Kaltura Access Control

Last Modified on 06/10/2026 3:15 pm IDT

This article is designated for administrators.

About

Organizations often need to control who can access their media and under what conditions. Depending on your requirements, you may want to restrict access to specific users, locations, domains, IP addresses, time periods, or applications.

Kaltura provides a range of access control features that help protect content and enforce viewing restrictions. The sections below summarize the available options and explain when to use each one.

This article provides an overview of Kaltura's access control capabilities. For configuration details, follow the links provided in each section.

These access control mechanisms do not encrypt the media itself. Instead, they restrict access to the content based on the configured rules and permissions.

Authentication on entry to the web page

Description	When to use it?	How to apply it?

Copyright © 2025 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.

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 Content Hubs / legacy Video Portal, 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 permissions, refer to the article User roles and permissions in Content Hubs. For integrations with LMSs (Learning 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

Description	When to use it?	How to apply it?

Copyright © 2025 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.

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 Rich Media Content Management System (Rich Media CMS) on each entry or in bulk. For more information, visit Create and manage access control profiles.

Authorized domains

Description	When to use it?	How to apply it?
Restricts access to media based on a predefined list of approved domains.	Domain restriction is useful, for example, if you want to make sure content can only be viewed from within your domains. An internal training video might only be viewable from within an enterprise domain, or a course video only from within a university domain.	Domain restriction can be applied using the Rich Media Content Management System (Rich Media CMS) on each entry or in bulk. For more information, visit Create and manage access control profiles.

Authorized IP addresses

Description	When to use it?	How to apply it?

Copyright © 2025 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.

Restricts access to media based on a predefined list of approved IP addresses.	When domain authorization is not granular enough (for example, if a large organization comprises 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 Rich Media Content Management System (Rich Media CMS) on each entry or in bulk. For more information, visit Create and manage access control profiles.

Make your content playable only within your Kaltura account and by your player

Description	When to use it?	How to apply it?
Restrict content playback to Kaltura players from your account only.	To help prevent video theft and ensure your content is viewed only through your branded player.	This setting can be turned on from within the Rich Media Content Management System (Rich Media CMS). 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

Description	When to use it?	How to apply it?
Configure a schedule for media entries by defining a start date and end date. Playback is allowed only within the defined schedule.	When you want to limit the period during which a media entry is available for viewing.	Scheduling can be applied using the Rich Media Content Management System (Rich Media CMS) on each entry or in bulk. For more information about scheduling, visit More Actions menu.

Kaltura Session Authentication for embed codes

Copyright © 2025 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.

Description	When to use it?	How to apply it?
Any published embed code of media requires a valid Kaltura Session (KS) 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 only in authorized applications.	Kaltura Session authentication for embed codes can be applied using the Rich Media Content Management System (Rich Media CMS) on each entry or in bulk. For more information, visit Create and manage access control profiles.

URL tokenization

Description	When to use it?	How to apply it?
URL tokenization is a content protection mechanism 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 URL has an expired TTL, end-user requests for CDN content are denied.	All the access control solutions described in this article are enforced at the Kaltura Player level. If a sophisticated user spoofs the content URL, these solutions will not be effective. URL tokenization helps prevent attempts to play content outside of the Kaltura player and is best combined with one of the other access control features described above.	URL tokenization is enabled at the CDN level. Kaltura Support can assist with setting it up.

Copyright © 2025 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.