Managing Content Entitlement

> This article is designated for administrators.

About

Kaltura's Categories come with entitlement settings and end-user permissions for associated media entries. This allows efficient control over who can access what content, enhancing application navigation. Kaltura provides infrastructure for managing these entitlements, including attributes, permission controls, and server utilities for enforcement.

With Kaltura's entitlement services, applications like Kaltura Video Portal (MediaSpace) can be expanded to include the following features:

- **Group Channels**: You can set specific channels that restrict access and content contribution to members of particular user groups.
- **Granular User Permission Control**: You can define various privacy and permission levels for accessing and managing content within channels.
- **Personalized Global Search**: Users can effortlessly search and discover relevant content from their entitled media collection.

End-user permissions

When any Entitlement option is set to Private, the access level is based on specific end-user permissions. The Kaltura server enforces basic access permissions which control UI settings and user flows in the video portal, such as Channel settings, moderation panel, Publish Module, etc.

Permission levels	View content and category	Add / remove content to category	Approve content added to category	Edit category's settings, privacy, and user permissions	Remove category
Member	x				
Contributor	x	x			
Moderator	x	x	x		
Manager	x	x	x	x	x

End-user permissions can be configured in the KMC in Bulk Process through CSV

formatting or via Kaltura APIs. They can be changed by selecting the "Manage Users" field.

In the video portal, Channel Managers have the authority to set their channel's group members and assign varying permission levels to them.

The content owner always has full access and editing permissions to their own content. They're also able to remove their content from any category, regardless of the category's settings.

Even if a category isn't private, applications can use end-user permissions. For example, in the video portal, users without admin roles can still publish content in specific galleries. The category's contribution policy is set to 'No Restriction,' and permissions allow publishing for video portal admins and designated contributors.

Entitlement settings

Entitlement settings can be managed in various ways: through the application, via CSV, or using the Kaltura API. Account administrators handle content entitlement settings in the category's Entitlements tab in the KMC. This tab is visible only in KMC accounts with entitlement enabled and for categories configured with entitlement settings for an application.

The Entitlement Settings are added to categories as part of the video portal installation. For other purposes, entitlement settings can be added to categories from the Integration Settings page under the settings tab in the navigation bar.

1. Log into your KMC.
   The Content menu displays by default.
2. Click the **Categories** tab.
3. Click on the desired category.
   The edit details page displays.
4. Click the **Entitlements** tab. If you don't have this option, see How to Add Entitlement to Categories.
   The Entitlements page displays.

Set the entitlement settings as follows. Informative tooltips are available for each one of the options:

Privacy Context Label

The Privacy Context is a free text label that indicates to which application the entitlement settings apply, for example, “MediaSpace”. For more information see Adding Entitlement to Categories.

Content Privacy

The Content Privacy defines the visibility of content associated with a category, including its related metadata. The Content Privacy setting is applied to:

- Who has access to content published in channel pages
- Which content will be available to the user in the application global search results
- Who can access to a single media item in the application.

The content privacy options are:

- **No Restriction** – The content is visible to all users who have access to the application page where it's published. In the video portal, this option is mainly used for creating open and publicly accessible galleries on the web, including anonymous viewers.
- **Requires Authentication** – This content is visible exclusively to authenticated end-users. In the video portal, this option is mainly used for setting galleries or open / restricted channels accessible to all authenticated users such as company users or customers with login. Authentication in video portal is done through the customer's Identity Management system or using Kaltura's authentication services. The authenticated user ID is then passed to the Kaltura server through the application session in either scenario.
- **Private** – This content is visible only to users with specific permission to access this category's content and to the owner of the content. In the video portal, this option is mostly relevant for setting private channels - accessible only to a group of users.

Category Listing

This option defines who can see the category's name and metadata in the video portal.

The Category Listing options are:

- **No Restrictions** - With this option, the category name and metadata is visible to everyone with access to the application page it is listed in. In MediaSpace - this option is used for having MediaSpace Galleries always listed in the top menus and side navigation layout and for having MediaSpace open or restricted channels

included in the Channels listing page.

- **Private** – With this option, the category name and metadata are visible only to users with permission to access the category and its content. In MediaSpace this option is used for having private channels visible only to group members.

Content Publish Permissions

This option defines which end-users can add content to this category through applications. The applicative permission to publish in MediaSpace's shared Galleries is set from the MediaSpace Application Role of the user. See the Kaltura MediaSpace Setup Guide for more information. This policy adds the ability to have this type of authorization for publishing content in specific galleries/channels.

The Content Publish Permissions options are:

- **No Restrictions** – With this option, any end-user authorized to publish content in MediaSpace can publish content in the gallery/channel associated with this category. In MediaSpace this option is used in shared galleries to which every user with a MediaSpace Admin Application Role can add content to, and in Open Channels to which all MediaSpace users with content can add their content to.
- **Private** - With this option, only end-users with specific permission to add content to this category can add content to it. In MediaSpace this option is used in Restricted/Private Channels.

Moderate Content

Enable this field to support the moderation of content prior to publishing in the channel. (Moderation is configured through Kaltura MediaSpace.) Media will not appear in the page until approved by the category manager/moderator.

Inherit Users Permissions

This option defines whether end-users can inherit specific permissions from the parent category.

⚠ Caution: Enabling the **Inherit Users Permissions** option may delete users that have already been assigned to the channel/category, unless they've been assigned to the Parent category.

Default Permission Level

Use this field to set the default permission level: Member, Contributor, Moderator or

Manager.

Owner

Use this option to change the category owner as follows:

1. Click **Change Owner**.

   The Change Owner window displays.

2. Enter the new category owner's name.
3. Click **Apply**.

Permitted Users

Use this option to manage users as follows:

1. Click **Manage Users**.

   The **Manage End-user Permissions** page displays.

2. Click the box next to the desired user or multiple users to activate the **More Actions** menu.

   You can use the search bar to find specific users as well as refine your search by using additional filters in the Refine drop-down menu.

   More Actions menu

   Active - activates the specific end user permissions for the category. Select **Yes** or **No**.

   - Yes – Access permission is active and enforced
   - No – Access permission is not active anymore (but can be activated again).

   Set Permission Level - Overrides the permission level of all selected end-users. See Specific End-Users Permissions.

   Update - Set to manual or automatic update. See End-User Permission

Attributes.

- **Automatic** - User permission is updated via an automatic process (either via a CSV formatted schema or an API based integration).
- **Manual** – User permission is updated manually only and will not be updated by an automatic process.

Delete Users- Deletes the selected end-user(s) from the category.

3. Click **Close** to save changes and exit.

Note: Hovering in the space at the end of the row will display a remove icon . Click on the icon to remove the user.

Add Users

To add additional users:

1. Click the **Add Users** button.

   The **Add Users** window displays.

2. Configure the following:
   - If you want to add users to a category that has users associated to its parent category, the click one of the buttons:
     - **Set End-user permissions for this category**
     - **Inherit users from parent category**
   - **Select End-Users -** Enter the name/s in the field.
   - **Permission Level** - Select the permission level (Member, Contributor, Moderator or Manager) from the drop-down menu.
   - **Update Method** - Select Automatic or Manual from the drop-down menu.
3. When you have finished, click the **Add (x) Users** button.

Content associated with multiple categories

If content belongs to multiple categories, its privacy and visibility are determined by the category with the lowest restriction level within the application's category tree. This ensures consistent access whether found via global search or a direct link.

Examples

- A video published in private channels and a public gallery (Content Privacy = No

Restriction) will be visible to everyone with site access. Users can find it on the public gallery page, via global search, or with a direct link.

- A video published in private channels and an organizational shared gallery (Content Privacy = Requires Authentication) will be visible to all organization members upon login. It's accessible from the shared gallery, global search, or via a direct link (anonymous viewers will be prompted to log in).
- A video published in private channels and placed in Kaltura categories managed outside the portal will have access controlled by integrated category entitlements governed by the "privacy content" label set to those specific categories.
- A video uploaded by an end-user but not published in any gallery or channel (private), is only accessible to the content owner

Visibility of content outside of the application

When entitlement is enabled, Kaltura manages internal enforcement, usually turned on by default for video portal accounts. This setting provides the highest level of content security, and is especially recommended for video portal accounts.

⚠ In the video portal, users can bypass this enforcement by grabbing embed codes, making the entry publicly accessible outside of the portal.

Entitlement enforcement is disabled by default and must be enabled by the application. When disabled, content in entitled categories can be accessed through any application, In this mode, the application itself activates entitlement enforcement, keeping entitlement rules within the application. However, all content in integrated categories can be accessed through other applications too. This is the default setting for Kaltura trial accounts.

To change the entitlement enforcement level for your account, please contact your Kaltura representative.

[template("cat-subscribe")]