Chrome 142 Enterprise and Education release notes

For administrators who manage Chrome browser or Chrome devices for a business or school.

These release notes were published on October 22, 2025.

See the latest version of these release notes online at https://g.co/help/ChromeEnterpriseReleaseNotes

Chrome 142 release summary

Current Chrome browser updates	Security / Privacy	User productivity / Apps	Management
Simplified sign-in and sync experience on Chrome Desktop	✓	✓	
Disable force-installed extensions with non-malware violations	✓		
Multiprofile support in the Share extension in Chrome on iOS		✓	
Client's LLM assistance in mitigating scams	✓		
Local network access restrictions	✓		
Origin-keyed process Isolation	✓		
PostQuantum Cryptography for DTLS in WebRTC	✓		
Sticky user activation across same-origin renderer-initiated navigations			✓
Chrome DevTools integration with Google Developer Program			✓
Chrome for iOS New tab page background customization		✓	
New policies in Chrome browser			✓
Chrome Enterprise Core updates	**Security / Privacy**	**User productivity / Apps**	**Management**
No updates in this release.			

Chrome Enterprise Premium updates	Security / Privacy	User productivity / Apps	Management
Chrome Browser Rule UX refactor	✓		✓
Streamlined Chrome Enterprise to Google SecOps integration	✓		
Upcoming Chrome browser updates	**Security / Privacy**	**User productivity / Apps**	**Management**
Allowlist for Isolated Web App managed installation			✓
Deprecate and remove XSLT	✓	✓	✓
Gemini in Chrome		✓	
ICU 77 (supporting Unicode 16)			✓
Origin-Bound Cookies (by default)			✓
Update to No HTTPS warning design	✓		
Bundled security settings	✓		
Deprecating savedTabGroups as individual value in SyncTypesListDisabled			✓
HSTS tracking prevention	✓		
Happy Eyeballs V3	✓		✓
Multicast support for Direct Sockets API			✓
ServiceWorkerAutoPreload			✓
2SV enforcement for admins			✓
CSS find-in-page highlight pseudos			✓
Change in launch schedule starting in Chrome *Early Stable* 145			✓

Clear window name for cross-site navigations that switches browsing context group			✓
Disallow spaces in non-file:// URL hosts	✓		
Remove third-party storage partitioning policies	✓		
X25519Kyber768 key encapsulation for TLS	✓		
Isolated Web Apps			✓
UI Automation accessibility framework provider on Windows		✓	
SafeBrowsing API v4 → v5 migration	✓		
Upcoming Chrome Enterprise Core updates	**Security / Privacy**	**User productivity / Apps**	**Management**
Enterprise-managed shortcuts on the *New tab* page		✓	✓
Profile reporting for Chrome on iOS			✓
Upcoming Chrome Enterprise Premium updates	**Security / Privacy**	**User productivity / Apps**	**Management**
Increased file size support for DLP scans	✓		✓

The enterprise release notes are available in 9 languages. You can read about Chrome's updates in English, German, French, Dutch, Spanish, Portuguese, Korean, Indonesian, and Japanese. Allow 1 to 2 weeks for translation for some languages.

Chrome Enterprise and Education release notes are published in line with the Chrome release schedule, on the Early Stable date for Chrome browser.

Current Chrome browser updates

Simplified sign-in and sync experience on Chrome Desktop

Chrome will launch a simplified and consolidated version of sign-in and sync in Chrome on Windows, Mac and Linux. Chrome sync will no longer be shown as a separate feature in settings or elsewhere. Instead, users can sign-in to Chrome to use and save data such as passwords, bookmarks and more in their Google Account, subject to the relevant enterprise policies. Additionally, users who are signed in to Chrome can also opt in to syncing their tabs and browsing history in their Google Account, here again subject to the relevant enterprise policies. As before, the functionality previously part of Chrome sync that saves and accesses Chrome data in the Google Account can be turned off via SyncDisabled and SyncTypesListDisabled. Sign-in to Chrome can be disabled via BrowserSignin as before.
The changes do not affect users' ability to sign in to Google properties on the web (for example, Gmail) without signing in to Chrome, their ability to remain signed out of Chrome, or their ability to control what information is synced with their Google Account.
These changes are pretty similar to the simplified sign-in and sync experience that was launched on iOS in 117 and on Android in 127.

- **Chrome 142 on Linux, macOS, Windows:** Gradual roll-out

Disable force-installed extensions with non-malware violations

This feature silently disables force-installed extensions exhibiting violations of Chrome Web Store policies (CWS) in unmanaged browser environments. Such violations include general program violations, unwanted software and potential security vulnerabilities not classified as malware. Users retain the ability to enable/disable these extensions, but will not be able to remove them.
A new enterprise policy, ExtensionForceInstallWithNonMalwareViolationEnabled, will be added in 142 to preserve the existing behavior for unmanaged browser environments, but will be removed in 145.

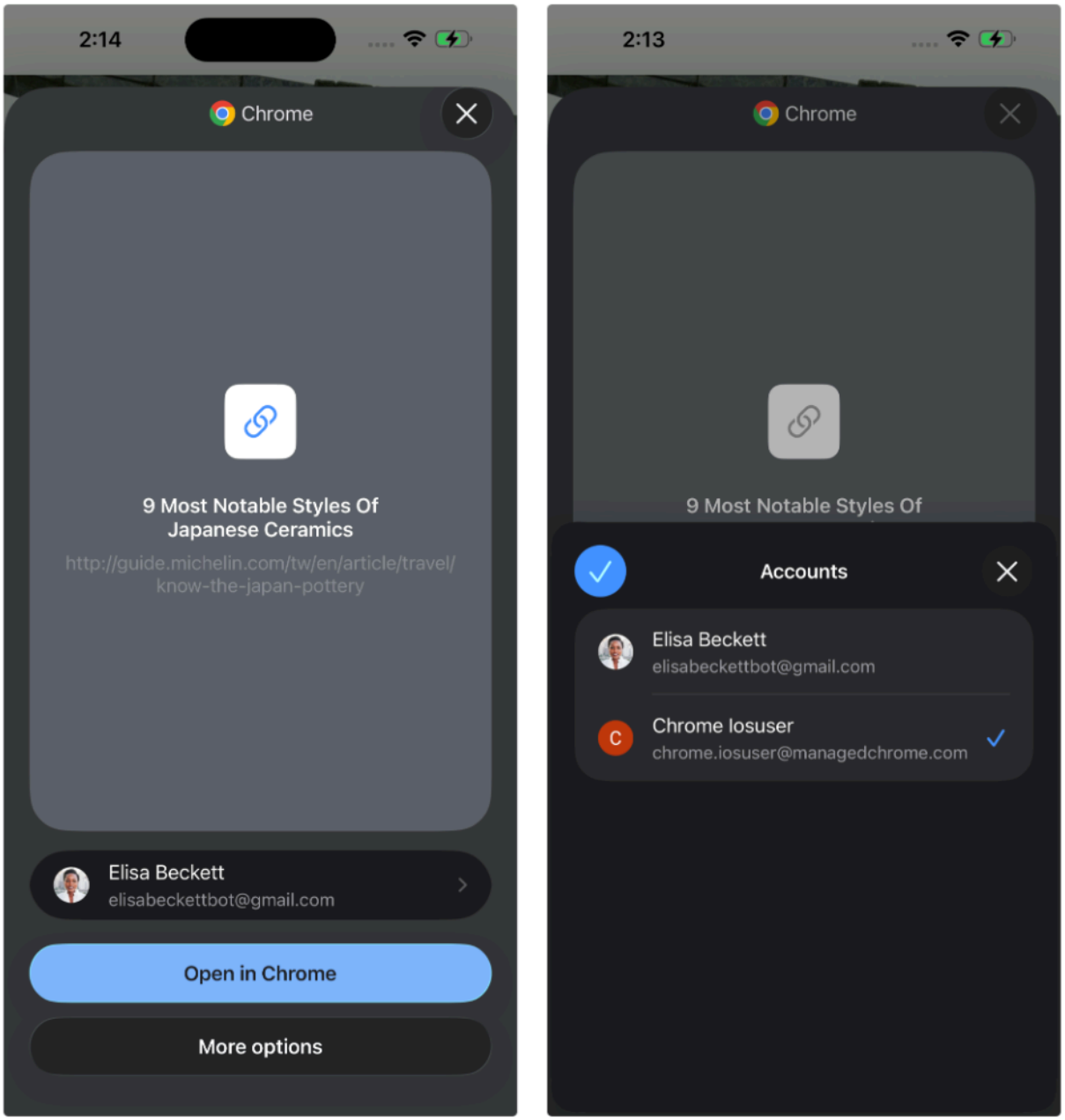
This change does not affect managed instances of Chrome that are joined to a Microsoft Active Directory domain, joined to Microsoft Azure Active Directory or enrolled in Chrome Enterprise Core. On macOS, this change does not affect instances of Chrome that are managed via MDM, joined to a domain or enrolled in Chrome Enterprise Core.

- **Chrome 142 on MacOS, Windows:** In Chrome 142 for Windows and macOS, force-installed extensions with minor policy violations will be silently disabled in low-trust environments.
- Chrome 145 on MacOS, Windows: The ExtensionForceInstallWithMinorPolicyViolationEnabled policy will be removed.

Multi-profile support in Share extension in Chrome on iOS

As early as Chrome 142 on iOS, Chrome Share extension allows users to see the currently-used profile and change it before opening a URL in Chrome or searching text or image. For users who have multiple profiles enabled, when they want to share a URL or select text or an image, then select Chrome they would be able to see Chrome Share extension with an account avatar. If users do nothing, it will open the share intent in the selected profile.
To change the profile from the Chrome Share extension, users click on it and select the desired profile. Chrome then switches the profiles accordingly. If work profiles are allowed by enterprise policy, users can set the widgets profile. If only personal or if only corporate profiles are allowed, multi-profile support is not enabled, then widgets continue to function as before.

- **Chrome 142 on iOS**



Client's LLM assistance in mitigating scams

Users on the webs are facing significant amounts of several kinds of scams on a daily basis. To combat these scams, Chrome leverages on-device Large Language Model (LLM) to identify scam websites for Enhanced Safe Browsing users. Chrome sends the page content to an on-device LLM to infer security-related signals of the page and send these signals to Safe

Browsing server side for a final verdict. When enabled, Chrome may consume more bandwidth to download the LLM.

- Chrome 134 on Linux, macOS, Windows: Gather the brand name and intent summary of the page that triggers keyboard lock to identify scam websites.
- Chrome 135 on Linux, macOS, Windows: Show the warnings to the user based on the server verdict which uses the brand and intent summary of the page that triggered keyboard lock.
- Chrome 137 on Linux, macOS, Windows: Gather brand and intent summary of the page based on server reputation scoring system.
- Chrome 138 on Linux, macOS, Windows: Show the warnings to the user based on the server verdict which uses the brand and intent of the pages that the server reputation system scored.
- **Chrome 142 on Android**

Local network access restrictions

Chrome 142 restricts the ability to make requests to the user's local network, gated behind a permission prompt.
A local network request is any request from a public website to a local IP address or loopback, or from a local website (for example, Intranet) to loopback. Gating the ability for websites to perform these requests behind a permission mitigates the risk of cross-site request forgery attacks against local network devices such as routers, and reduces the ability of sites to use these requests to fingerprint the user's local network.
This permission is restricted to secure contexts. If granted, the permissions additionally relaxes mixed content blocking for local network requests (since many local devices are not able to obtain publicly trusted TLS certificates for various reasons).
This work supersedes a prior effort called Private Network Access which used preflight requests to have local devices opt-in.
Information on how to adapt to this feature can be found here.

- **Chrome 142 on Windows, MacOS, Linux, Android**

Origin-keyed process isolation

Chrome 142 introduces a shift in the process isolation policy from locking processes to a site like `https://example.com` to locking them to a specific origin, such as, https://foo.example.com.
To further enhance security, Chrome is moving to a more granular process isolation model called **Origin Isolation**. Previously, Chrome used **Site Isolation**, which grouped different origins from the same site (for example, `https://a.example.com` and https://b.example.com) into a single renderer process.
With Origin Isolation, each individual origin (for example, `https://foo.example.com`) will be isolated in its own renderer process. This change strengthens Chrome's security architecture by better aligning process boundaries with the web's fundamental origin-based security model, offering greater protection against potential vulnerabilities within sites.

Potential performance considerations: While each individual process will be smaller, this increase in process granularity may lead to higher overall memory and CPU usage. To balance security and performance, Origin Isolation will be enabled by default only on devices with at least 4GB of RAM.
Enterprise Control: Admins can control this feature using the OriginKeyedProcessesEnabled policy.

- **Chrome 142 on ChromeOS, Linux, Windows**

PostQuantum cryptography for DTLS in WebRTC

This feature will enable the use of PostQuantum Cryptography (PQC) with WebRTC connections. The motivation for PQC is to get WebRTC media traffic up to date with the latest cryptography protocols and prevent *Harvest Now to Crack Later* scenarios.

Admins will be able to control this feature using an enterprise policy WebRtcPostQuantumKeyAgreement, to allow enterprise users to opt out of PQC. The policy will be temporary and is planned to be removed by Chrome 152.

- **Chrome 142 on Android, ChromeOS, Linux, macOS, Windows, Fuchsia**
- Chrome 152 on Android, ChromeOS, Linux, macOS, Windows, Fuchsia: Remove Enterprise Policy

Sticky user activation across same-origin navigations

This feature preserves the sticky user activation state after a page navigates to another same-origin page. The lack of user activation in the post-navigation page prevents some use cases like showing virtual keyboards on auto-focus, and this has been a blocker for the developers who want to build Multi-page Applications (MPAs) over Single-page Applications (SPAs).

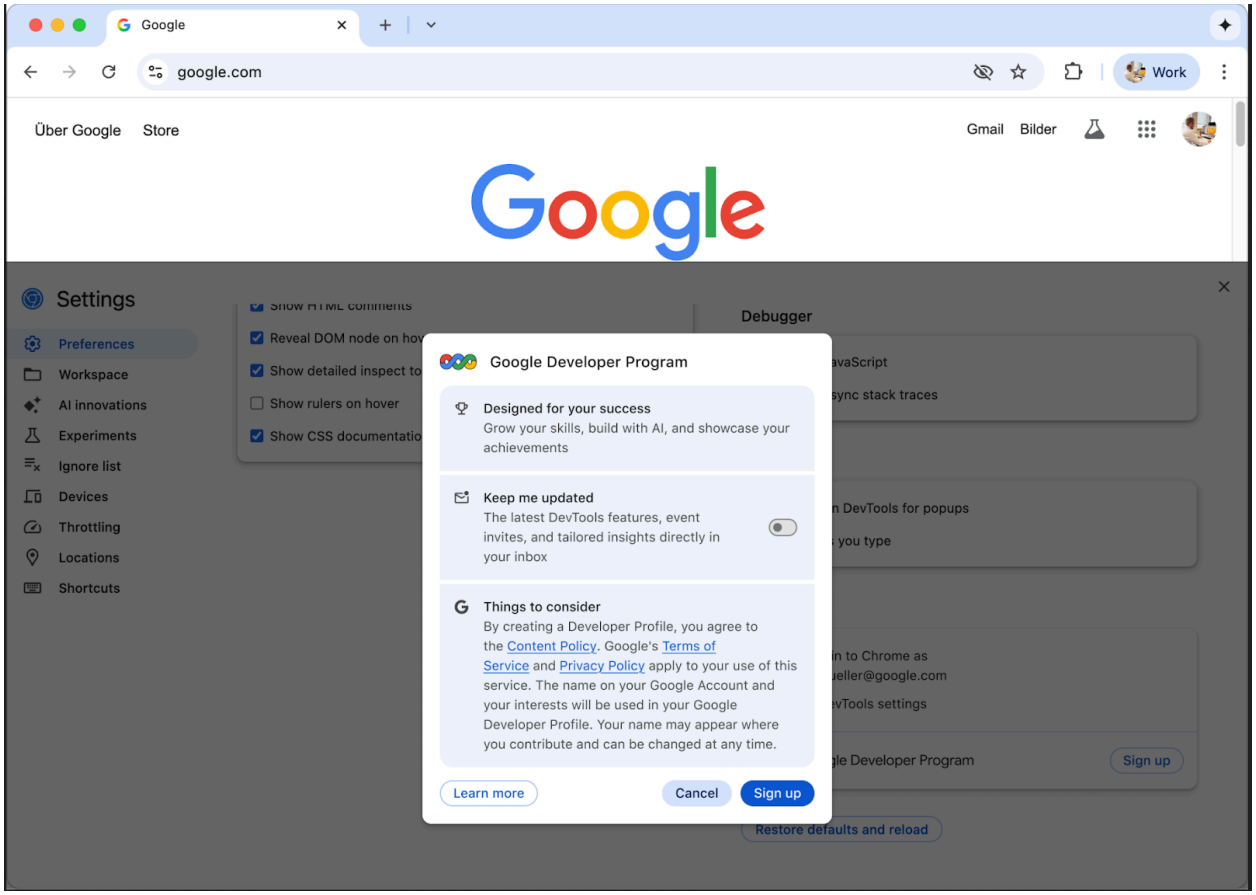
- **Chrome 142 on Windows, macOS, Linux, Android**

Chrome DevTools integration with Google Developer Program

This feature will integrate the Google Developer Program (GDP) with Chrome DevTools (CDT) to enable and enhance developer engagement. The integration will introduce a badge system to reward users for interacting with DevTools and provide a seamless in-tool experience for signing up for the GDP, ultimately fostering a more connected and discoverable ecosystem for developers.

The DevToolsGoogleDeveloperProgramProfileAvailability policy would enable the admins to integrate the Google Developer Program with Chrome DevTools. The user's Google Developer Program profile is shown in Chrome DevTools, and users receive badges for performing specific actions within.

- **Chrome 142 on ChromeOS, Linux, MacOS, Windows:** Chrome DevTools offers web developers the ability to connect and integrate with the Google Developer Program.

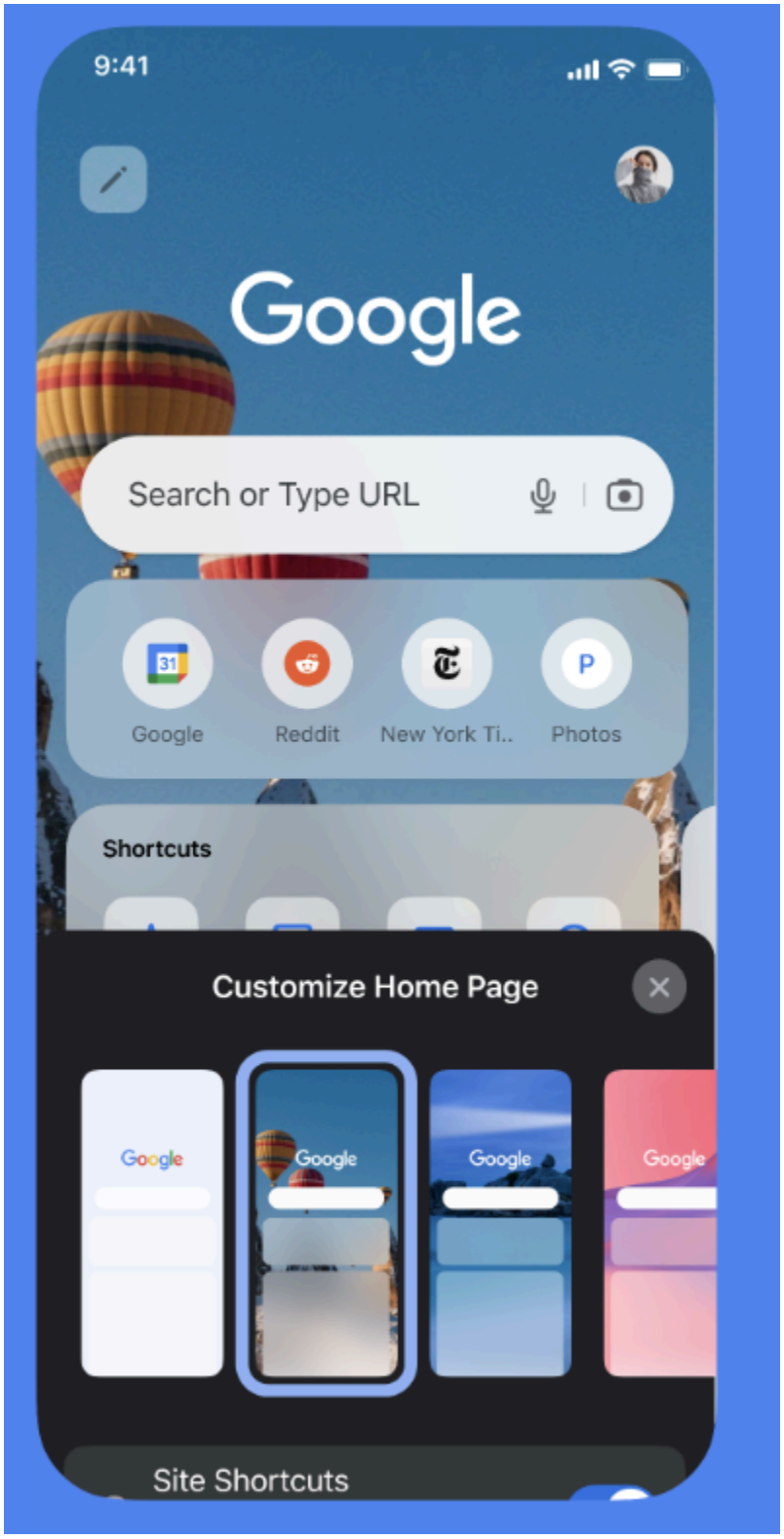


Chrome for iOS *New tab* page background customization

Chrome for iOS will now allow users to customize their New tab page (NTP) background. Admins will have the ability to set NTPCustomBackgroundEnabled to True or False, which will determine whether users will be able to customize their NTP background. The admin can set the BrowserThemeColor, which supports a hex code for specifying a color. If a hex value is specified, the user will not be able to override it.

The admin can also specify a recommended hex value, which the user can override. If fully enabled, the user can also select from the preselected gallery within Chrome, or from their phone's camera roll.

- **Chrome 142 on iOS** feature would roll out gradually



New policies in Chrome browser

Policy	Description
ScreenCaptureAllowedByOrigins	Allow Desktop, Window, and Tab capture by these origins
TabCaptureAllowedByOrigins	Allow Tab capture by these origins
GenAILocalFoundationalModelSettings	Settings for GenAI local foundational model
WindowCaptureAllowedByOrigins	Allow Window and Tab capture by these origins
SameOriginTabCaptureAllowedByOrigins	Allow Same Origin Tab capture by these origins
LocalNetworkAccessRestrictionsTemporaryOptOut	Specifies whether to (temporarily) opt out of Local Network Access restrictions
DevToolsGoogleDeveloperProgramProfileAvailability	Enable Google Developer Program Profiles in Chrome DevTools
ExtensionForceInstallWithNonMalwareViolationsEnabled	Enable Force-installed Extensions With Non-Malware Violations
ExtensionInstallCloudPolicyChecksEnabled	Enables additional cloud policy checks to allow/block installation of extensions

Current Chrome Enterprise Core updates

There are no Chrome Enterprise Core updates in this release.

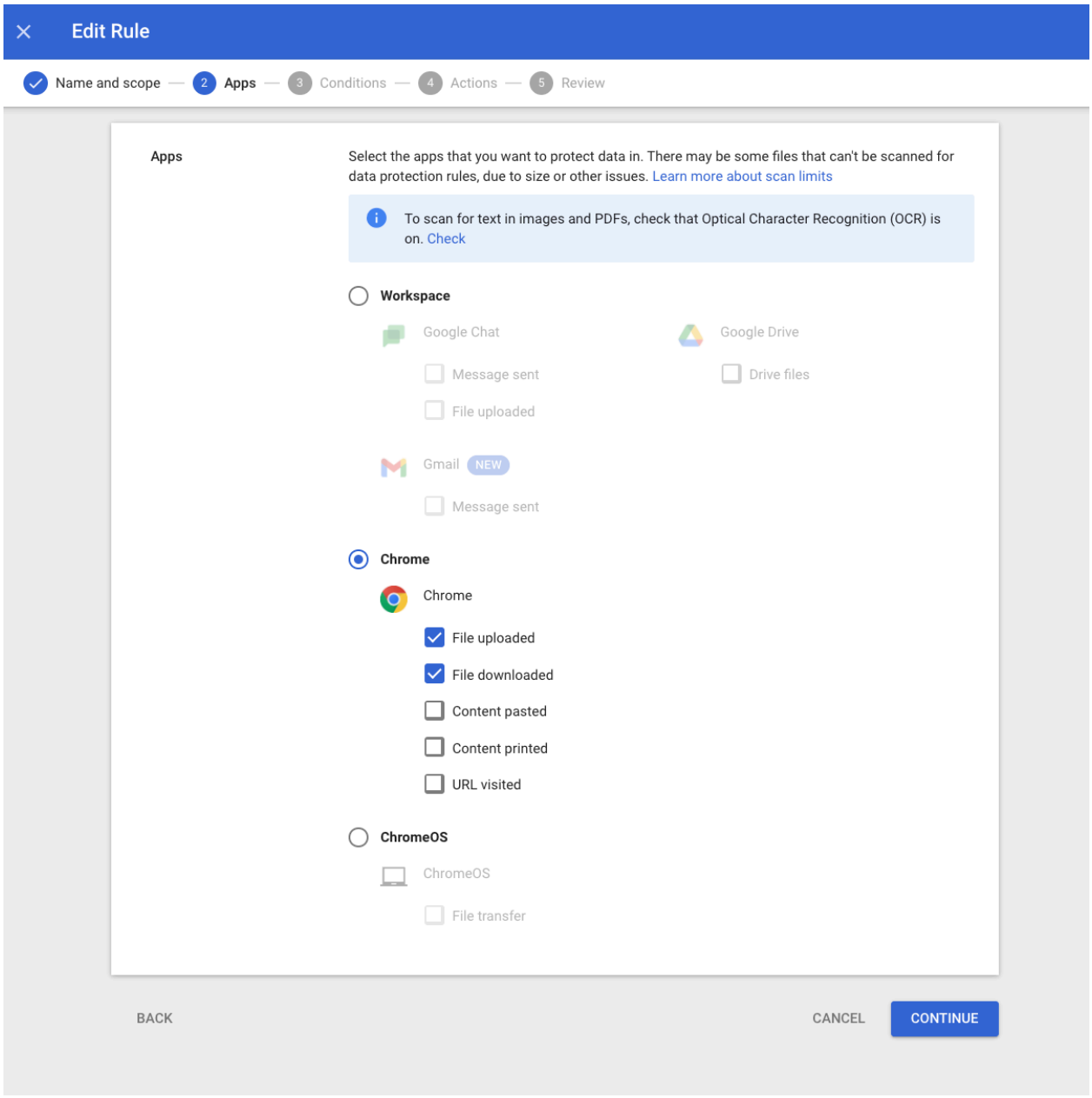
Current Chrome Enterprise Premium updates

Chrome browser rule UX refactor

To enhance the Data Loss Prevention (DLP) rule creation experience, the Google Admin console is being updated to streamline how administrators define policies for different applications like Chrome and Workspace. This introduces mutually exclusive application groups, meaning that a single DLP rule can now only target one application group at a time—either Workspace apps (like Drive, Gmail), Chrome browser triggers (like file upload, URL visited), or ChromeOS triggers. This change simplifies rule configuration, eliminates potential conflicts from overlapping app selections, and lays the groundwork for more specialized and user-friendly workflows tailored to each platform's needs.

Administrators will see an updated **Apps** selection interface using radio buttons to enforce this single-group selection for new rules. Existing rules that previously combined applications from multiple groups will be transparently migrated by the system into separate, compliant, single-platform rules to ensure continued protection and a seamless transition. Banners within the Admin console will provide information regarding these changes and the migration process. No new enterprise policies are introduced with this update; the changes are to the rule configuration interface. For more information, see What are ChromeOS data controls? - Chrome Enterprise and Education Help.

- **Chrome 142 on ChromeOS, Linux, macOS, Windows:** Enables mutually exclusive app selection for DLP rule configuration in Admin console



Streamlined Chrome Enterprise to Google SecOps integration

The new Chrome Enterprise Premium (CEP) and Google Security Operations (SecOps) integration provides a native, direct connection between the two systems. This feature transforms the browser into a primary security sensor, enabling organizations to prevent, detect, investigate, and respond to web-based threats (phishing, malware, and data exfiltration) by

sending a richer set of security events and detailed browser telemetry from Chrome directly to SecOps.
For administrators, the integration introduces enhanced security event types like URL navigation and suspicious URL visits, automatically enriched with Safe Browsing risk scores and threat intelligence. A new, streamlined *one-click* setup in the Admin Console replaces the previous manual workflow.
NOTE: The collection of high-volume events (for example, URL navigation) is opt-in. The feature requires no end-user-facing policy changes.

- **Chrome 142 on iOS, ChromeOS, Linux, MacOS, Windows**

Coming soon

Note: The items listed below are experimental or planned updates. They might change, be delayed, or canceled before launching.

Upcoming Chrome browser updates

Allowlist for Isolated Web App managed installation
Starting in Chrome 143, only Isolated Web Apps (IWAs) that are on a Google-managed allowlist can be installed or updated via administrator policies. This change affects all managed scenarios, including Managed User Sessions, Managed Guest Sessions, and Kiosk mode.

This allowlisting process is being implemented to enhance platform security and stability. It ensures that IWA developers adhere to Google's platform policies and establishes a verified contact with them. This direct contact is critical for addressing emergency cases, such as a security vulnerability or a major application defect, to better protect your organization.

For administrators, there are several key changes regarding the handling of Installed Web Apps (IWAs):

- **New Installations & Updates:** Any new installation or update of an IWA will now fail if its application ID is not included on Google's managed allowlist. The installation method itself remains unchanged.
- **Existing Installations:** IWAs that are already installed on user devices will continue to function. However, they will not receive any further updates until they are added to the allowlist.
- **Admin Console Notifications:** Administrators will be alerted when attempting to configure an installation policy for an IWA not on the allowlist. Additionally, the admin panel will highlight any installed non-allowlisted applications. In such instances, administrators should ensure that their IWA developer partners have completed Google's mandatory, one-time allowlisting procedure.

- **Chrome 143 on ChromeOS**

Deprecate and remove XSLT

XSLT v1.0, which all browsers adhere to, was standardized in 1999. In the meantime, XSLT has evolved to v2.0 and v3.0, adding features, and growing apart from the old version frozen into browsers. This lack of advancement, coupled with the rise of JavaScript libraries and frameworks that offer more flexible and powerful DOM manipulation, has led to a significant decline in the use of client-side XSLT. Its role within the web browser has been largely superseded by JavaScript-based technologies, such as JSON+React.

Chromium uses the libxslt library to process these transformations, and libxslt was unmaintained for ~6 months of 2025. Libxslt is a complex, aging C codebase of the type notoriously susceptible to memory safety vulnerabilities like buffer overflows, which can lead to arbitrary code execution. Because client-side XSLT is now a niche, rarely-used feature, these libraries receive far less maintenance and security scrutiny than core JavaScript engines, yet they represent a direct, potent attack surface for processing untrusted web content. Indeed,

XSLT is the source of several recent high-profile security exploits that continue to put browser users at risk.
For these reasons, Chromium (along with both other browser engines) plans to deprecate and remove XSLT from the web platform.

- **Chrome 143 on Android, ChromeOS, Linux, MacOS, Windows**: Deprecation (but not removal) of the APIs

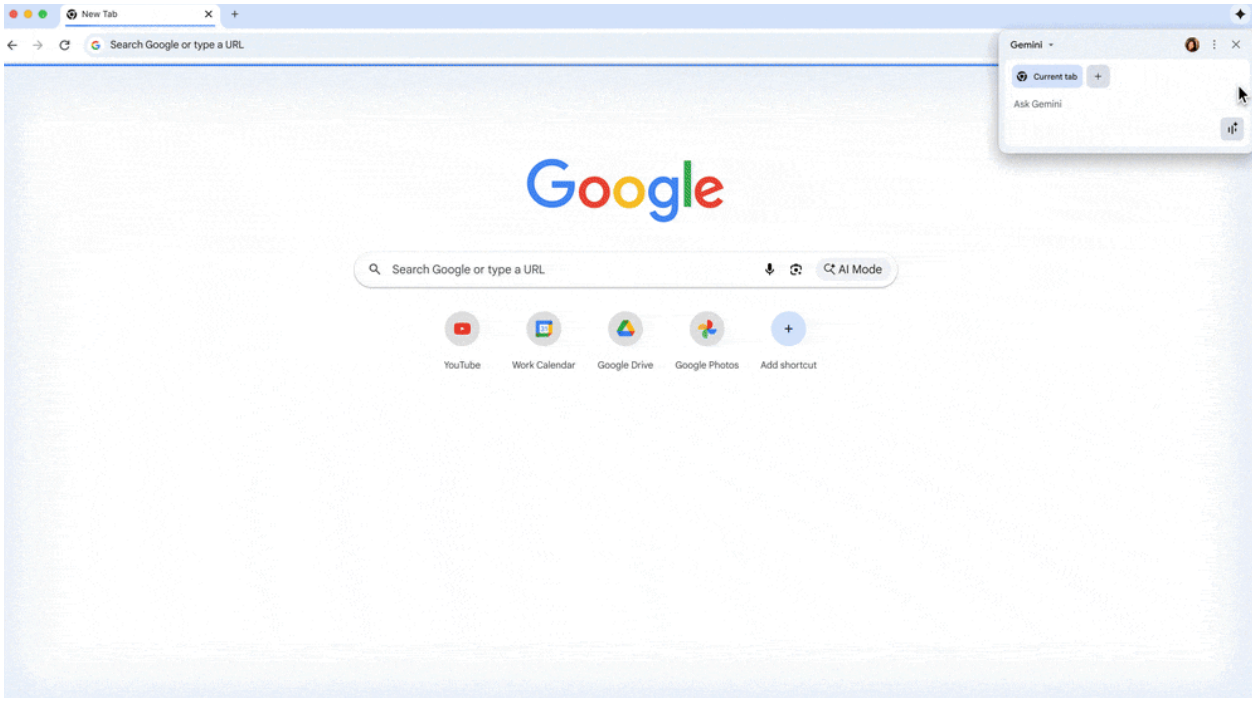
Gemini in Chrome

Gemini is now integrated into Chrome on macOS and Windows, and can understand the content of your current page. Users can now seamlessly get key takeaways, clarify concepts, and find answers, all without leaving their Chrome tab. This integration includes both chat—where users can interact with Gemini via text, and "Gemini Live", by which users can interact with Gemini via voice.

In Chrome 143, Gemini in Chrome will start the roll out to most Google Workspace users with access to the Gemini app in the US. Admins can turn off this feature (value 1) using the GeminiSettings policy or by using the GenAiDefaultSettings (value 2). For more details, see Gemini in Chrome in the Help Center or this blog post.

Also coming in Chrome 143 is the multi-tab context feature. Gemini in Chrome can now see more of your opened tabs (10 max) so you can ask questions across multiple pages to help you compare, find information more efficiently. Gemini in Chrome also serves as a productivity agent by enabling YouTube, Maps, Gmail, Drive, Keep, Calendar, and Tasks tools.

- Chrome 137 on MacOS, Windows: Feature is available for some Google AI Pro and Ultra subscribers in the US and on pre-Stable (Dev, Canary, Beta) channels in the US.
- **Earliest Chrome 143 on macOS, Windows:** Agentic capabilities in Gemini in Chrome available to some users (non-enterprise). Enterprise policy GeminiActOnWebSettings will be available at launch.
- Earliest Chrome 147 on macOS, Windows: Agentic capabilities in Gemini in Chrome available to enterprise users.



ICU 77 (supporting Unicode 16)

The Unicode support library ICU (International Components for Unicode) is upgraded from version 74.2 to 77.1, adding support for Unicode 16 and updating locale data. Two changes could pose some risk for web applications that assume a specific format from the Intl JS APIs:

1. The default Italian number formatting changed to omit the thousand separator for 4-digit numbers. For example `new Intl.NumberFormat("it").format(1234)` will return *1234* instead of *1.234*. The old behavior can be achieved with the useGrouping parameter for the `Intl.NumberFormat` constructor.
2. In some English locales (en-AU, en-GB, and en-IN), a comma was added after full-length weekdays, for example, changing Saturday 30 April 2011 to Saturday, 30 April 2011. Web applications should avoid relying on the precise formatting of dates and they may change again in future.

- **Chrome 143 on Windows, MacOS, Linux, Android**

Origin-Bound Cookies (by default)

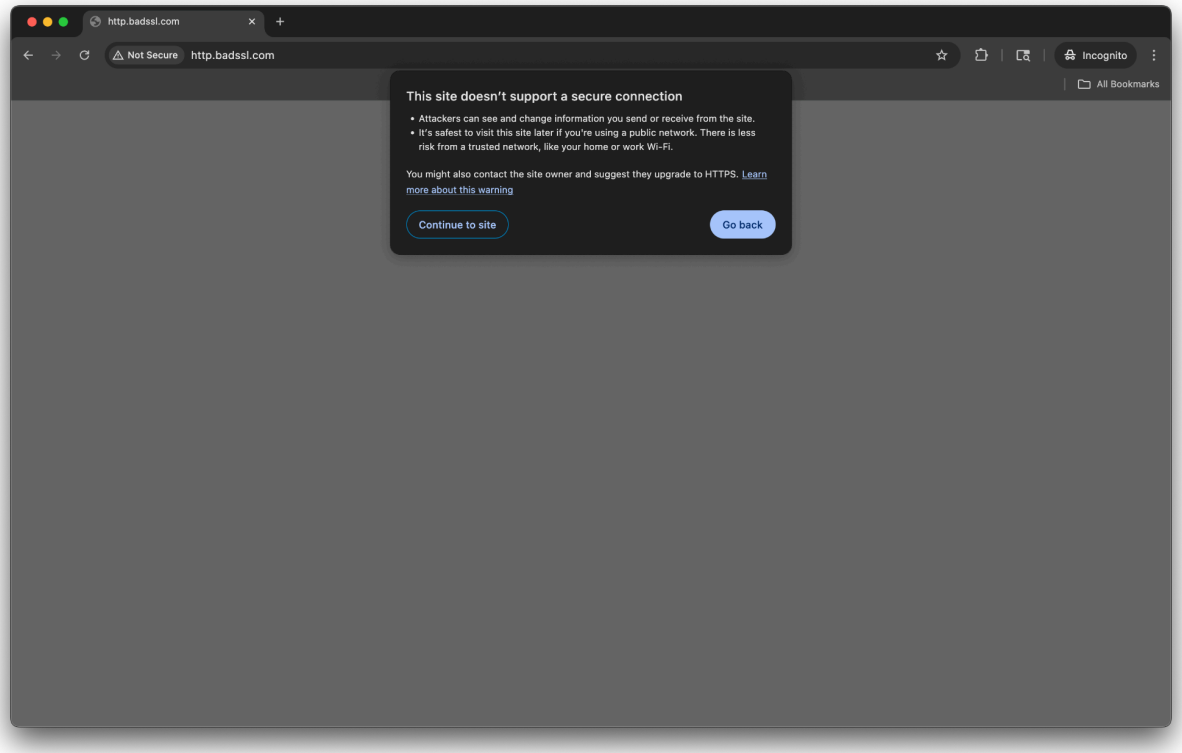
In Chrome 143, cookies are bound to their setting origin (by default) such that they're only accessible by that origin, that is, sent on a request or visible through `document.cookie`. Cookies might ease the host and port binding restrictions through use of the `Domain` attribute but all cookies will be bound to their setting scheme.
Temporary enterprise policies **LegacyCookieScopeEnabled** and **LegacyCookieScopeEnabledForDomainList** are available to revert this change. These policies will stop working in Chrome 150.

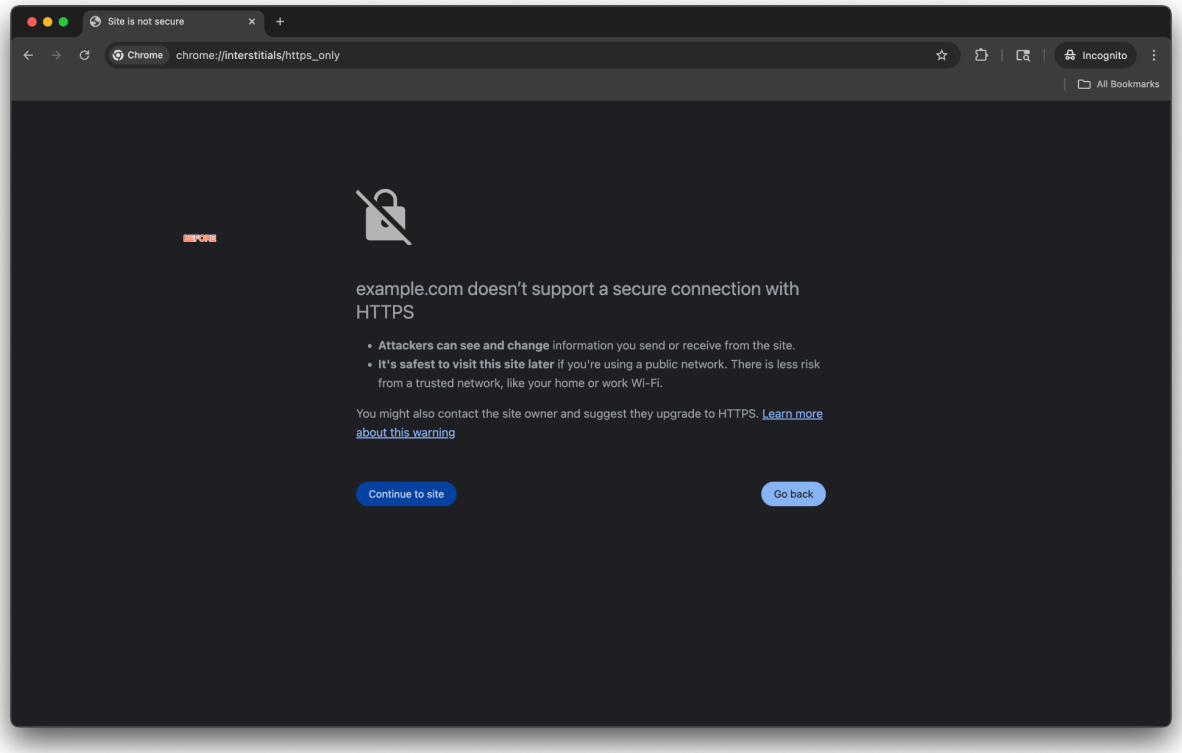
- **Chrome 143 on Android, iOS, Linux, macOS, Windows**: Enterprise policies will be available
- Chrome 150 on Android, iOS, Linux, macOS, Windows: Enterprise policies would be removed

Update to *No HTTPS* warning

Chrome 141 updated the warning displayed when a user opts in to the **Always use secure connections** on `chrome://settings/security` from an interstitial to a dialog. The URL content security indicator on the warning changes from an asterisk to a broken lock, while the full page load remains blocked and the functionality remains unchanged. Some users might see this warning automatically when visiting HTTP sites. Users can opt in to the warning on `chrome://settings/security`.

- Chrome 141 on ChromeOS, Linux, macOS, Windows: New warning design on desktop platforms
- **Chrome 143 on Android: New warning design on Android**


http.badssl.com
Not Secure
http.badssl.com
Incognito
All Bookmarks
This site doesn't support a secure connection
• Attackers can see and change information you send or receive from the site.
• It's safest to visit this site later if you're using a public network. There is less risk from a trusted network, like your home or work Wi-Fi.
You might also contact the site owner and suggest they upgrade to HTTPS. Learn more about this warning
Continue to site
Go back


Site is not secure
Chrome
chrome://interstitials/https_only
Incognito
All Bookmarks
BEFORE
example.com doesn't support a secure connection with HTTPS
• Attackers can see and change information you send or receive from the site.
• It's safest to visit this site later if you're using a public network. There is less risk from a trusted network, like your home or work Wi-Fi.
You might also contact the site owner and suggest they upgrade to HTTPS. Learn more about this warning
Continue to site
Go back

Bundled security settings

This feature provides users with bundled security options to configure security settings based on their desired level of protection while using Chrome. Users can choose between Enhanced for the highest level of security and Standard for the default balanced protection. Users can still set custom values for the settings, as they can today. This simplifies the user experience and makes it easier for users to get the level of protection they want without needing to understand advanced configuration options.
Existing enterprise policies take precedence over end-user bundle selections. If an existing policy is configured for security settings, the values will not be overridden by a user's choice of security bundle.

- **Chrome 144 on ChromeOS, Linux, macOS, Windows**

Deprecating savedTabGroups as individual value in SyncTypesListDisabled

Currently, the SyncTypesListDisabled enterprise policy allows administrators to disable the synchronization of `savedTabGroups` datatype on desktop platforms. On mobile platforms, however, Tab Groups synchronization is already managed by the tabs datatype. To align desktop behavior with mobile and simplify sync management, the individual `savedTabGroups` datatype will be deprecated and will no longer be an individually customizable value within the SyncTypesListDisabled policy

Action required by administrators:
Starting with Chrome 144, if your SyncTypesListDisabled policy disables either tabs or `savedTabGroups`, both data types will now be considered disabled. This means that disabling tabs will also disable saved tab groups, and vice-versa. The `savedTabGroups` value will be entirely removed from the list of supported datatypes for this policy. Administrators who have saved tab groups disabled and intend to keep this behavior must explicitly disable the tabs datatype. This will ensure the desired behavior before the savedTabGroups value is fully removed.

- **Chrome 144 on Windows, macOS, Linux**

HSTS tracking prevention

This update will mitigate user tracking by third-parties via the HTTP Strict Transport Security (HSTS) cache. This feature only allows HSTS upgrades for top-level navigations and blocks HSTS upgrades for sub-resource requests. Doing so makes it infeasible for third-party sites to use the HSTS cache to track users across the web.

- **Chrome 144 on Windows, macOS, Linux, Android**

Happy Eyeballs V3

This launch is an internal optimization in Chrome that implements Happy Eyeballs V3 to achieve better network connection concurrency. Happy Eyeballs V3 performs DNS resolutions asynchronously and staggers connection attempts with preferable protocols (H3/H2/H1) and address families (IPv6 or IPv4) to reduce user-visible network connection delay. This feature is gated by a temporary policy HappyEyeballsV3Enabled.

- **Chrome 144 on Android, ChromeOS, Linux, macOS, Windows**

Multicast Support for Direct Sockets API

Allows Isolated Web Apps to subscribe to multicast groups and receive UDP packets from there, and to specify additional parameters when sending UDP packets to multicasts addresses.

- **Chrome 144 on Windows, MacOS, Linux**

ServiceWorkerAutoPreload mode

ServiceWorkerAutoPreload is a mode where the browser issues the network request in parallel with the service worker bootstrap, and consumes the network request result inside the fetch handler if the fetch handler returns the response with respondWith(). If the fetch handler result is fallback, it passes the network response directly to the browser. *ServiceWorkerAutoPreload* is defined as an optional browser optimization, which will change the existing service worker behavior. Admins can control this feature using an enterprise policy called ServiceWorkerAutoPreloadEnabled.

- Chrome 140 on Android, Windows: ServiceWorkerAutoPreloadEnabled policy
- **Chrome 144 on Android, Windows:** ServiceWorkerAutoPreloadEnabled policy will be removed

2SV enforcement for admins

To better protect your organization's information, Google will soon require all accounts with access to `admin.google.com` to have 2-Step Verification (2SV) enabled. As a Google Workspace administrator, you need to confirm your identity with 2SV, which requires your password plus something additional, such as your phone or a security key.

The enforcement will be rolled out gradually over the coming months. You should enable 2SV for the admin accounts in your organization before Google enforces it. For more information, see this About 2SV enforcement for admins.

- Chrome 137 on ChromeOS, Linux, macOS, Windows: 2SV enforcement starts
- **Chrome 145 on ChromeOS, Linux, macOS, Windows: 2SV mandatory**

CSS find-in-page highlight pseudos

This feature will expose **find-in-page** search result styling to authors as a highlight pseudo-element, like selection and spelling errors. This allows authors to change the foreground

and background colors or add text decorations, which can be especially useful if the browser defaults have insufficient contrast with the page colors or are otherwise unsuitable.

- **Chrome 145 on Windows, macOS, Linux, Android**

Change in launch schedule starting in Chrome *Early Stable* 145

Starting in Chrome 145, Chrome will be rolled out to the Early Stable channel one week earlier than previously communicated. For example, the Chrome 145 Early Stable release moves from February 4, 2026 to January 28, 2026. There are no changes to the Stable channel release. For reference, you can check the updated Release Schedule.

- **Chrome 145 on Android, iOS, MacOS, Windows:** Chrome will be rolled out to the Early Stable channel one week earlier.

Clear window name for cross-site navigations that switches browsing context group

The value of the `window.name` property is currently preserved throughout the lifetime of a tab, even with navigation that switches browsing context groups, which can leak information and potentially be used as a tracking vector. As early as Chrome 142, the `window.name` property will no longer be preserved in this case, which will mitigate this issue.

This update will introduce a new temporary enterprise policy, **ClearWindowNameCrossSiteBrowsing**, which will stop working in Chrome 146.

- **Chrome 145 on Windows, macOS, Linux, Android, iOS:** Enterprise policy would be available
- Chrome 148 on Windows, macOS, Linux, Android, iOS: Enterprise policy would be removed

Disallow spaces in non-file:// URL hosts

According to the URL Standard specification, URL hosts cannot contain the space character, but currently URL parsing in Chromium allows spaces in the host. This causes Chromium to fail several tests included in the Interop2024 HTTPS URLs for WebSocket and URL focus areas. To bring Chromium into spec compliance, we would like to remove spaces from URL hosts altogether, but a difficulty with this is that they are used in the host part in Windows `file://` URLs (Github).

- **Chrome 145 on Android, ChromeOS, LaCrOS, Linux, macOS, Windows, Fuchsia**

Remove third-party storage partitioning policies

Third-party storage partitioning became the default in Chrome 115. The `chrome://` flag that allowed users to disable this feature was removed in Chrome 128, and the deprecation trial ended with Chrome 139.
In Chrome 145, the enterprise policies DefaultThirdPartyStoragePartitioningSetting and ThirdPartyStoragePartitioningBlockedForOrigins will be removed. Users are advised to transition to alternative storage solutions, either by adapting to third-party storage partitioning or by using document.requestStorageAccess({...}) where needed.
If you have any feedback, you can add it here in the Chromium bug.

- **Chrome 145 on Android, ChromeOS, Linux, macOS, Windows, Fuchsia:** Removal of DefaultThirdPartyStoragePartitioningSetting and ThirdPartyStoragePartitioningBlockedForOrigins

X25519Kyber768 key encapsulation for TLS

Chrome 124 enabled by default on all desktop platforms a new post-quantum secure TLS key encapsulation mechanism X25519Kyber768, based on a NIST standard (ML-KEM). This protects network traffic from Chrome with servers that also support ML-KEM from decryption by a future quantum computer. This change should be transparent to server operators. This cipher will be used for both TLS 1.3 and QUIC connections.

However, some TLS middleboxes might be unprepared for the size of a Kyber (ML-KEM) key encapsulation, or a new TLS ClientHello cipher code point, leading to dropped or hanging connections. This can be resolved by updating your middlebox, or disabling the key encapsulation mechanism via the temporary PostQuantumKeyAgreementEnabled enterprise policy, which will be available through the end of 2024. However, long term, post-quantum secure ciphers will be required in TLS and the enterprise policy will be removed. Post-quantum cryptography is required for CSNA 2.0. To learn more, see Protect Chrome Traffic with Hybrid Kyber KEM.

- Chrome 131 on Linux, macOS, Windows: Chrome will switch the key encapsulation mechanism to the final standard version of ML-KEM
- **Chrome 145 on Linux, macOS, Windows:** Enterprise policy will be removed

Isolated Web Apps

Isolated Web Apps (IWAs) are an extension of existing work on PWA installation and Web Packaging that provide stronger protections against server compromise and other tampering that is necessary for developers of security-sensitive applications. Rather than being hosted on live web servers and fetched over HTTPS, these applications are packaged into Web Bundles, signed by their developer, and distributed to end-users through one or more of the potential methods described in the explainer.
In the initial release, IWAs will only be installable through an admin policy on enterprise-managed ChromeOS devices.

- **Chrome 150 on Windows** This rollout adds support for Isolated Web Apps in enterprise-managed browser configurations on Windows.

UI Automation accessibility framework provider on Windows

Starting in Chrome 126, Chrome will start directly supporting accessibility client software that uses Microsoft Windows's UI Automation accessibility framework. Prior to this change, such software interoperated with Chrome by way of a compatibility shim in Microsoft Windows. This change is being made to improve the accessible user experience for many users. It provides

complete support for Narrator, Magnifier, and Voice Access; and will improve third-party apps that use Windows's UI Automation accessibility framework. Users of Chrome will find reduced memory usage and processing overhead when used with accessibility tools. It will also ease development of software using assistive technologies.
Administrators may use the UiAutomationProviderEnabled enterprise policy starting in Chrome 125 to either force-enable the new provider (so that all users receive the new functionality), or disable the new provider. This policy will be supported through Chrome 146, and will be removed in Chrome 147. This one-year period is intended to give enterprises sufficient time to work with third-party vendors so that they may fix any incompatibilities resulting from the switch from Microsoft's compatibility shim to Chrome's UI Automation provider.

- Chrome 125 on Windows: The UiAutomationProviderEnabled policy is introduced so that administrators can enable Chrome's UI Automation accessibility framework provider and validate that third-party accessibility tools continue to work.
- Chrome 126 on Windows: The Chrome variations framework will be used to begin enabling Chrome's UI Automation accessibility framework provider for users. It will be progressively enabled to the full stable population, with pauses as needed to address compatibility issues that can be resolved in Chrome. Enterprise administrators may continue to use the UiAutomationProviderEnabled policy to either opt-in early to the new behavior, or to temporarily opt-out through Chrome 146.
- **Chrome 147 on Windows:** The UiAutomationProviderEnabled policy will be removed from Chrome. All clients will use the browser's UI Automation accessibility framework provider.

SafeBrowsing API v4 to v5 migration

Chrome calls into the SafeBrowsing v4 API will be migrated to call into the v5 API instead. The method names are also different between v4 and v5. If admins have any v4-specific URL allowlisting to allow network requests to https://safebrowsing.googleapis.com/v4*, these should be modified to allow network requests to the whole domain instead: safebrowsing.googleapis.com. Otherwise, rejected network requests to the v5 API will cause security regressions for users. For more details, see Migration From V4 - Safe Browsing.

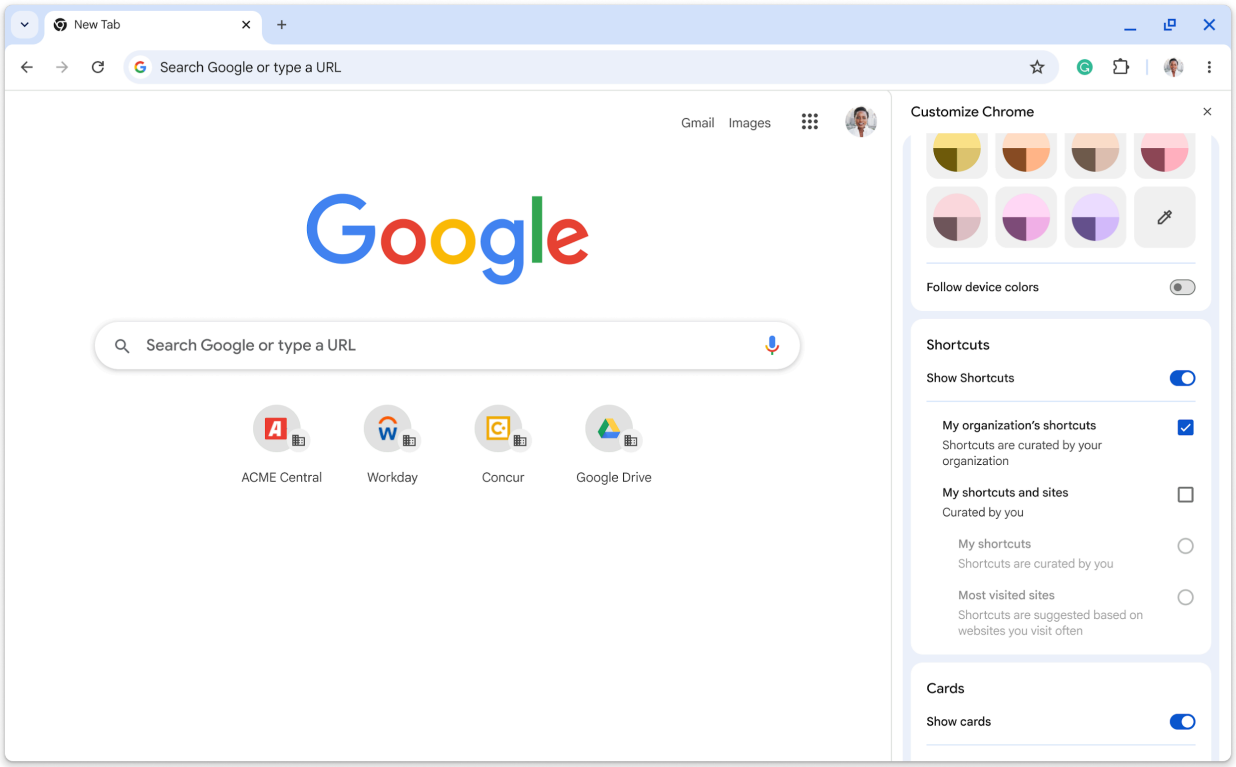
- **Chrome 145 on Android, iOS, ChromeOS, Linux, macOS, Windows:** Feature would gradually roll-out

Upcoming Chrome Enterprise Core updates

Enterprise-managed shortcuts on the New tab page

Shortcuts on the **New tab** page can provide quick access to internal resources and applications. Admins can set up to 10 shortcuts on the user's **New tab** page using the NTPShortcuts policy. As early as Chrome 141, this feature will be available to Chrome Enterprise Core Trusted Testers.

- Chrome 141 on ChromeOS, Linux, macOS, Windows: Early preview of policy is available for Trusted Testers. Admins can set up to 10 shortcuts and users can switch to My organizations shortcuts by navigating to **Customize Chrome**.
- **Chrome 143 on ChromeOS, Linux, macOS, Windows:** Policy will be generally available. Shortcuts set by admins will be shown in addition to user-set shortcuts (My shortcuts or Most visited sites). Users can control visibility of shortcuts by navigating to the **Customize Chrome** panel.



Profile reporting for Chrome on iOS

Chrome Enterprise Core is launching cloud profile reporting for Chrome on iOS. To turn on profile reporting on iOS, IT administrators will need to enable the Managed profile reporting policy in the **Chrome browser > Settings** section of the Google Admin console. If you have already turned on Managed profile reporting, you will automatically receive profile reporting on Chrome on iOS. Admins can control this feature using the CloudProfileReportingEnabled policy.

The profile reporting data can be found on the **Google Admin console > Chrome browser > Managed profiles**. The reporting information includes profile information, browser information (browser versions, OS, channel, and so on), the policies that are applied, and more.

- **Chrome 143 on iOS**: Feature would roll out gradually

Upcoming Chrome Enterprise Premium updates

Increased file size support for DLP scans

Chrome Enterprise Premium now extends its Data Loss Prevention (DLP) and malware scanning capabilities to include large and encrypted files. Previously, files larger than 50 MB and all encrypted files were skipped during content scanning. This update closes that critical security gap. For policies configured to save evidence, files **up to 2GB** can now be sent to the Evidence Locker. This provides administrators with greater visibility and control, significantly reducing the risk of data exfiltration through large file transfers.

No new policy is required to enable this feature. It is automatically controlled by the existing DLP rule configurations in the Google Admin console. If admins have rules that apply to file uploads, downloads, or printing, they will now also apply to large and encrypted files. For more information, see What are ChromeOS data controls? - Chrome Enterprise and Education Help.

- **Chrome 145 on Linux, macOS, Windows:** This stage enables the collection of large (>50 MB) and encrypted files for the Evidence Locker, closing a key DLP security gap.

Additional resources

- For emails about future releases, sign up here.
- To try out new features before they're released, sign up for the trusted tester program.
- Connect with other Chrome Enterprise IT admins through the Chrome Enterprise Customer Forum.
- How Chrome releases work—Chrome Release Cycle
- Chrome Browser downloads and Chrome Enterprise product overviews—Chrome Browser for enterprise
- Chrome version status and timelines—Chrome Platform Status | Google Update Server Viewer
- Announcements: Chrome Releases Blog | Chromium Blog
- Developers: Learn about changes to the web platform.

Still need help?

- Google Workspace, Cloud Identity customers (authorized access only)—Contact support
- Chrome Browser Enterprise Support—Sign up to contact a specialist
- Chrome Administrators Forum
- Chrome Enterprise Help Center