

Teams Integration

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.

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.
- The KMC user specified in the Teams configuration screen is designated as the owner of all recordings transferred to Kaltura, **unless** individual Teams users have input their Kaltura User ID in their Teams profile.
- Consider creating a dedicated KMC user specifically for Teams configuration settings. It's recommended to set this up before proceeding with the administrator setup process.

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

The **Request API permissions** page displays.


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

Step 2 - Create a client secret

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

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.

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.

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

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

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 step 2](#)).
 - **Application (client) ID** - Copy your Azure Application ID from overview tab of the Azure application you just created (see [number 6 of step 2](#)).
 - **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.*

[template("cat-subscribe")]
