Kaltura Online Video Security Capabilities

User Information

Version: 1.0

Kaltura Business Headquarters

250 Park Avenue South, 10th Floor, New York, NY 10003

Tel.: +1 800 871 5224

Contents

Overview of Kaltura Online Video Security Capabilities

Kaltura’s online video platform offers advanced video publishing, management, syndication and monetization solutions suitable for many verticals, including education, enterprise, government, media and entertainment, advertising, and many others. Kaltura’s flexible platform and APIs allow publishers and organization to rapidly, and cost-effectively, build video applications, widgets and plug-ins, as well as add core video services to their existing offerings.

Whether you publish video on the web or use it only for internal audiences, it is important for you to address the security aspects of your online video strategy. Kaltura offers various effective ways to implement the right level of security for your needs and has built in physical, architectural and applicative security measures that provide end-to-end protection for your assets and information.

Whether you choose a Software as a Service (SaaS) implementation using our scalable infrastructure and trusted CDN partner, or opt for a self-hosted and self-operated platform on your own premises (Kaltura On-Prem™), Kaltura will help you implement the security measures you need to have in place, while assuring an intuitive and smooth experience for your end users.

This guide provides an overview of the security capabilities that Kaltura offers and includes a high level description of the Kaltura security capabilities for video based content – including ingestion, storage and delivery. The methods that Kaltura uses to protect user information are described, in addition to Kaltura’s business continuity and disaster recovery policies, Kaltura’s secure platform architecture, and the physical security Kaltura maintains in its hosting facilities. If you require a more in depth description of Kaltura’s security capabilities, please contact a Kaltura representative.

The options can be used as standalone capabilities – or used together to provide a full security package.

.

Forensic Watermarking

Forensic watermarking is a process where a unique indivisible mark is added to the content. This mark indicates the originator of the video content (e.g. the studio, aggregator, content owner) and also the authorized user accessing the content. This makes it easy for the content owners to track down any acts of illegal use of the content, such as piracy, illegal recordings and distributions.

Kaltura adds the forensic watermark to the content on the fly, minimizing the storage footprint and making sure the watermark can be added to any supported delivery profile.

Kaltura Access Control

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) 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 within your Kaltura account and by your player	Restrict content playback to Kaltura players from your account only	To prevent video theft, this feature also enhances brand awareness by showing your videos only on your branded player.	This setting can be turned on from within the Kaltura Management 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 How to configure content scheduling?

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 URL has an expired TTL, end-user requests for CDN content are denied.	All the access control solutions described in this table are enforced on 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 the content outside of the Kaltura player. It is best to combine this feature with one of the other described access control features	URL tokenization is enabled on the CDN level, Kaltura's support team is available to set this up on your behalf.

This form of protection does not encrypt the content itself, but only restricts access to the content – according to the specifications above

Protecting Content in Transit

Some organizations are concerned about the security of their media as it is being streamed. Content can be hijacked using man-in-the-middle attacks or other stream capture methods, and then the content can be stored locally or published illegally.

To protect your content in transit, you can use a secured streaming protocol. You can configure the CDN to stream over an encrypted protocol (HTTPS/RTPME) to prevent exposure of the content in transit. The Kaltura platform allows you to easily implement secured streaming.

AES Encryption

To support content protection on delivery, Kaltura supports AES standard encryption of content delivery for HLS delivery. Content is encrypted on the fly utilizing the Kaltura on the fly packager, and the Kaltura player can access the decryption key on the Kaltura servers to decrypt content as it is being played back.

Encryption at Rest

To support secure storage of content on the Kaltura servers, Kaltura employs encryption at rest of content. Encryption is on a per rendition level, with the encryption done as part of the transcoding process. Content is securely transitioned and stored thought the whole ingest/transcoding process.

Encryption at rest is especially beneficial for customers utilizing the Kaltura uDRM module. Since Kaltura utilizes on the fly packaging and encryption for DRM content, customers can enjoy the benefits of storing only the original content renditions – without the need of storing pre encrypted DRM flavors, and still make sure content is stored securely utilizing encryption at rest.

See Digital Rights Management for more information.

Digital Rights Management

DRM offers another layer of content protection, by adding a license policy to the content encryption.

By adding a license, content owners can make sure that only authorized users can have access to decryption keys – and can tie their content to their business modules and protection policies.

The Kaltura uDRM module is fully integrated with Kaltura business modules definitions, making it possible for content owners to define complex business scenarios – supporting AVOD, TVOD and SVOD configurations.

Kaltura offers a full multi DRM solution – supporting all major DRM schemas including

- Microsoft PlayReady
- Google Widevine
- Apple Fairplay

By supporting all DRM schemas – content owners can ensure their content is fully DRM protected across all devices, browsers and OS, as Kaltura delivers the most natively supported and security enhanced schema on playback – utilizing the Kaltura on the fly packager. This also ensures a minimal storage foot-print, by enabling the content owners to store only the original transcoded renditions – instead of pre encrypted renditions for all DRM schemas.

DRM protection is usually required when using premium content on a monetized service and is usually a content owner/studio requirement.

The Kaltura uDRM module is integrated with the Kaltura player and the Kaltura on the fly packager, to offer a complete, easy to setup DRM eco system. In addition, since the uDRM module is API-driven – it is easily integrated with external video head ends and players is needed.

For additional information about the Kaltura uDRM solution, see here.

Desktop Browser Support for DRM

Browser	Delivery Format	DRM
IE < 11	Smooth Stream	PlayReady
IE >= 11, Edge	Dash	PlayReady
Chrome	Dash	Widevine
Safari	HLS	Fairplay
Firefox	Smooth Stream Dash	PlayReady Widevine

Mobile Device Support for DRM

Mobile Device/OS	Delivery Format	DRM
Android 4.1	WVM	Widevine Classic
Android >= 4.2	Dash	Widevine Modular
iOS	HLS	Fairplay

Connected Devices Support

- ⭐ marks devices that are not supported by Kaltura player SDK and DRM plugin. Support is in the form of uDRM licensing API with integration to external players

Device	Delivery Type	DRM
Chromecast	Dash Dash	Widevine PlayReady
XBox⭐	Smooth Stream	PlayReady
AppleTV⭐	HLS	Fairplay
GoogleTV⭐	WVM Smooth Stream	Widevine Classic PlayReady

Device	Delivery Type	DRM
FireTV⭐	Smooth Stream	PlayReady
SmartTV Alliance (LG, Phillips, Panasonic, Toshiba)⭐	Smooth Stream WVM	PlayReady Widevine Classic
Samsung TV⭐	Smooth Stream WVM	PlayReady Widevine Classic
HBBTV (1.5+)⭐	DVB Dash	PlayReady