Overview of Kaltura security features

Last Modified on 06/10/2026 2:13 pm IDT

This article is designated for administrators.

About

This article provides an overview of the security capabilities available in Kaltura. These capabilities help protect content during storage, delivery, and playback and support a range of organizational security requirements.

The security features described here can be used individually or together to help protect your content and control access to your media.

Content protection

Protecting content in transit

Content can be vulnerable to interception while it is being delivered across a network. To help protect content during delivery, Kaltura supports secure streaming and encrypted transport protocols.

Content can be delivered over encrypted protocols such as HTTPS, helping protect content while it is in transit between the server and the viewer.

AES encryption

Kaltura supports AES encryption for HLS content delivery.

Content is encrypted during delivery, and authorized players can securely obtain the decryption key required for playback.

Encryption at rest

To protect content stored in Kaltura, media assets are encrypted at rest using AWS Key Management Service (KMS).

For organizations with advanced security requirements, Kaltura also supports Hold Your Own Key (HOYK), which allows customers to manage the encryption keys used to protect their content.

Encryption at rest protects content while it is stored within Kaltura's infrastructure. DRM can be applied in addition to encryption at rest to protect content during delivery

and playback.

For more information, see Hold Your Own Key (HOYK).

Digital Rights Management (DRM)

Digital Rights Management (DRM) adds an additional layer of protection by controlling access to encrypted content during playback.

Kaltura supports multi-DRM delivery, including:

- Microsoft PlayReady
- Google Widevine
- Apple FairPlay.

For more information, see Digital Rights Management (DRM).

Access control

Kaltura provides several mechanisms for controlling access to media, including:

- Authentication and authorization
- Geographic restrictions
- Domain restrictions
- IP address restrictions
- Time-based availability windows
- Kaltura Session authentication
- URL tokenization

For detailed information, see Kaltura Access Control.

Application security

HTML Purifier

HTML Purifier is a standards-compliant HTML filtering library that removes potentially malicious code and helps protect against vulnerabilities such as cross-site scripting (XSS).

It sanitizes user-generated HTML while preserving valid content and can be configured to allow specific tags and attributes when needed.

Kaltura accounts can be configured to use HTML Purifier with different filtering policies based on customer requirements. For more information, contact your Kaltura

representative.

Related security features

Depending on your deployment and requirements, additional security features may be available, including:

- Secure embed (authenticated and entitlement-based access for embedded content)
- Authentication and single sign-on (SSO)
- Access control
- Customer-managed encryption keys (HOYK)
- Digital Rights Management (DRM)