Kaltura Access Control

Last Modified on 03/09/2024 6:08 pm IST

In many cases, organizations are interested in restricting access to content. You may want or need to employ broad controls such as allowing access only from a specific geographic location, domains, or you may want to restrict access to specific assets to certain authorized individuals only.

Kaltura offers several features that are designed to help you achieve the right level of access control to your media.

The options are summarized in the following table:

Feature	Description	When to use it?	How to apply it?
Authentication on entry to the web page	Restricts access to the web page in which the media is hosted. Only authorized users will be able to access the web page using a password or any other secret.	In case access needs to be granted to specific people.	For Kaltura's Video Portal, MediaSpace, Kaltura offers multiple authorization options – manage users through our system or integrate with external authorization systems (LDAP, Shibboleth, CAS) as well as custom databases for single sign-on (SSO), or use a hybrid approach where authentication is done by your organization and authorization is handled by Kaltura. For more information about the MediaSpace permissions, refer to the article Kaltura Entitlement Infrastructure. For integrations with LMSs (Learning Management Systems)

			Management Systems) and CMSs (Content Management Systems), Kaltura operates within the context of the LMS or CMS. The authentication method used in the organization for access to the LMS or CMS is in effect and the media file can only be viewed by those with access permissions to the page that hosts it per the LMS/CMS configuration. If the video is embedded in the customer's website, password protection needs to be set up by the customer. on their web page.
Geo Restriction	Restricts access to media based on the viewer's IP address geo location. This is set using the browser IP address received within the HTTP requests and the use of IP to location lookup services. For example, a Spanish client can deny access to their media to all users outside of Spain, allowing users with Spanish IPs only to access the site's media.	Geo restriction is a good way to help enforce licensing agreements, which often limit viewership to a list of approved countries.	Geo restriction can be applied using the Kaltura Management Console (KMC) on each entry or in bulk. For more information about creation of access profiles via the KMC, refer to the article How to create an access profile.

Authorized domains	Restricts access to media based on a predefined list of approved domains.	Domain restriction is useful, for example, in case you want to make sure content can only be viewed from within your domains. For example – an internal training video can only be viewed from within the enterprise domain, or a course video can only be viewed from within the university domain.	Domain restriction can be applied using the Kaltura Management Console (KMC) on each entry or in bulk. For more information about creation of access profiles via the KMC refer to the article How to create an access profile.
Authorized IP addresses	Restricts access to media based on a predefined list of approved IP addresses	In case domain authorization is not granular enough (for example if there is a large organization comprising several networks serving different divisions, and there is a desire to limit access to a specific division only).	IP address restriction can be applied using the Kaltura Management Console (KMC) on each entry or in bulk. For more information about creation of access profiles via the KMC, refer to the article How to create an access profile.
Make your content playable only	Restrict content playback to Kaltura players from your	To prevent video theft, this feature also enhances	This setting can be turned on from within the Kaltura Management

within your Kaltura account and by your player	account only	brand awareness by showing your videos only on your branded player.	Console (KMC). If you already have content that was not secured this way, Kaltura support can assist in applying this security measure to existing entries as well.
Make your content available only in specific time windows	Configure a schedule for media entries, defining a start and end date. Playback will be allowed only within the defined schedule.	When you want to limit the time in which a media entry is available for viewing.	Scheduling can be applied using the Kaltura Management Console (KMC) on each entry or in bulk. For more information about scheduling, refer to the article More Actions Menu.
Kaltura Session Authentication for embed codes	Any published embed code of media requires a valid Kaltura Session to be passed to the embed code before the content is played. A Kaltura Session has a time expiration.	If you would like to restrict embed codes to play in authorized applications only.	Kaltura Session authentication for embed codes can be applied using the Kaltura Management Console (KMC) on each entry or in bulk. For more information about creation of access profiles via the KMC, refer to the article How to create an access profile.
URL tokenization	URL tokenization is a content protection offered at the CDN level. The token includes a TTL (time-to-live), so that if an end user tampers with the URL, their request for CDN content is denied. If a	All the access control solutions described in this table are enforced on the Kaltura Player level. If a sophisticated user spoofs the content URL,	URL tokenization is enabled on the CDN level, Kaltura's support team is available to set this up on your behalf.

	URL has an expired TTL, end-user requests for CDN content are denied.	these solutions will not be effective. URL tokenization helps prevent attempts to play the content outside of the Kaltura player. It is best to combine this feature with one of the other described access control features		

Note: This form of protection does not encrypt the content itself, but only restricts access to the content – according to the specifications listed.