

Teams integration setup guide

Last Modified on 05/06/2026 8:41 pm IDT

 This article is designated for administrators.

About

Kaltura's Teams integration enables you to effortlessly upload and archive your Teams recordings, ensuring everything stays neatly organized in one centralized location.

The integration supports both **scheduled Teams meetings** and **ad-hoc session recordings**.

As the owner and host, you'll retain full control and enjoy easy collaboration with co-hosts.

Before you start

- A paid Microsoft Teams account
- A registered Azure app (enabled in your tenant)
- Rich Media CMS account and access
- Teams integration service enabled in Kaltura (paid service)



Each Teams account can be linked to only one Kaltura account.

Step 1 - Set up Azure account

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

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.

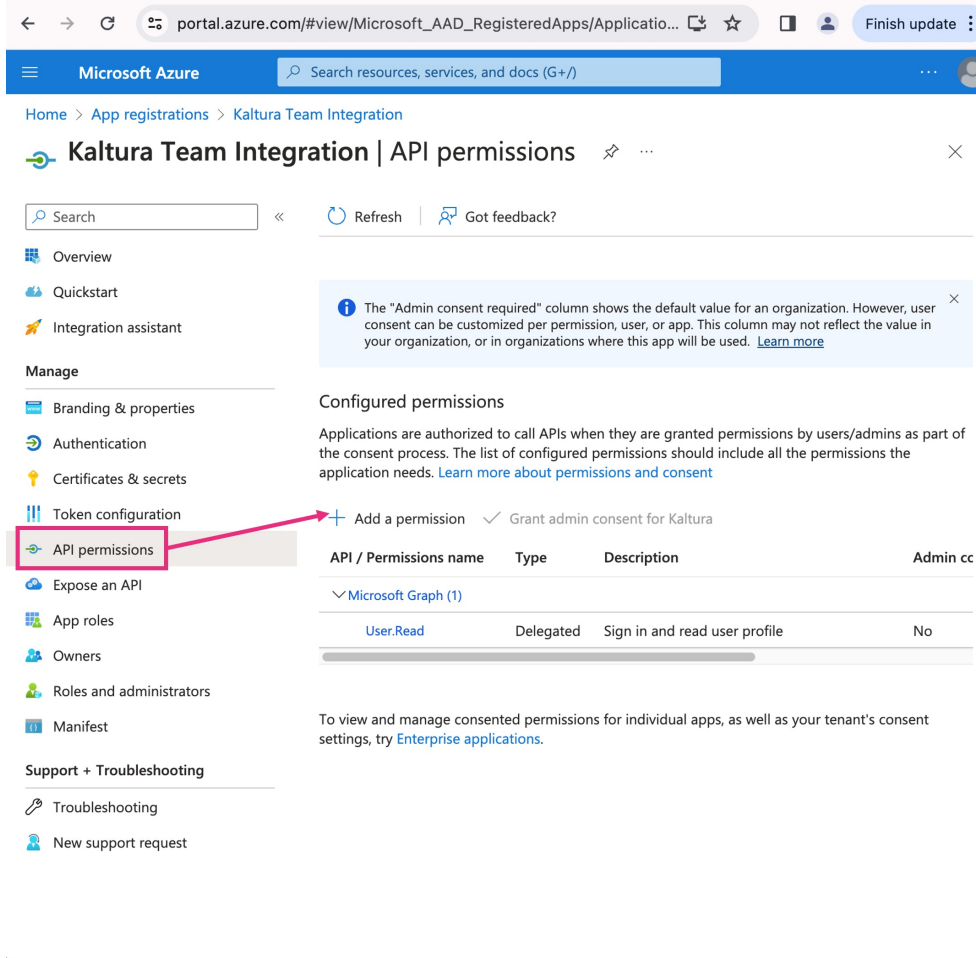
Select a platform

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**.



The screenshot shows the Microsoft Azure portal interface. The browser address bar displays the URL: `portal.azure.com/#view/Microsoft_AAD_RegisteredApps/Applicatio...`. The page title is "Kaltura Team Integration | API permissions".

On the left sidebar, the "API permissions" option is highlighted with a red box and a red arrow pointing to the "Add a permission" button in the main content area.

The main content area shows a notification: "The 'Admin consent required' column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)".

Below the notification, the "Configured permissions" section is visible. It includes a sub-section for "Microsoft Graph (1)" with the following table:

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

At the bottom of the page, there is a note: "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
 - e. CallTranscripts.Read.All
 - f. CallRecordings.Read.All
 - g. CallRecords.Read.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](#)

🔍 Start typing a permission to filter these results

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

Add permissionsDiscard

12. 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]*.

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

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

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](#).

Create a client secret

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

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.

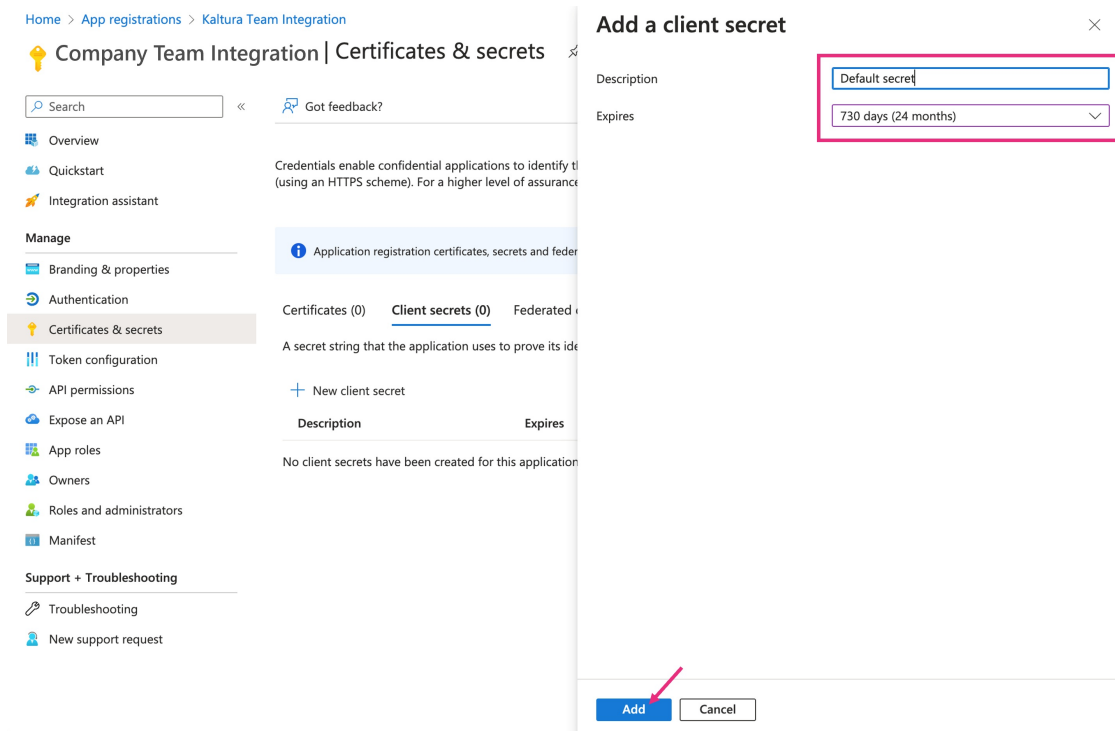
The **Add a client secret** window displays.

- In the **Description** field, type in a description.
- 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.



The screenshot shows the Azure portal interface for managing application registrations. On the left, a navigation pane is visible with 'Certificates & secrets' selected. The main content area shows the 'Add a client secret' dialog box. The dialog has a 'Description' field containing 'Default secret' and an 'Expires' dropdown menu set to '730 days (24 months)'. At the bottom of the dialog, there are 'Add' and 'Cancel' buttons. A red arrow points to the 'Add' button.

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



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

[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? →

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 (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 Rich Media CMS.

[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](#)

Application (client) ID

Object ID

Directory (tenant) ID

Supported account types

[My organization only](#)

Client credentials

[0 certificate, 1 secret](#)

Redirect URIs

[Add a Redirect URI](#)

Application ID URI

[Add an Application ID URI](#)

Managed application in local directory

[Kaltura Teams Integration](#)
[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](#)



Configure an application access policy

To allow your Azure app to access online meetings via Microsoft Graph, follow

Microsoft's instructions in [Configure application access policy](#)*



*In **Microsoft's instructions**, you'll need to follow steps 1-3, then skip step 4 and proceed to step 5. Step 4 is not needed for Kaltura.

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
```

Enable metered API on Microsoft Graph

Once the application access policy is created and assigned, return here to complete this step in Kaltura.

To use Microsoft Graph's metered APIs, your Azure app must be linked to an active subscription. For guidance, refer to [Enable metered APIs and services in Microsoft Graph](#).

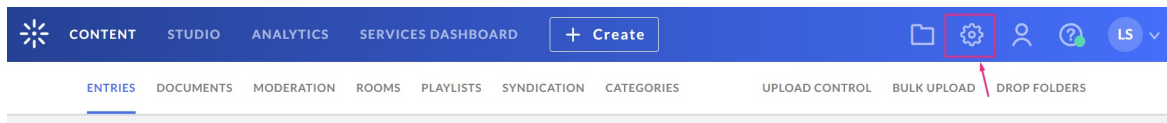
Here are the high-level steps:

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

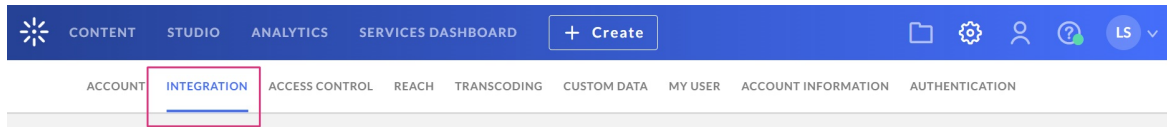
```
az login --scope https://management.core.windows.net//.default  
az resource create --resource-group TeamsAPI --name TeamsAPIAppBilling --resource-  
type Microsoft.GraphServices/accounts --properties '{"appId":  
"REPLACE_WITH_APP_ID"}' --location Global --subscription  
REPLACE_WITH_SUBSCRIPTION_ID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

Step 2 - Configure Teams integration in Kaltura

1. Login to the Rich Media CMS and click the **settings icon**.



2. Click the **Integration** tab.



3. On the Integrations page, scroll down to **Teams integration**.

CONTENT STUDIO ANALYTICS SERVICE DASHBOARD [+ Create](#)

ACCOUNT INTEGRATIONS ACCESS CONTROL REACH TRANSCODING CUSTOM DATA MY USER ACCOUNT INFORMATION AUTHENTICATION

Account info

Partner ID [REDACTED]
 Sub partner ID [REDACTED]
 Administrator secret [REDACTED]
 User secret [REDACTED]

Entitlement

To add entitlement settings for categories, click 'Add entitlement'.

API Default Entitlement enforcement enabled

[Add entitlement](#)

Application Root Category	Privacy Context Label
KMS	intube ...
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
ogatWBdQHrVUJoamTyNYw	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**.

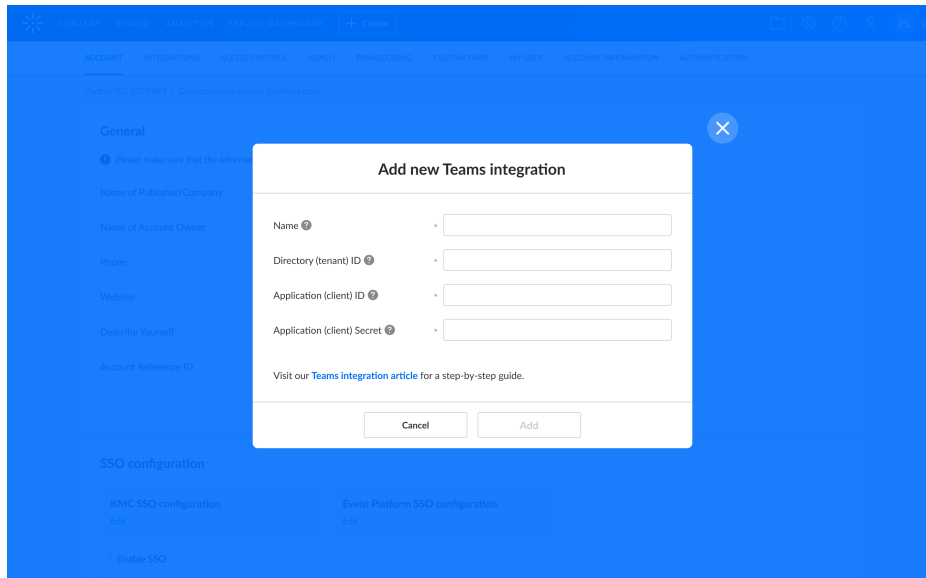
Teams integration

[Add new integration](#)

Teams integrated accounts

Teams account ID	Account description	Creation date	Updated at	Status
------------------	---------------------	---------------	------------	--------

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

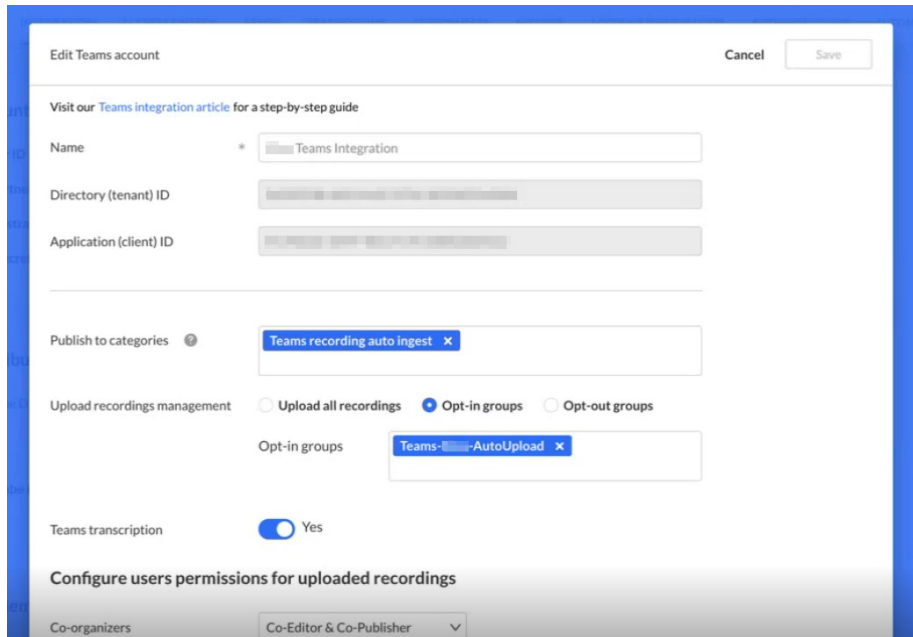


5. Complete the required fields

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

6. Click **Create**.

The edit 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** - Enter one or more categories for Teams recordings.
- **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.
 - Upload ad-hoc sessions recordings - Select whether to upload recordings from ad-hoc Teams sessions in addition to scheduled meeting recordings.
- **Teams transcription** - Set to 'Yes' to include the transcription when uploading the recording.

Assign user 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

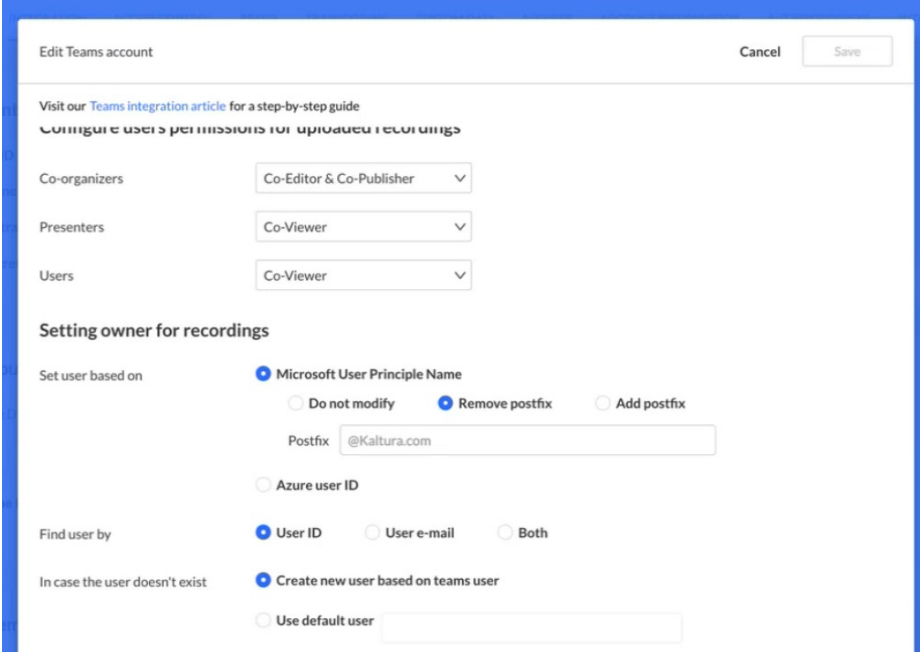
Users - Choose an option from the drop-down menu:

- None
- Co-viewers
- Co-publishers



The Users setting also applies to participants of ad-hoc session recordings.

Set owner for recordings



The screenshot shows the 'Edit Teams account' settings page. At the top, there are 'Cancel' and 'Save' buttons. Below that, a link to a 'Teams integration article' is provided. The main section is titled 'Configure users permissions for uploaded recordings'. It contains three dropdown menus: 'Co-organizers' set to 'Co-Editor & Co-Publisher', 'Presenters' set to 'Co-Viewer', and 'Users' set to 'Co-Viewer'. Below this is the 'Setting owner for recordings' section. It has a 'Set user based on' section with radio buttons for 'Microsoft User Principle Name' (selected), 'Do not modify', 'Remove postfix', and 'Add postfix'. A 'Postfix' text box contains '@Kaltura.com'. There are also radio buttons for 'Azure user ID'. The 'Find user by' section has radio buttons for 'User ID' (selected), 'User e-mail', and 'Both'. The 'In case the user doesn't exist' section has radio buttons for 'Create new user based on teams user' (selected) and 'Use default user' with an empty text box.

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 User Principal Name**

- **Do not modify** (default) - This will be the user ID.
- **Remove postfix** - Select to remove postfix. For example, if your UPN is [john.doe@example.com](#) and the Kaltura user ID is john.doe, the postfix is @example.com.
- **Add postfix** - Select to add a postfix to the field. For example, if your UPN is [john.doe](#) and the Kaltura user ID is [john.doe@example.com](#), the postfix is @example.com.

- **Azure user ID**

- Azure user ID is a unique identifier assigned to a user in Azure Active Directory.



When using this method for ad-hoc session recordings, only the recording owner is identified. Other participants won't automatically receive access permissions to the recording.

Find user by - Set where the system should look for the user. Choose from:

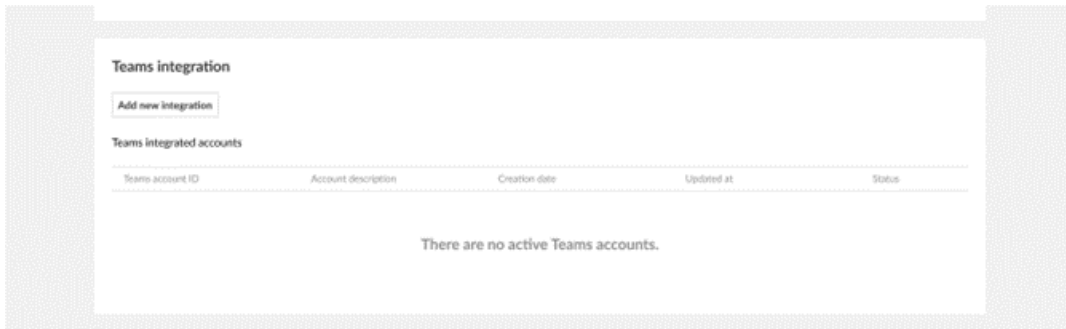
- **User ID**
- **User email**
- **Both**

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

- **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:

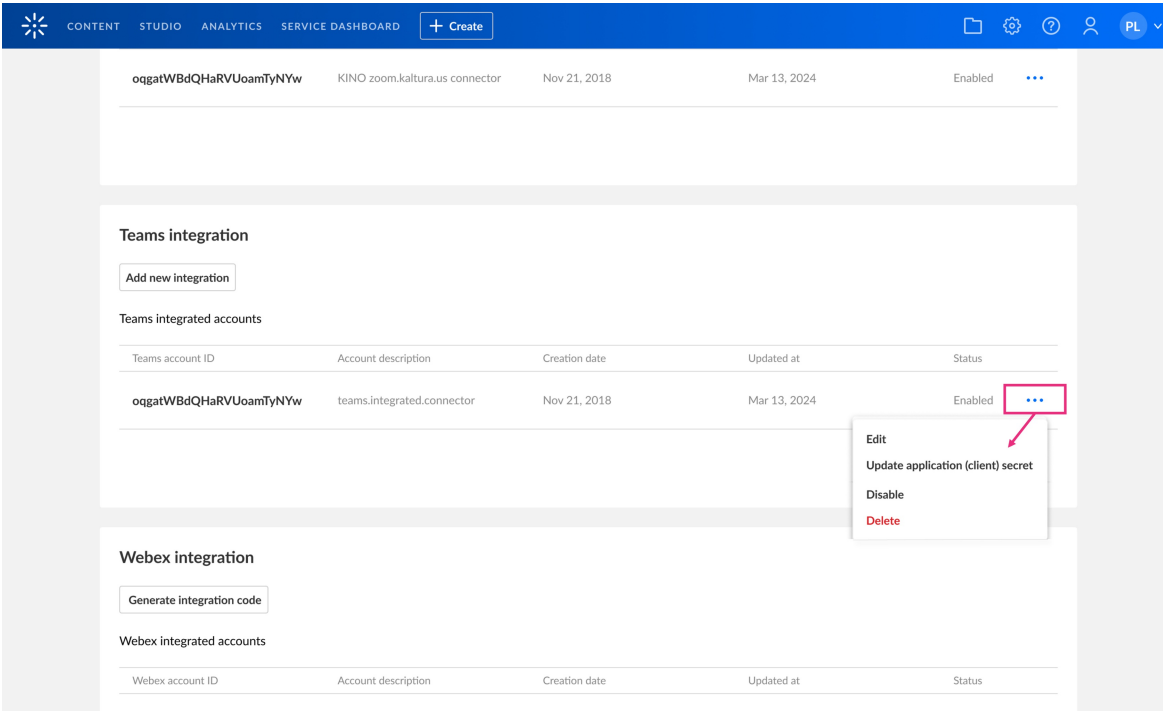
- **Account name**
- **Creation date**
- **Updated at**
- **Status** - Enabled or Disabled

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.



If the profile status is enabled, a message will display: *Please change integration status to 'Disable' in order to delete it.*



oggatWBdQHaRVUoamTyNYw 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
oggatWBdQHaRVUoamTyNYw	teams.integrated.connector	Nov 21, 2018	Mar 13, 2024	Enabled ...

Webex integration

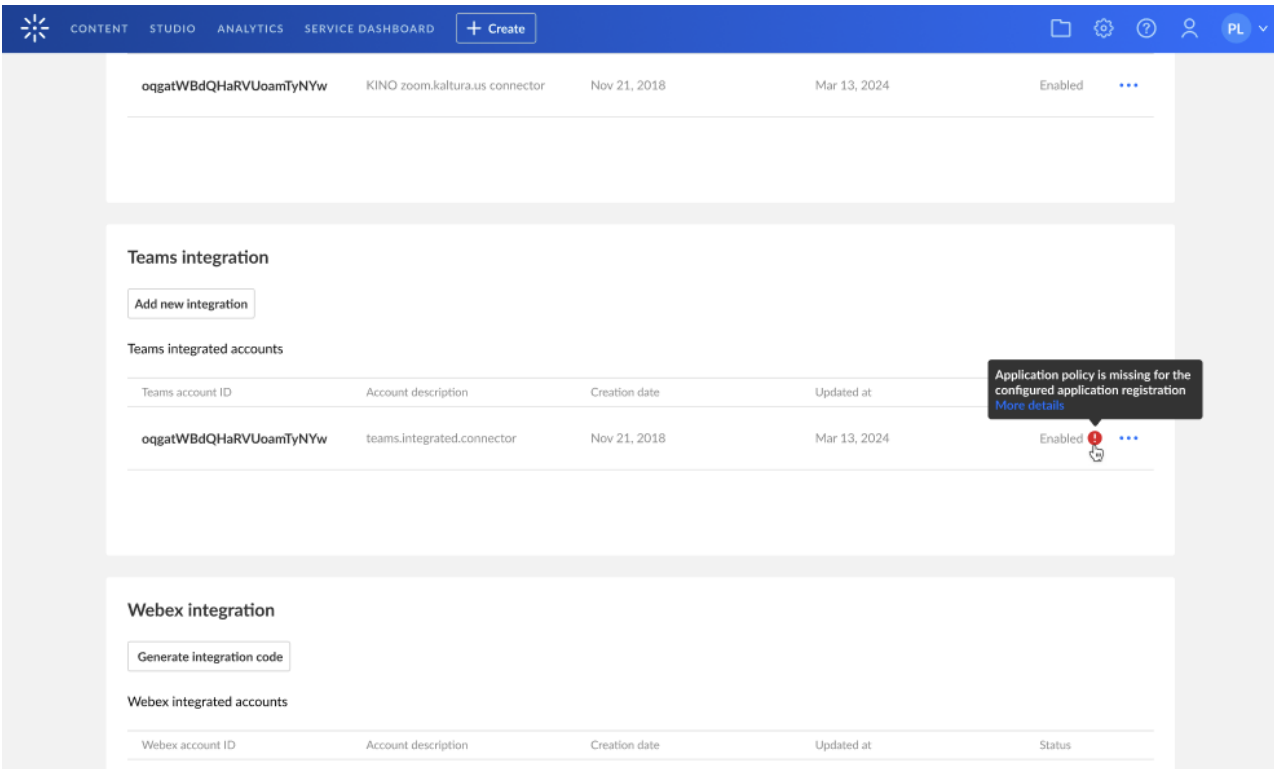
Generate integration code

Webex integrated accounts

Webex account ID	Account description	Creation date	Updated at	Status
------------------	---------------------	---------------	------------	--------

Troubleshooting

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



oggatWBdQHaRVUoamTyNYw 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
oggatWBdQHaRVUoamTyNYw	teams.integrated.connector	Nov 21, 2018	Mar 13, 2024	Enabled ! ...

Webex integration

Generate integration code

Webex integrated accounts

Webex account ID	Account description	Creation date	Updated at	Status
------------------	---------------------	---------------	------------	--------

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 'Request permissions' .
<i>The provided application credentials are missing the 'OnlineMeetingTranscript.Read.All' permission.</i>	Double-check the permissions created in 'Request permissions' .
<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 Configure an application access policy .
<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.)
<i>Application is disabled</i>	The Azure app you registered for the Teams integration (e.g., “Kaltura Teams Integration”) is currently disabled. Ask your Azure administrator to enable the app in your organization's Azure environment (Azure tenant), then try setting up the integration again.