Access Control

This article is designated for administrators.

Overview

Kaltura supports several publication restrictions allowing limited access to content when business requirements dictate it. These restrictions can be placed on the entry-level but can also be streamlined to be set automatically or on demand, on a group of items based on a set of criteria, during upload via a bulk upload CSV file, or during an update transaction using Kaltura's APIs. See Kaltura API documentation.

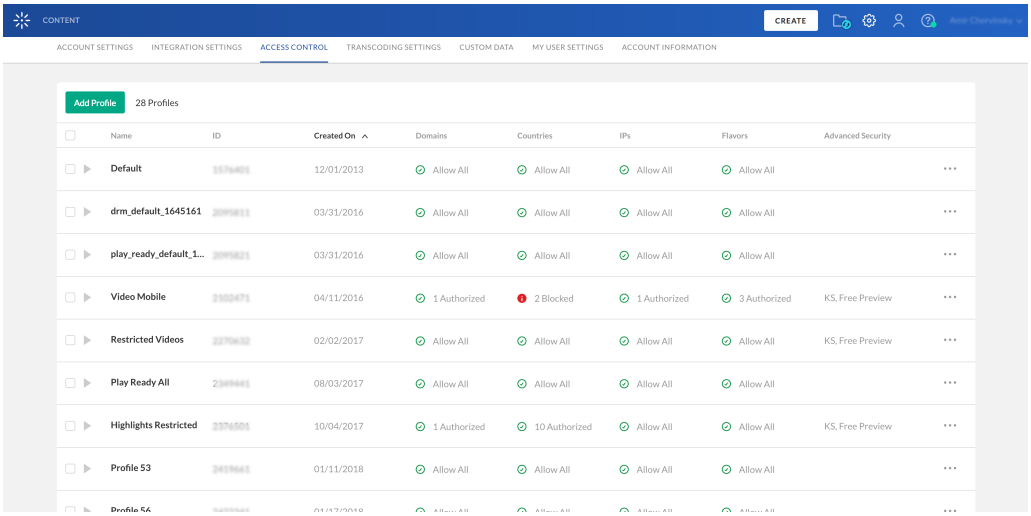
An Access Control Profile defines authorized and restricted domains where your content can or cannot be displayed, countries from which it can or cannot be viewed, white and black lists of IP addresses and authorized and unauthorized domains in which your media can be embedded. Use the Access Control tab to view existing profiles and create new ones.

Controlled access provides authentication and authorization capabilities. Developer authentication is done using a combination of the Partner ID and one of two "secrets", each providing a different set of authorization capabilities. In return, a Kaltura Session token ("KS") is generated, through which API calls can be made.

You can segregate your content based on your various user groups and audiences. You can create content channels to be accessed only by certain users and allow other content items to be available to all. Access profiles also allow you to manage groups and users on your own identity.

View Access Control settings

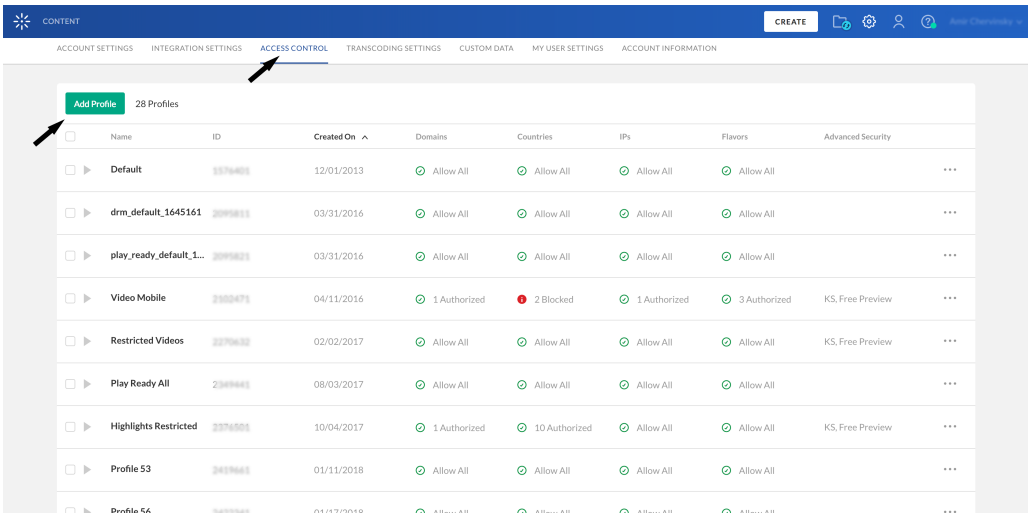
- Select the **Settings** icon and then select the **Access Control** tab.
  The Access Control Profiles window is displayed. A default access control profile that permits access to all is configured automatically.



Creating an Access Profile

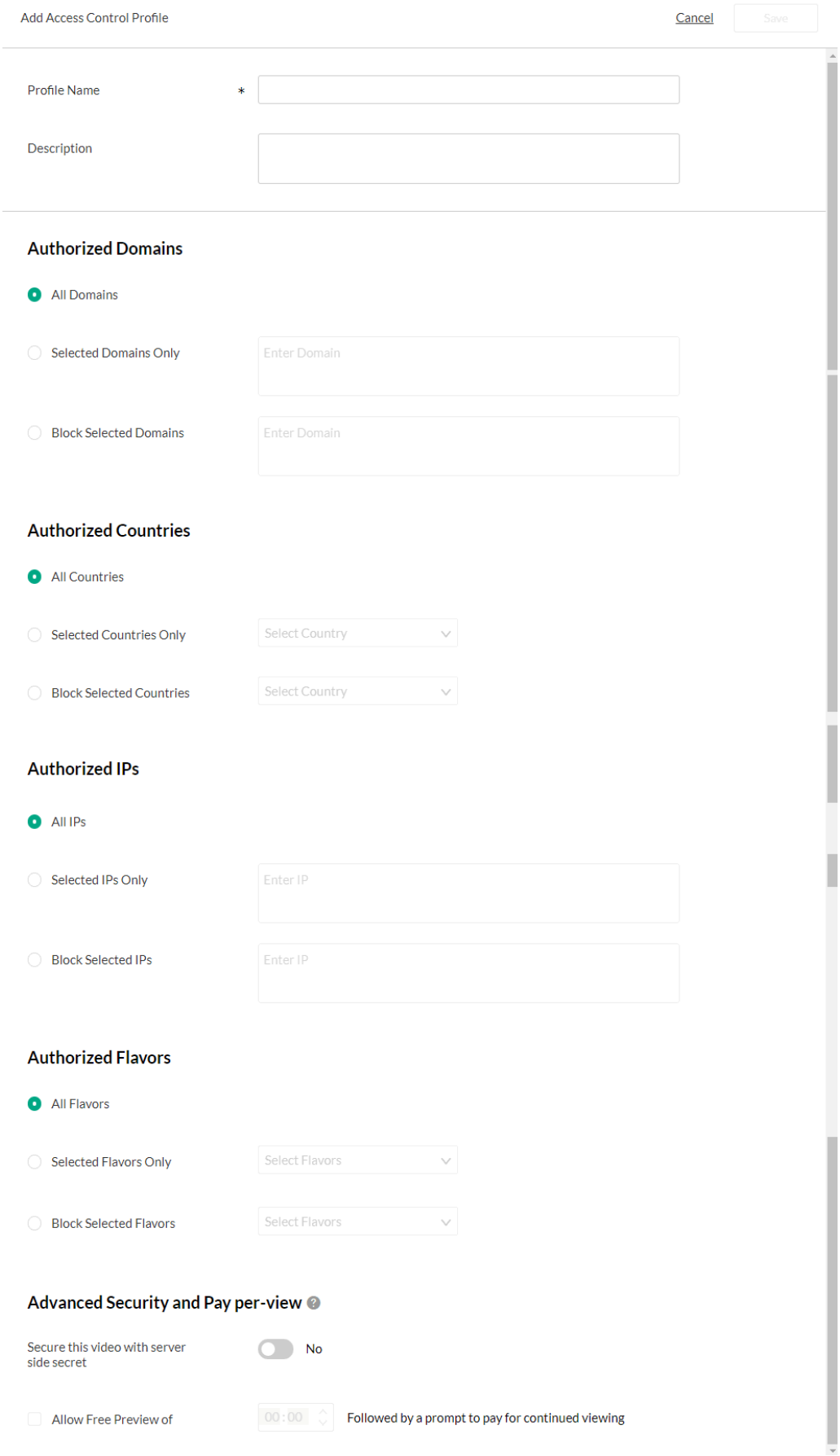
1. Select the Settings icon and select the Access Control tab.

   The Access Control Profiles window is displayed.



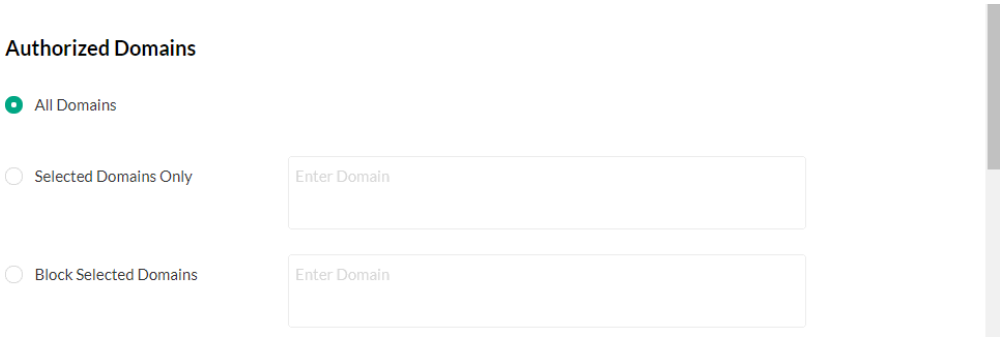
2. Click Add Profile.

   The Add Access Control Profile window is displayed.

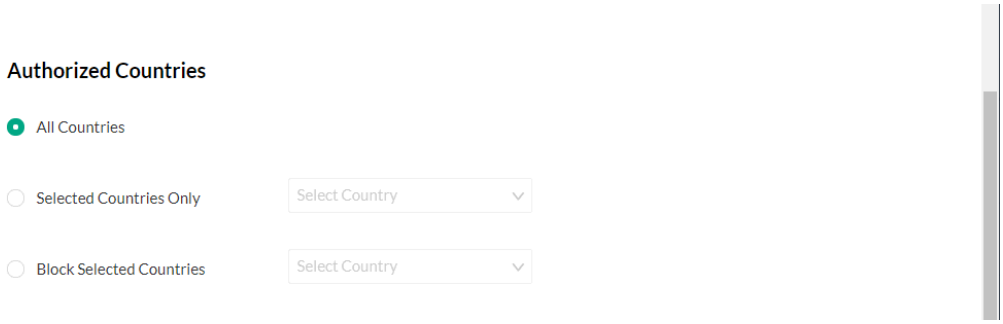


3. Enter an informative Profile Name and Description for the profile.

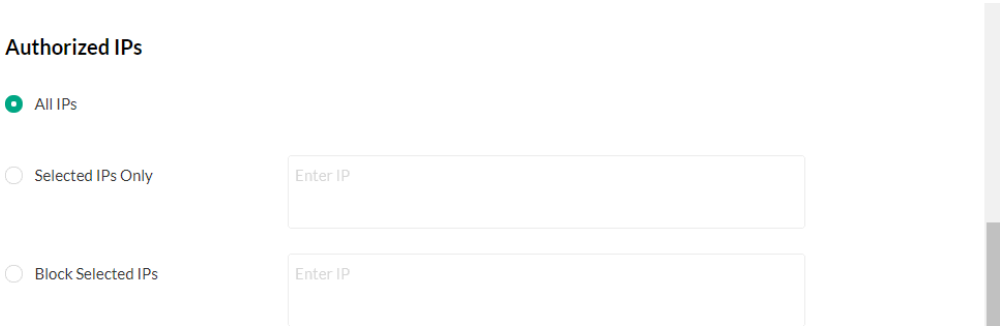
4. Configure the Authorized Domains. See Restricting Domains.



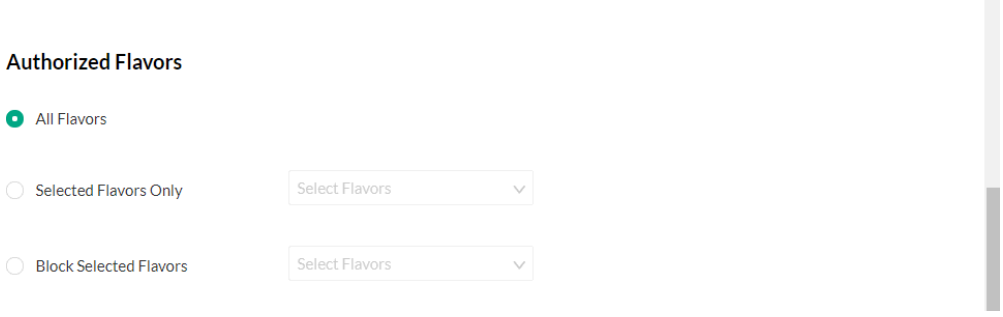
5. Configure the Authorized Countries. See Restricting Countries for Viewing.



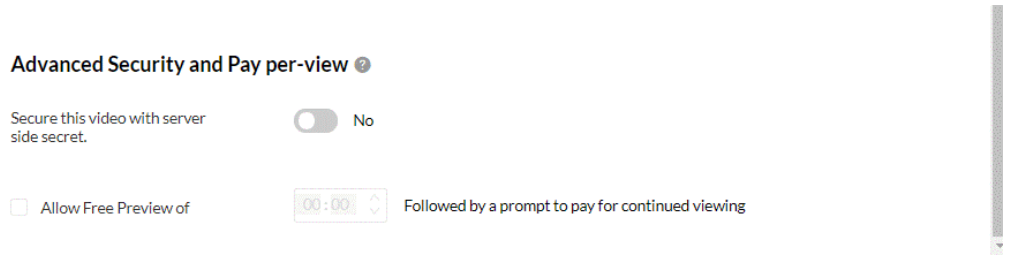
6. Configure the Authorized IP Addresses. See Restricting Views by IP Address.



7. Configure the Authorized Flavors. See Restricting Access for Specific Flavors.



8. Configure the Advanced Security and Pay per-view options. See Restricting Views with a Kaltura Session.



9. Click Save.

Editing an Access Profile

To edit an access control profile

1. Select the Settings icon and then select the Access Control tab.
   The Access Control Profiles window is displayed.
2. Click on the 3 dots on the right and select Edit to edit.
   The Edit Access Control Profile window is displayed.
3. Modify the profile according to the sections described in Creating an Access Profile.

Restricting IPs

You can restrict content view by IP addresses or ranges and determine which IP ranges will be allowed to view the content.

To Restrict Views by an IP Address

1. Create and Access Profile.
2. In the Authorized IPs section, select one of the following options:

Toggle All IPs – content will be displayed for all IP addresses.
Toggle Only from the following IPs- select a range of approved IPs that will display content. See Add or Remove IP Addresses.
Toggle Block from the following IPs- enter a range of approved IPs that should be excluded from content viewing. See Add or Remove IP Addresses.

Restricting Domains

Kaltura's Access Control mechanism provides the means to restrict content playback from specific domains. This is useful to prevent scraping of content from your website

or re-sharing of content on other sites that are not yours.

Domain restrictions allow you to define a “white list” of domains that allow only playback attempts of content placed on these domains to be granted. In the same manner a “black list” can be defined performing the opposite constraint. Any playback attempt from these domains will be denied. You can create a combination of both “white listed” and “black listed” domains.

> If you are using Access Control Profiles and are embedding a V7 player, please note that Domain Restriction is not supported with Iframe embed. This is due to the referrer which is always taken from the parent domain, and there is no access to parent domains in the Iframe element.

To restrict content to specific domains

In the Authorized Domains section, select one of the following options:

- Toggle All Domains – content will display in all domains.
- Toggle Selected Domains Only - enter a site or list of approved sites that can display Kaltura content. See Add or Remove a Domain.
- Toggle Block Selected Domains - enter a domain or list of approved of domains that are not allowed to display Kaltura content. See Add or Remove a Domain.

Adding or Removing a Domain

To add a domain

- In the Selected Domains Only section, enter the domain(s) you want to authorize. Click Enter after each domain you add.

To remove a domain

- Select a domain from the listed domains and press Enter.

Restricting Countries

Geographic restrictions, like domain restrictions, allow you to define a “white list” or a “black list” of specific geographical locations, limiting or enabling playback attempts of content for users located in these locations. For example, a Kaltura Player entry assigned with geo-restrictions where the white list contains only Spain can be placed on any domain but will only be playable by viewers located in Spain.

To restrict content to specific countries

In the New/Edit Access Control Profile window, scroll down to the Authorized Countries section. Select one of the following options:

- Toggle All Countries– content will be displayed in all countries.
- Toggle Selected Countries Only - select a country or list of approved countries that will display content. See Add or Remove Geographic Regions (Countries)
- Toggle Block Selected Countries - enter a country or list of approved of countries to exclude. See Add or Remove Geographic Regions (Countries).

Adding or Removing Geographic Regions (Countries)

To add a geographic region

1. In the New/Edit Access Control Profile window, scroll down to the Authorized Countries section.
2. Toggle Selected Countries Only and use the drop-down menu to select the countries from the Countries List.
3. Click Save.

To remove a geographic region

1. In the New/Edit Access Control Profile window, scroll down to the Authorized Countries section.
2. Toggle Selected Countries and use the drop-down menu to select and remove the countries from the Countries List.
3. Use the arrow buttons to transfer the selected countries to the Allowed Countries.
4. Click Save.

To block selected countries

1. In the New/Edit Access Control Profile window, scroll down to the Authorized Countries section.
2. Toggle Block Selected Countries and use the drop-down menu to select and remove the countries from the Countries List.
3. Click Save.

Restricting Views by IP Address

You can restrict content view by IP addresses or ranges and determine which IP ranges will be allowed to view the content.

To restrict Views by IP Address

In the New/Edit Access Control Profile window, scroll down to the Authorized IPs section. Select one of the following options:

- Toggle All IPs – content will be displayed for all IP addresses.
- Toggle Selected IPs Only - select a range of approved IPs that will display content. See Add or Remove IP Addresses.
- Toggle Block Selected IPs - enter a range of approved IPs that should be excluded from content viewing. See Add or Remove IP Addresse

Adding or Removing IP Addresses

To add IP addresses

1. In the New/Edit Access Control Profile window, scroll down to the Authorized IPs section. Toggle Selected IPs and enter the IPs.
2. Click Save.

To remove IP addresses

1. In the New/Edit Access Control Profile window, scroll down to the Authorized IPs section. Toggle Block Selected IPs.
2. Click on the x of the IP address to remove.
   A warning message is displayed.
3. Click Yes.

Restricting Specific Flavors

You can restrict content view by flavors and determine which flavors will be allowed for playback and download authorization and for DRM licensing authorization when applicable. The access control flavor authorization enables you to define restriction rules that are enforced by the Kaltura server, adding a stronger level of security to player tag-based flavor controls.

To restrict access for specific flavors

In the New/Edit Access Control Profile window, scroll down to the Authorized Flavors section. Select one of the following options:

- All Flavors – content will not be restricted by access control for any flavors
- Toggle Only flavors defined in the following list - select the approved flavors that will display content. See Adding or Blocking Flavors.
- Toggle Block flavors defined in the following list - select the approved flavors that should be excluded from content viewing. See Adding or Blocking Flavors..

Adding or Blocking Flavors

To add or block flavors

1. In the New/Edit Access Control Profile window, scroll down to the Authorized Flavors section.
2. Toggle All Flavors– content will be displayed for all flavors.
3. Toggle Selected Flavors Only - select the flavors from the drop-down list that will display content.
4. Toggle Block Selected Flavors - select the flavors from the drop-down menu that will be blocked from displaying.
5. Click Save.

Removing Flavors

To remove flavors

1. In the New/Edit Access Control Profile window, scroll down to the Authorized Flavors section.
2. Click on the X for the flavor you want to remove from the restricted list.
3. Click Save.

Restricting a Kaltura Session

Often, the user authentication/entitlement mechanism that decides whether a user is entitled to access a specific media entry or not, will reside outside of Kaltura. When the authentication mechanism resides outside Kaltura, we recommend that you use an Advanced Kaltura Session (KS) based Access Control mechanism, that permits access to the media only when a valid Kaltura Session is provided. . The external entitlement mechanism will then generate the valid Kaltura Session when users should be permitted to view the content.

The session is created using a secret. The external entitlement mechanism will then generate the valid KS when users should be permitted to view the content. Common examples include -

When implementing paid content where the payment gateway is not Kaltura, the server processing the payment will be the mechanism deciding on entitlement. After the payment is processed, the payment server creates a valid Kaltura Session by calling the Kaltura API and passes that KS to the Kaltura player.

When implementing a single-sign-on and permissions mechanism using LDAP or other authentication mechanism outside of Kaltura, the server responsible for user authentication contains the entitlement logic. The authentication server will call the Kaltura API and generate a valid KS when appropriate.

A Kaltura Player marked with tokenized access requires a “session token” to be created and provided during every playback. A session token can only be created by a developer possessing valid credentials and expires after a limited amount of time. Thus, even if an attempt to grab the item’s direct URL is successful, the playback session will soon expire and without possession of the valid credentials, regeneration of a new token will not be possible.

This option is useful to prevent scraping of content from your website or re-sharing of content on other sites that are not yours and provides an additional amount of security to content display.

Pay-Per-View

You can enable paid programming with a video preview, and easy, on-the-fly payment options for full video access.

To create a Kaltura Session restriction to view content

- Check Secure viewing of this video with Kaltura Session (KS).

To enable a free preview

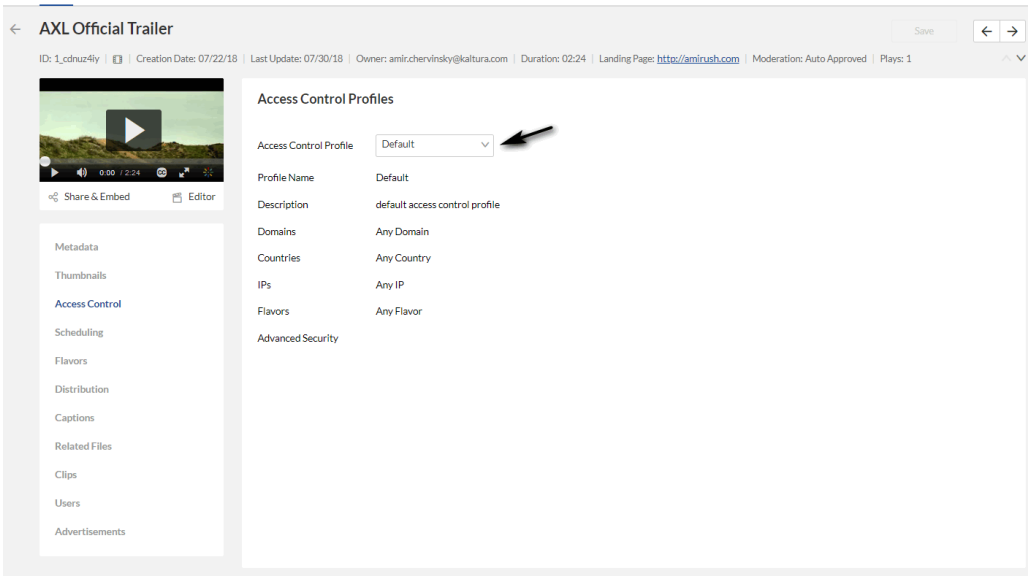
1. Check Free Preview.
2. Enter the amount of time in seconds for the free preview display.

Assigning an Access Profile to an Entry

You can assign an Access Control Profile to an single entry or to multiple entries via bulk upload.

To assign an access control profile to an entry

1. Go to Content tab and select the Entries tab.
2. Click on the entry to which you want to assign an Access Control Profile.
3. Go to the Access Control tab and select an existing profile from the drop-down menu.



4. Click Save.

Assigning an Access Profile to a Bulk Upload

A default access profile is included with the KMC. After you create an Access Profile, an ID is created and listed in the Access Control page.

To assign an access profile to a bulk upload

- Set the ID from the Access Control List to the accessControlProfileId in your CSV
- Set the profile ID from the Access Control List to the accessControlId in your XML file.

For more information see The Kaltura Media Access Control Model.

[template("cat-subscribe")]