Understand third-party cookie restrictions in Content Hubs, legacy Video Portal and KAF

Content updated: 01/22/2024

This article is designated for administrators.

About

Google Chrome is gradually restricting third-party cookies and introducing partitioned cookies (CHIPS). This change affects several Kaltura use cases. This article explains how the change affects Kaltura and how to prepare for it.

To resolve third-party cookie issues, see Set up an alias hostname for Content Hubs and KAF integrations.

What are third-party cookies?

A third-party cookie is a small piece of data stored on your device, such as a computer, phone, or tablet, by a website other than the one you're viewing. These cookies allow cross-site tracking, so browsers are restricting them to protect privacy.

Affected Kaltura use cases

Kaltura uses cookies in some use cases. When Kaltura components are embedded in other websites, these cookies can count as third-party cookies. This change mainly affects these products and features:

- KAF integrations, including **LMS Extensions**
- Secure embed
- Player embed

In this article, "your site" means your Content Hubs, legacy Video Portal or KAF site. This change doesn't affect your site unless you use secure embed. Embedded Kaltura rooms and chat widgets aren't affected either.

If you use marketplace partner applications with your site, check with the partner that their application supports this change.

Prepare for the change

Set an alias domain to avoid third-party cookies

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.

Give your KAF URL an alias that matches your LMS URL. This puts Kaltura under the same domain as your LMS, so its cookies don't count as third-party cookies. For step-by-step instructions, see Set up an alias hostname for Content Hubs and KAF integrations .

Use partitioned cookies

If you can't use an alias hostname, you can use partitioned cookies, also called CHIPS (Cookies Having Independent Partitioned State). To enable partitioned cookies, contact your Kaltura representative. After you enable them, all users might need to clear their cookies for your site.

When partitioned cookies are enabled, KAF URLs might not work outside the LMS. For example, if you open **My Media** directly, outside the LMS, you might get an access denied error.

More tips for Chrome users

To reduce third-party cookie error messages, turn off the setting that blocks third-party cookies in your Chrome settings. For details, see Google's help on managing cookies in Chrome.

Taking these steps helps Kaltura keep working as expected while browsers tighten privacy and security.

What to expect with partitioned cookies

Secure embed

Secure embeds require users to log in before they can watch the content. The login process uses cookies, and it depends on the authentication method and identity provider set up for your Kaltura account.

If you use secure embeds with partitioned cookies, here's what to expect:

- **Logging in to your site first:** After a user logs in to your site and then goes to another site with a secure embed, they need to log in again to watch the secure embed content.
- **Logging in on another site first:** If a user logs in on another site with secure embed content before logging in to your site, they need to log in again when they go to your site.
- **Multiple tabs:** If a user has one tab open on your site and another on a site with a secure embed, logging out of your site doesn't log them out of the secure embed, as

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.

long as the session is active.

- **Automatic logout:** Users can't log out of a secure embed. Instead, they're logged out automatically when the session times out.
- **One login per external site:** Users log in once for a secure embed on a specific external site. They're then authenticated for secure embeds on other pages in the same domain, because the cookie is in the correct partition.
- **Separate login for each external site:** Users need to log in separately to secure embeds on different external sites, because the browser treats each external site as a separate partition.

Partitioned cookies handle some cases, but browser security and privacy limits still apply. If authentication happens **outside the secure embed iframe**, the partitioned cookie flow doesn't complete, and the user can't watch the embedded video.

This affects many users, because most identity providers (IdPs) can't be opened in an iframe (`x-frame-options: DENY`).

Here's what happens when secure embed is set to authenticate outside the iframe:

1. A user visits an external site, such as `sharepoint.company.com` , that loads your site (for example, `12345.mediaspace.kaltura.com`) in an iframe.
2. The browser creates a partition for `sharepoint.company.com` and places an anonymous cookie from `12345.mediaspace.kaltura.com` in that partition.
3. Your site, inside the iframe, redirects to authentication in the browser's top window, where `sharepoint.company.com` was loaded.
4. Your site authenticates the user, through the IdP or with a username and password, and sets a user cookie in a new partition that belongs to `12345.mediaspace.kaltura.com` .
5. Your site redirects back to the SharePoint page.
6. The browser loads the `sharepoint.company.com` page and your site's iframe inside it, using the anonymous cookie from the `sharepoint.company.com` partition.
7. Your site redirects to authentication again, because the user isn't authenticated in that partition.

In this setup, secure embed doesn't work on the external site when partitioned cookies are enabled. Secure embed works with any of these setups:

- No alias hostname, authentication **inside** the iframe, and partitioned cookies enabled. This works if your authentication method can load in an iframe. For example, it might not work with Okta.

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.

- No alias hostname, authentication **outside** the iframe, and partitioned cookies disabled. This works if the browser allows third-party cookies.
- An alias hostname, authentication **inside or outside** the iframe, and partitioned cookies disabled. This setup always works, because there's no third-party cookie issue.

Player embed

Kaltura Player stores some user preferences in cookies, and this change affects them. To keep storing preferences correctly, upgrade to the latest Kaltura Player (v7). For more information, see How to upgrade your V2 players to v7 in Kaltura.

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.