globally

```
Grant-CsApplicationAccessPolicy -PolicyName Teams-policy -Global
```

Step 4 - Enable metered API on Microsoft Graph

To utilize Microsoft Graph, ensure your application registration is linked to an active Azure subscription. For guidance, refer to [Enable metered APIs and services in Microsoft Graph](#).

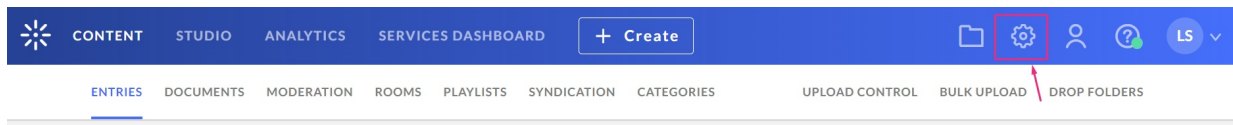
Here are the high-level steps:

1. Create a resource group in the Azure portal under your subscription.
2. Using the Azure CLI, execute the following commands:

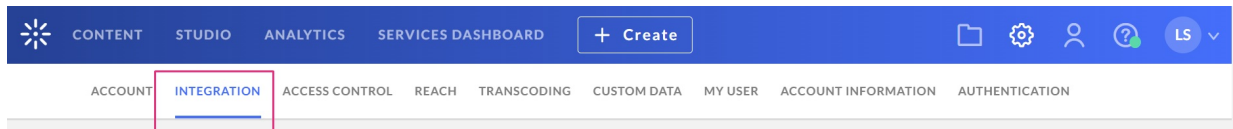
```
az login --scope https://management.core.windows.net//.default
az resource create --resource-group TeamsAPI --name TeamsAPIAppBilling --resource-type Microsoft.GraphServices/accounts --properties '{"appId": "REPLACE_WITH_APP_ID"}' --location Global --subscription REPLACE_WITH_SUBSCRIPTION_ID
```

Configure Teams integration in KMC

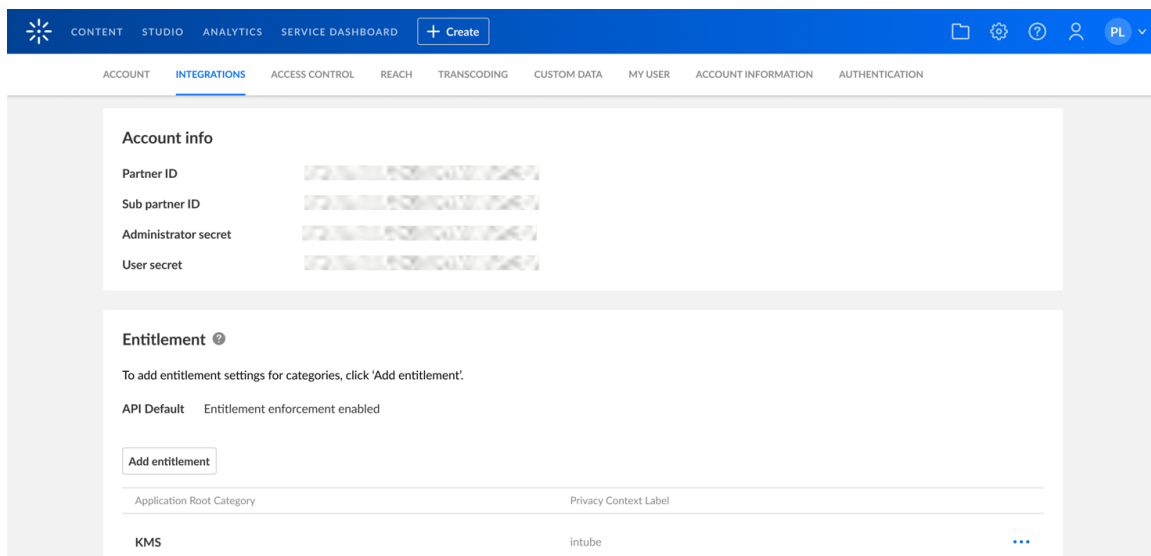
1. Login to the [KMC](#) and click the **settings icon**.



2. Click the **Integration** tab.



3. Scroll down to **Teams integration**.



MediaSpace intube ⋮

Distribution Profiles

YouTube Distribution Profiles

Name	Creation date	Updated At	Youtube Account	
YouTube Distribution Demo	May 3, 2012	Jul 8, 2022	demodistro	⋮

Zoom integration

[Generate integration code](#)

Zoom integrated accounts

Zoom account ID	Account description	Creation date	Updated at	Status	
oqgatWBdQHArVUoamTYNYw	KINO zoom.kaltura.us connector	Nov 21, 2018	Mar 13, 2024	Enabled	⋮

Teams integration

[Add new integration](#)

Teams integrated accounts

Teams account ID	Account description	Creation date	Updated at	Status
There are no active Teams accounts.				

Webex integration

[Generate integration code](#)

Webex integrated accounts

Webex account ID	Account description	Creation date	Updated at	Status
There are no active Webex accounts.				

4. In the Teams integration section, click **Add new integration**.

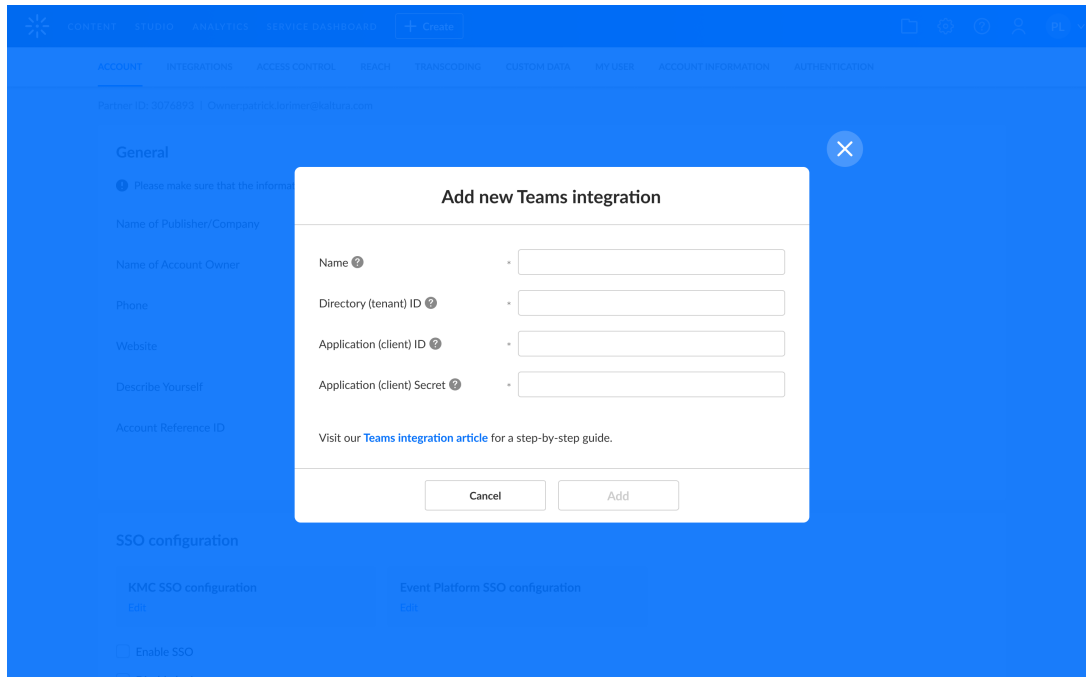
Teams integration

[Add new integration](#)

Teams integrated accounts

Teams account ID	Account description	Creation date	Updated at	Status
There are no active Teams accounts.				

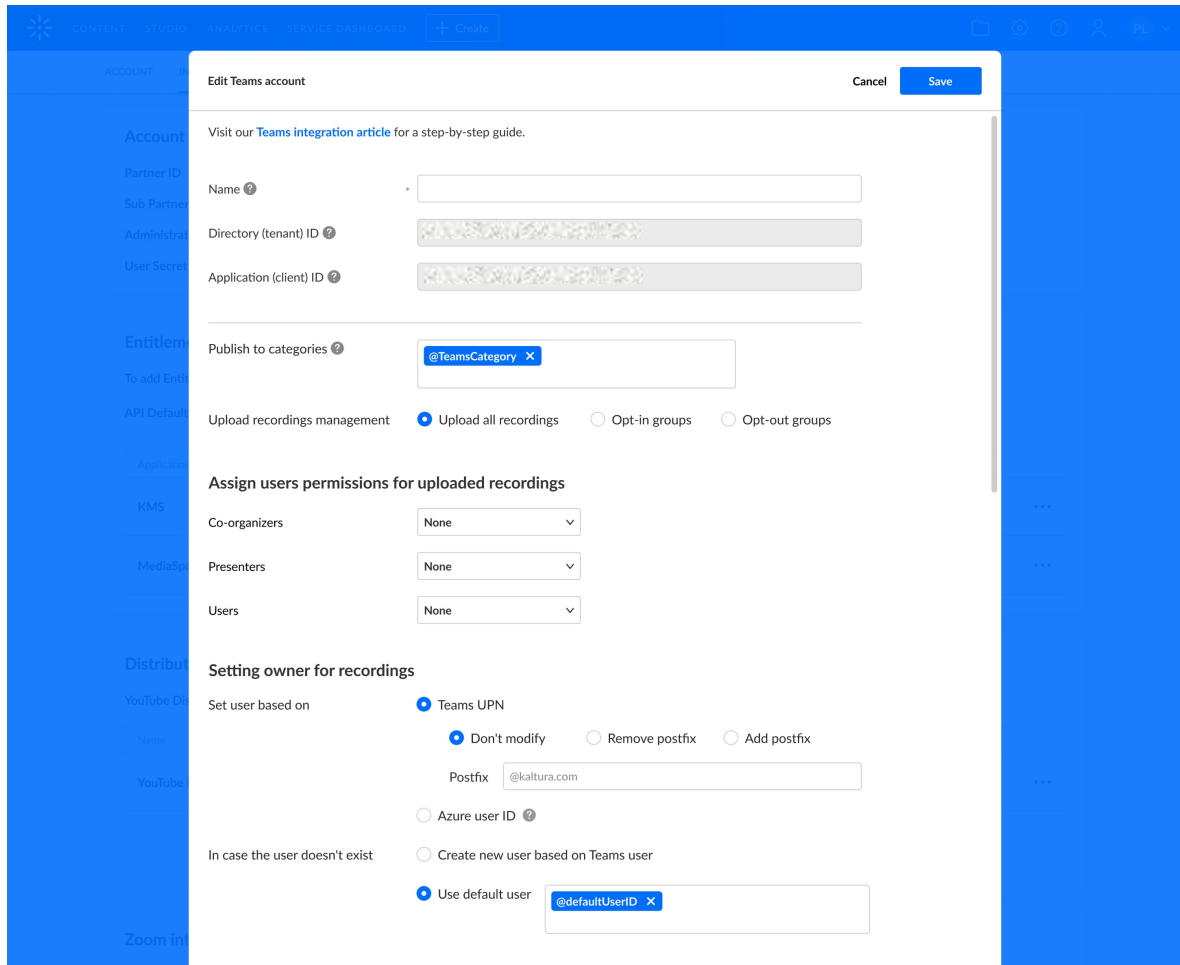
The **Add new Teams integration** window displays.



5. Complete the required fields

- o **Name** - Enter a name for your integration.
- o **Directory (tenant) ID** - Copy your Azure directory ID from the overview tab of the Azure application you just created (see number 6 of step 2).
- o **Application (client) ID** - Copy your Azure Application ID from overview tab of the Azure application you just created (see number 6 of step 2).
- o **Application (client) Secret** - Copy your Azure application of the secret you created previously (see number 6 of step 2).

6. Click **Create**. The edit integration settings window displays.



Edit integration settings


You can edit an existing Teams integration. The settings are as follows:

- **Name**
- **Directory (tenant) ID** (read only)
- **Application (client) ID** (read only)
- **Publish to categories**
- **Upload recordings management:**
 - Upload all recordings - All recordings in the account will be uploaded to Kaltura.
 - Opt-in groups - Recordings will be uploaded to Kaltura if the owner of the recordings is in one of the opt-in groups.
 - Opt-out groups - Recordings will be uploaded to Kaltura if the owner of the recordings is not in one of the opt-out groups.

Assign users permissions for uploaded recordings

Co-organizers - Choose an option from the drop-down menu:

- None
- Co-viewers
- Co-editors
- Co-publishers
- Co-editors & Co-publishers

 Please note that the option Co-organizers is not currently supported by Microsoft.

Presenters - Choose an option from the drop-down menu:

- None
- Co-viewers
- Co-editors
- Co-publishers
- Co-editors & Co-publishers

Users - Choose an option from the drop-down menu:

- None
- Co-viewers
- Co-publishers

Set owner for recordings

In Azure, user identification may differ from Kaltura. For instance, the Microsoft User Principal Name (UPN) may include the entire email address (e.g. [first.last@company.com](#)) or just the user name (e.g. first.last). This setting enables synchronization between Azure and Kaltura users by adding or removing a postfix (e.g. @company.com) or maintaining the same user ID as in Azure.

Set user based on - Choose from the following:

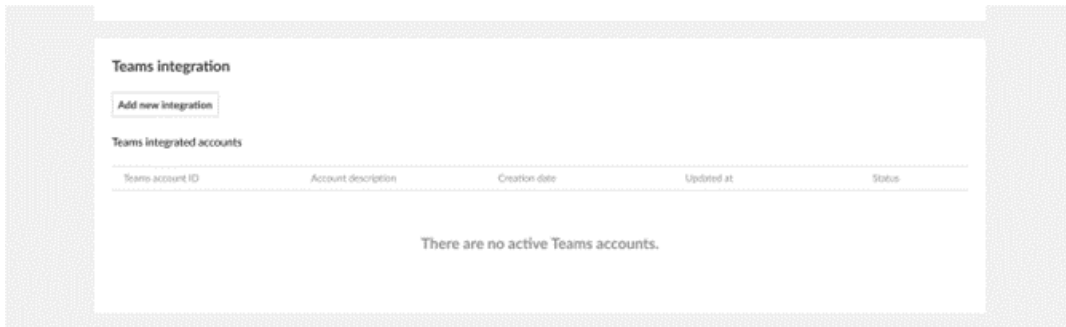
- Microsoft UPN
 - Do not modify (default) - this will be the user ID
 - Remove post-fix. For example, if your UPN is [john.doe@example.com](#) and in Kaltura user ID is john.doe, set postfix to @example.com.
 - Add postfix - add Postfix to field. For example, if your UPN is [john.doe](#) and in Kaltura user ID is [john.doe@example.com](#), set postfix to @example.com.
- Azure user ID
 - Azure user ID is a unique identifier assigned to a user in Azure Active Directory.

In case the user doesn't exist - Choose from the following:

- Create new user based on Teams user (default)
- Use default user - add user from account

Edit Teams account information

In Teams integration, you'll see a list of all active integrations.

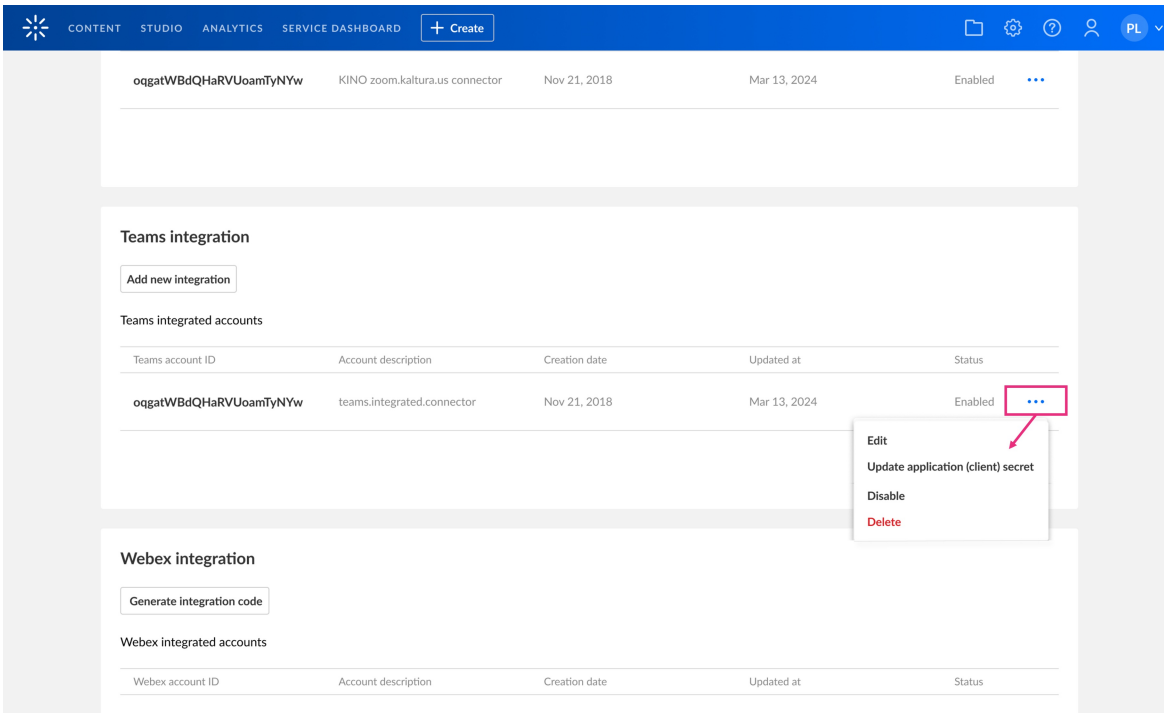


The following information is available:

- **Account name**
- **Creation date**
- **Updated at**
- **Status** - Enabled or Disabled

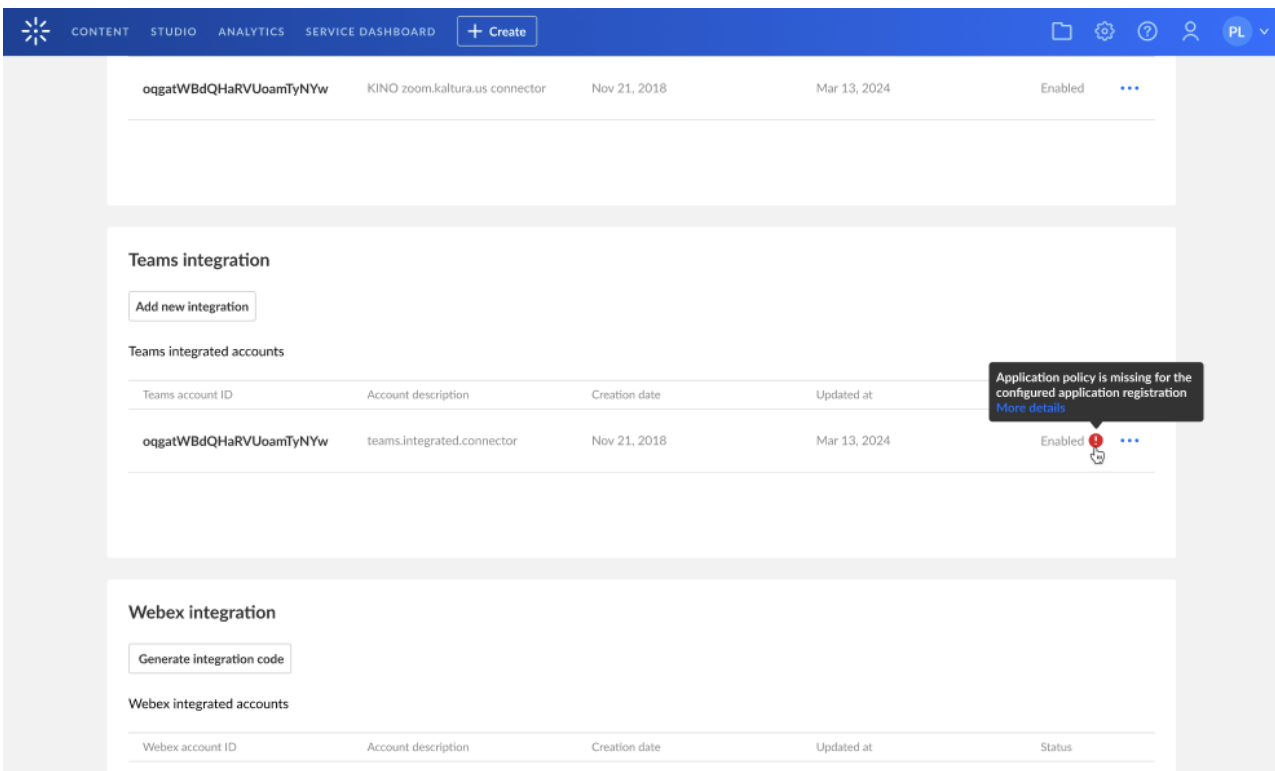
Use the **three dots menu** next to the relevant integration to:

- **Edit** - This opens the integration form.
- **Enable / Disable** - This allows you to enable / disable the integration.
Note: Integration is created in 'disabled' status. To activate it, switch the status to 'enabled' manually.
- **Delete** - This allows you to delete the account.
Note: If the profile status is enabled, a message will display: *Please change integration status to 'Disable' in order to delete it.*



Troubleshooting

If an error occurs, it will be indicated by a red exclamation mark in the status column (as shown in the example below). Hover over it to see a detailed message, such as *Application policy is missing for the configured application registration*.



Here's a list of possible error messages and troubleshooting tips:

Error message	Troubleshooting
<i>The provided application credentials are missing the 'OnlineMeetingRecording.Read.All' permission.</i>	Double-check the permissions created in Step 1 .
<i>The provided application credentials are missing the 'OnlineMeetingTranscript.Read.All' permission.</i>	Double-check the permissions created in Step 1 .
<i>Application policy is missing for the configured application registration.</i>	This likely means the application access policy wasn't created or granted correctly. Check Step 3 .
<i>Access to the Microsoft API was denied.</i>	This means we failed to access the Microsoft API using the configured credentials.
<i>The provided application secret has expired.</i>	To fix this, create a new integration with a new secret. (In the future, it will be possible to update the secret.)
<i>The provided application secret is invalid.</i>	This probably means the application secret was deleted in the Azure console. To fix this, create a new integration with a new secret. (In the future, it will be possible to update the secret.)