Chrome / Edge Local Network Access (LNA) and Kaltura eCDN

Last Modified on 08/30/2026 7:33 pm IDT

This article is designated for administrators.

About

Starting with **Chrome 142**, Google enforces **Local Network Access (LNA)** restrictions that control requests from public websites to private or local network addresses. Microsoft Edge is introducing similar restrictions.

This change can affect **Kaltura eCDN** environments where a public-facing Kaltura domain communicates with **Kaltura Edge Servers (KES)** or peers on your internal network. When users access Kaltura using an affected browser, this communication can be blocked unless your organization allows the required access.

No changes are required in Kaltura products. Your IT or security team should determine whether an exception is required and configure the appropriate browser policy.

For more information about the browser changes, see:

- Chrome 142 stable release notes
- Local Network Access restrictions

Why this is happening

Chrome's Local Network Access (LNA) feature helps protect local networks by restricting requests from public websites to private network or local device addresses unless access is permitted. LNA replaces Google's earlier Private Network Access (PNA) approach.

Affected: Requests from public domains to private network or local addresses on Chrome 142 or later. eCDN features that depend on local or peer connections can be blocked without an allow-list.

Not affected: Older Chrome versions, Firefox, Safari, and environments that use only public CDN delivery with no local network connections.

For more information, see New permission prompt for Local Network Access.

What you might see

If Local Network Access is blocked, you might experience:

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.

- Playback failures when an internal eCDN endpoint is involved.
- Errors in the browser's Console or Network tools, such as Permission was denied for this request to access the unknown address space.
- CORS errors for requests from a public website to a private network address.
- eCDN optimization or peering features not working as expected.

The exact behavior depends on your eCDN deployment.

Check if your eCDN is affected

1. If playback fails in Chrome 142 or later, open the browser's developer tools and check the **Console** and **Network** tabs for Local Network Access or CORS errors.
2. Identify the public-facing Kaltura domain that needs local network access, such as your Content Hubs, legacy Video Portal, or custom Kaltura domain.
3. Determine whether your eCDN workflow requires communication between the public domain and a local network endpoint.
   - If local network access is required, configure an enterprise allow-list as described in **Option A** below.
   - If local network access isn't required, no browser policy change is needed. Don't globally disable LNA.

Remediation options

Option A: Add an enterprise allow-list (recommended)

The recommended approach is to use the `LocalNetworkAccessAllowedForUrls` enterprise policy in Chrome or Edge to allow only the public origins that require Local Network Access.

Add the requesting public origin to the allow-list, not the local endpoint it connects to. Depending on your environment, this can include:

- Your custom Kaltura host.
- Your organization's Kaltura domain.
- Other trusted SaaS origins that need to communicate with local endpoints.

For Windows, use the following registry paths:

Chrome

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\LocalNetworkAccessAllowedForUrls`

Edge

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.

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge\LocalNetworkAccessAllowedForUrls`

Limit the exception to the minimum set of required origins. Set an appropriate time limit for the exception and monitor it using your endpoint or browser policy reporting.

You can also use `BlockedForUrls` to block unknown origins from accessing the local network.

Option B: Use a temporary opt-out

If an allow-list can't be deployed immediately, you can use a temporary opt-out as a short-term emergency measure.

Apply the following Chrome Enterprise policy:

`LocalNetworkAccessRestrictionsEnabled: false`

Set a date to remove the temporary opt-out and have a rollback plan in place. Move to **Option A** as soon as possible.

Browser policy options can change or be deprecated. Check the current browser documentation before applying or updating the policy.

Document and review the exception

Any allow-list for Local Network Access is a security exception. It gives specified public sites access to resources on your local network.

Your IT or security team should:

- Document who owns and approves the exception.
- Record why each origin requires local network access.
- Document which sites are allowed and how long the exception will remain in place.
- Review and monitor the exception regularly.
- Remove origins when they no longer require access.
- Make sure the configuration follows your organization's security policies and applicable regulations.

Kaltura provides guidance, but your organization is responsible for deciding whether Local Network Access should be allowed and for managing the associated browser policies.

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.

Browser policies can change. Check the official browser documentation for the latest information.

References

- Chrome Enterprise Policy List
- Chrome Local Network Access
- Chrome 142 stable release notes
- Local Network Access restrictions
- Microsoft Edge LocalNetworkAccessAllowedForUrls policy

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.