Preparing for Third-party Cookie Restrictions

This article is designated for all users.

Phasing out third-party cookies in Chrome

Google Chrome is gradually restricting third-party cookies, and introducing "partitioned cookies" (CHIPS). This affects various Kaltura use cases, necessitating proactive measures by users to navigate these adjustments smoothly.

Understanding third-party cookies

A third-party cookie is a tiny data snippet stored on a user's device (like a computer, cellphone, or tablet) by a website other than the one the user is currently viewing. These cookies enable cross-site tracking but face restrictions due to privacy concerns.

Kaltura use cases affected

Kaltura utilizes cookies in specific use cases. These may qualify as “third-party cookies” when Kaltura components are embedded in other websites. These are the main products and features impacted by this change:

- KAF integrations, including LMS video
- Secure embed
- Player embed

Video Portal (Mediaspace) customers are not impacted by this change unless using secure embed. In addition, customers embedding Kaltura rooms or chat widget won't be affected.

Customers leveraging marketplace partner applications as part of Video Portal or KAF applications will need to validate and ensure support with the relevant partner.

How to prepare for change

Avoid third-party cookies by setting an alias domain

Give your KAF url an alias to match your LMS url to avoid a "cross-domain" situation. This ensures Kaltura will be under the same domain, preventing cookies from being considered “third-party”. You can follow the instructions in the How to avoid the "3rd party cookie" error message in the KAF based LMS Integrations article.

CHIPS (Cookies Having Independent Partitioned State)

If an alias hostname is not available, use CHIPS to enable partitioned cookies. Supported only on Chrome, CHIPS maintains a consistent user experience across sites. To enable partitioned cookies support in Kaltura, navigate to your KMS Admin, locate the Application module, and enable the **usePartitionedCookies** field.

For KAF instances using the default Kaltura.com domain, partitioned cookies are dynamically enabled upon page load. Please note that although the admin field may display "No," this functionality is active.

Additional tips for Chrome users

Manually uncheck the option to block third-party cookies in Chrome's settings to reduce the likelihood of encountering "third-party cookie" error messages. For details, refer to Google's guide on managing cookies in Chrome.

These adjustments are part of ongoing efforts to enhance user privacy and security. By taking these steps, you ensure a smooth transition and continued optimal functionality with Kaltura.

Implications of using partitioned cookies

Secure Embed

Secure embeds require authentication before you can watch the content. The process depends on the authentication method and identity provider in your Kaltura setup using cookies.

For users employing secure embeds with partitioned cookies, here's what to expect:

- **User authentication to Video Portal (KMS):** After authenticating to Video Portal, if the user goes to another site with a secure embed, they'll need to re-login to access the secure embed content.
- **User authentication across sites:** If the user isn't authenticated to Video Portal and logs in on another site with secure embed content, then goes back to Video Portal, they'll need to re-login to the Video Portal.
- **Multiple tabs scenario:** If a user has two tabs open - one for Video Portal and another for a site with secure embed, and they log out of Video Portal, they'll still be logged into the secure embed (assuming the session is active).
- **Automatic logout:** There's no active logout option for users in secure embed. Instead, users are automatically logged out when the session times out.
- **Single login for external sites:** Users only need to log in once for a secure embed on a specific external site. If there are additional secure embeds on other

pages within the same domain, the user is considered authenticated for all of them (the cookie is in the right partition).

- **Separate authentication for different sites:** For secure embeds on different external sites, users need to authenticate separately, as each external site is treated as a separate partition.

While partitioned cookies can handle some cases, existing browser security and privacy limitations mean that if authentication occurs **outside the secure embed iframe**, the partitioned cookie flow won't complete, preventing access to the embedded video. This issue is particularly impactful for users leveraging this capability, as most Identity Providers (IdPs) today can't be opened in an iframe (x-frame-options: DENY).

In a scenario where secure embed is set to authenticate outside the iframe, here's what happens:

1. User visits an external site like sharepoint.company.com, loading an iframe of KMS (e.g., *12345.mediaspace.kaltura.com*).
2. The browser creates a "partition" on sharepoint.company.com and places an anonymous cookie of *12345.mediaspace.kaltura.com* in that partition.
3. KMS inside the iframe redirects to authentication in the browser's top window (where *sharepoint.company.com* was loaded).
4. KMS performs authentication (with IdP or user/password) and sets a user cookie in a new partition belonging to *12345.mediaspace.kaltura.com*.
5. KMS redirects back to the sharepoint page.
6. The browser loads the *sharepoint.company.com* page and the KMS iframe inside it, using the anonymous cookie from the *sharepoint.kaltura.com* partition.
7. KMS redirects again to authentication because the user is not authenticated within that partition.

In this setup, when partitioned cookies are enabled, the secure embed won't work on the external site. Valid options for secure embed to work are:

- Not using alias; secure embed, authentication of secure embed **inside** the iframe; partitioned cookies enabled. Note: This works if your authentication method can be loaded in an iframe (may not work with Okta, for example).
- Not using alias; secure embed, authentication of secure embed **outside** the iframe; partitioned cookies disabled. Note: This works if the browser allows third-party cookies.
- Using alias; secure embed, authentication **inside or outside** the iframe; partitioned cookies disabled. Note: This setup always works because there's no 3rd

party cookie issue.

KAF

Turning on partitioned cookies will also block KAF urls outside the LMS, for example, navigating to the KAF's my-media after the user has been identified via the LMS will results in access denied.

Player Embed

Kaltura Player's cookie-based user preferences face changes. Upgrade to the latest Kaltura Player version (V7) for seamless preference storage. To learn more, visit our articles in Upgrading to the Kaltura Player.

[template("cat-subscribe")]