![chrome enterprise]

Chrome 141 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 September 24, 2025, updated October 17, 2025.

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

Chrome 141 release summary

Current Chrome browser updates	Security / Privacy	User productivity / Apps	Management
New search hijacking heuristic signal in extension telemetry	✓		
Gemini in Chrome		✓	
New tab page footer	✓	✓	✓
Remote commands for 3P-authenticated profiles			✓
Origin-keyed Process Isolation	✓		
Strict Same Origin policy for Storage Access API	✓		
New policies in Chrome browser			✓
Chrome Enterprise Core updates	**Security / Privacy**	**User productivity / Apps**	**Management**
Enrolled browsers support for the enterprise Chrome Web Store customizations		✓	✓
Enterprise-managed shortcuts on the New tab page		✓	✓
Inactive profile deletion in Chrome Enterprise Core	✓		✓
Chrome Enterprise Premium updates	**Security / Privacy**	**User productivity / Apps**	**Management**
Watermarking customization	✓		✓

Upcoming Chrome browser updates	Security / Privacy	User productivity / Apps	Management
Local network access restrictions	✓		
Chrome on iOS multi-profile support in the Share extension		✓	
A simplified sign-in and sync experience on Chrome Desktop	✓	✓	
Bundled security settings	✓		
Clear window name for cross-site navigations that switches browsing context group			✓
Client's LLM assistance in mitigating scams	✓		
HSTS tracking prevention	✓		
Interoperable pointerrawupdate events exposed only in secure contexts	✓		
Origin-bound cookies (by default)			✓
PostQuantum Cryptography for DTLS in WebRTC	✓		
Sticky user activation across same-origin navigations			✓
Update to No HTTPS warning design	✓		
Web App manifest: update eligibility algorithm	✓		
CSS find-in-page highlight pseudos			✓
Deprecating savedTabGroups as individual value in SyncTypesListDisabled			✓
Happy Eyeballs V3	✓		✓
ServiceWorkerAutoPreload			✓

	Security / Privacy	User productivity / Apps	Management
Change in *Early Stable* launch schedule			✓
2SV enforcement for admins			✓
Disallow spaces in non-file:// URL hosts	✓		
Remove third-party storage partitioning policies	✓		
SafeBrowsing API v4 to v5 migration	✓		
X25519Kyber768 key encapsulation for TLS	✓		
Isolated Web Apps			✓
UI Automation accessibility framework provider on Windows		✓	
Upcoming Chrome Enterprise Core updates	**Security / Privacy**	**User productivity / Apps**	**Management**
Profile reporting for Chrome on iOS			✓
Upcoming Chrome Enterprise Premium updates	**Security / Privacy**	**User productivity / Apps**	**Management**
Chrome browser rule UX refactor	✓		✓
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

New search hijacking heuristic signal in extension telemetry

Malicious Chrome extensions intercept and redirect Omnibox and Realbox (the search box in the **New tab** page) search queries from the Search Engine Results Page (SERP) to an attacker-controlled URL. This feature adds a client-side heuristic to detect such search hijacking. The core idea is to compare user-initiated searches with successful SERP landings; a significant discrepancy over time strongly indicates hijacking activity. This heuristic generates a new signal, uploaded to the Safe Browsing CRX telemetry server via the existing Extension Telemetry service in Chrome. Server-side analysis of signal data from multiple Chrome browsers can then identify potential search hijacking.

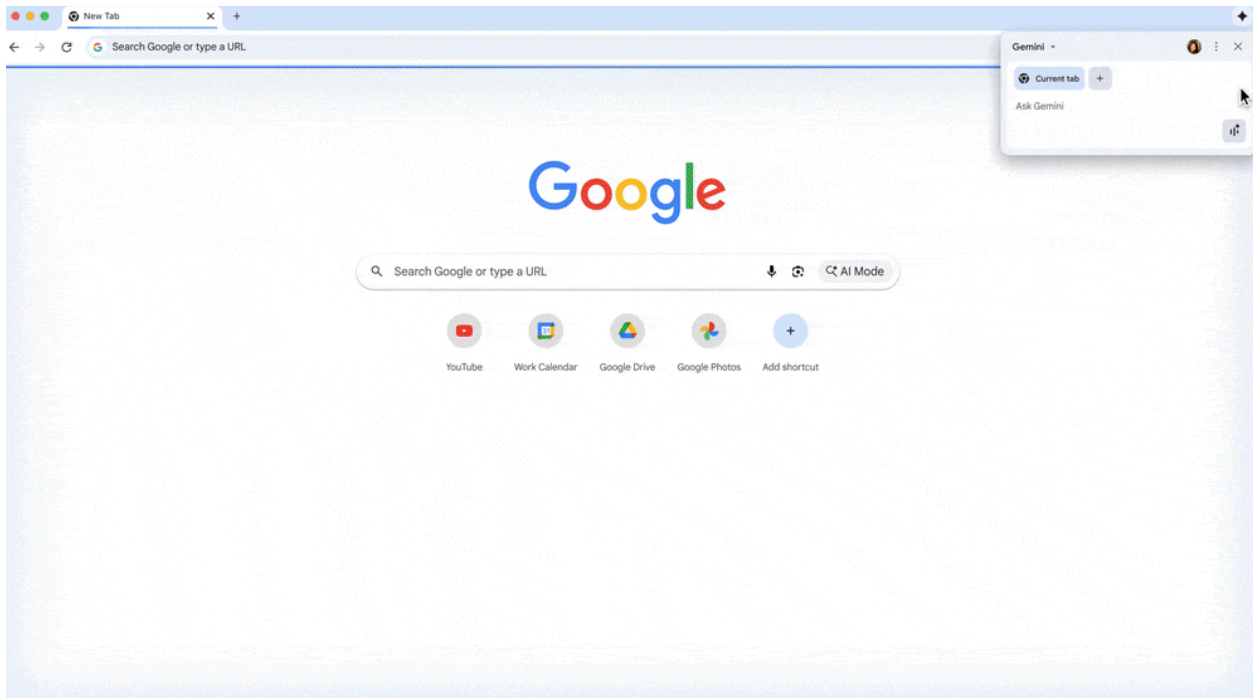- **Chrome 141 on ChromeOS, Linux, macOS, Windows**

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 141, [Gemini in Chrome](#) starts rolling 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](#).

- 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.
- **Chrome 141 on iOS, macOS, Windows**: Feature gradually rolls out on Stable for users for most all Google Workspace users with access to the Gemini app in the US

- **Chrome 143 on macOS, Windows**: Introducing agentic capabilities to Gemini in Chrome. Enterprise policies will be available at launch


New tab page footer

An update to the **New tab** page includes a new footer designed to provide users with greater transparency and control over their Chrome experience.

- Chrome 138 on ChromeOS, Linux, macOS, Windows: Extension Attribution will begin to show on the NTP. If an extension has changed your default **New tab** page, you'll now see a message in the footer that attributes the change to that specific extension. This message often includes a link directly to the extension in the Chrome Web Store, making it easier to identify and manage unwanted extensions. If you're an administrator, you can disable this attribution using the NTPFooterExtensionAttributionEnabled policy.

- Chrome 139 on Linux, macOS, Windows: Browser management disclosure will be shown if one of the policies to customize the footer is set by an enterprise admin. For users whose Chrome browser is managed by a trusted source, the **New tab** page footer will

now display a management disclosure notice. This helps you understand how your browser is being managed. Administrators can disable this notice with the [NTPFooterManagementNoticeEnabled](#) policy. Additionally, organizations can customize the footer's appearance using the [EnterpriseLogoUrlForBrowser](#) and [EnterpriseCustomLabelForBrowser](#) policies to display a custom logo and label.

- **Chrome 141 on Linux, macOS, Windows:** A default notice (*Managed by <domain name>*) will display in the **New tab** page footer for all managed browsers. Visibility can be controlled with the [NTPFooterManagementNoticeEnabled](#) policy.
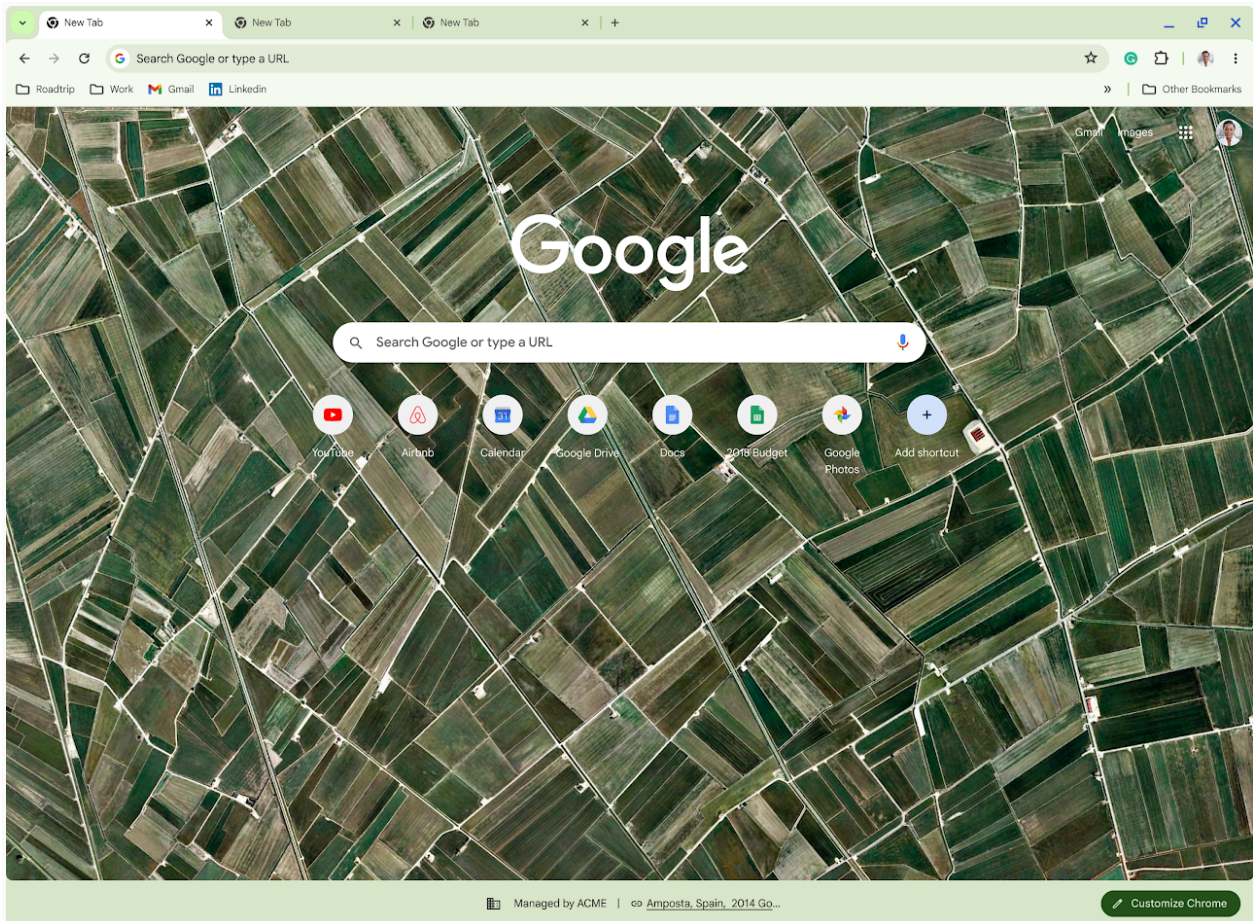
Remote commands for 3P-authenticated profiles

This feature introduces remote administrative commands, such as clearing cache and cookies, for Chrome profiles authenticated via third-party identity providers. This enhancement extends management capabilities to these newly-supported profiles, allowing administrators to remotely manage a broader range of user accounts.

- **Chrome 141 on Linux, macOS, Windows:** We now support remote commands for 3P-authenticated profiles

Local network access restrictions

Chrome 141 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. Enterprises that need to disable or auto-grant the permission can do so using the [LocalNetworkAccessAllowedForUrls]() and [LocalNetworkAccessBlockedForUrls]() policies. The value of '*' can be used to allow local network access on all URLs, matching the behavior prior to rolling out the restrictions.

- **Chrome 141 on Windows, macOS, Linux, Android**

Origin-keyed process isolation

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, `a.example.com` and `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. 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.

Administrators can control this feature using the [OriginKeyedProcessesEnabled](#) policy.

- **Chrome 141 on Windows, macOS, Linux:** Feature will roll out gradually

Strict Same Origin policy for Storage Access API

In Chrome 141, [Storage Access API](#) semantics now strictly follow the [Same Origin policy](#), to enhance security. Using `document.requestStorageAccess()` in a frame only attaches cookies to requests to the iframe's origin (not site) by default. The [CookiesAllowedForUrls](#) policy or Storage Access Headers can still be used to unblock cross-site cookies.

- **Chrome 141 on Windows, macOS, Linux, Android**

New policies in Chrome browser

Policy	Description
[NTPShortcuts](#)	Configure a list of shortcuts on the **New tab** page
[GloballyScopeHTTPAuthCacheEnabled](#)	Configure whether the HTTP authentication cache is scoped to a top-level site or a browser tab

Current Chrome Enterprise Core updates

Enrolled browsers support for the Enterprise Chrome Web Store customizations

The Customized Chrome Web Store now supports managed browsers enrolled in [Chrome Enterprise Core](#) (Cloud machine settings). This allows admins to [customize the Chrome Web Store](#) without the need for users to sign in. The customizations include:

- Add company logos
- Add hero banners and custom announcements
- Curate extension collections
- Hide extension categories

The [Chrome Web Store customization](#) settings were previously launched in Chrome 132 but only supported user-level policies (for signed-in users). As early as Chrome 140, this feature will be available to Chrome Enterprise Core Truster Testers.

- **Chrome 141 on Linux, macOS, Windows**: As early as Chrome 141, this feature will launch to General Availability (GA).

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 Truster 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.
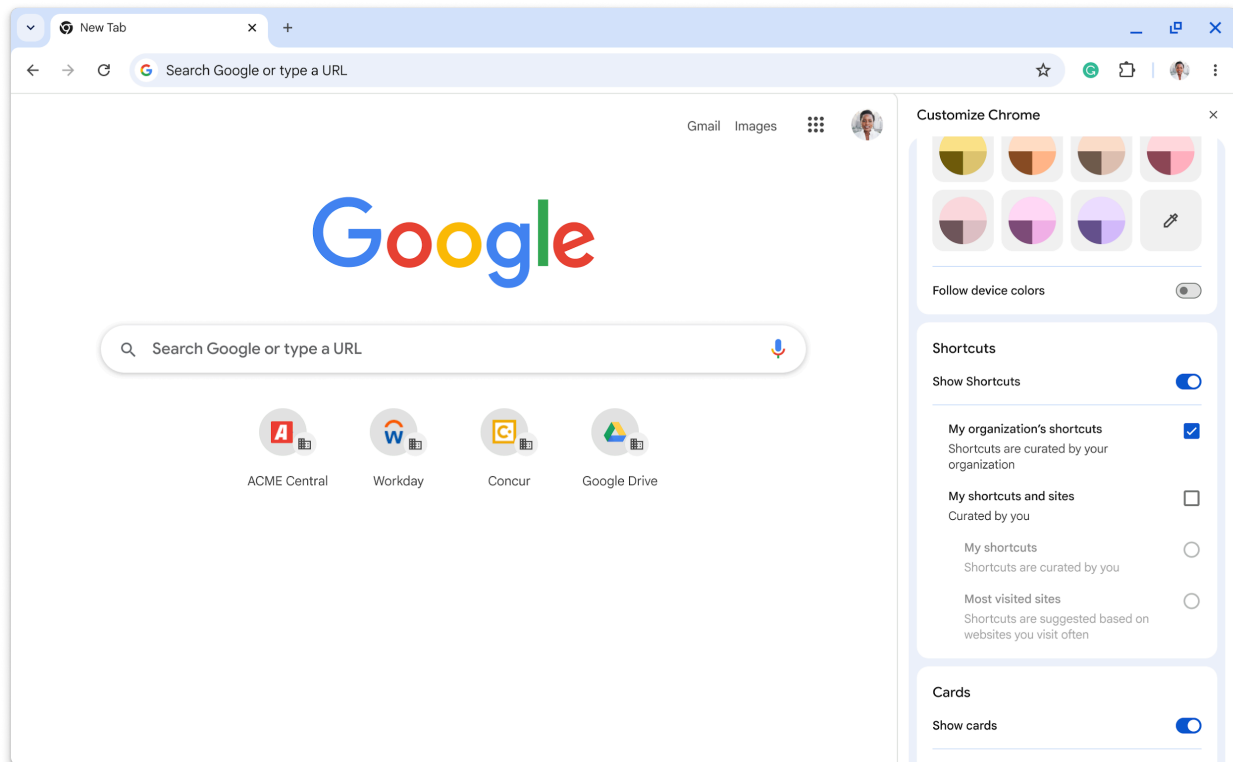
Inactive profile deletion in Chrome Enterprise Core

In June 2025, the inactive period for profile deletion setting started to roll out. In September 2025, the setting begins to automatically delete managed profiles in the Admin console that have been inactive for more than the defined inactivity period. When releasing the setting, the inactivity period of time has a **default value of 90 days**. Meaning that by default, all managed profiles that have been inactive for more than 90 days are deleted from your account. Administrators can change the inactive period value [using this setting](#):

- Maximum value is 730 days
- Minimum value is 28 days

If the set value is lowered, it might have a global impact on any currently managed profiles. All impacted profiles will be considered inactive and, therefore, be deleted. This does not delete the

user account. If an inactive profile is reactivated on a device, that profile will reappear in the console.

- **Chrome 141 on Android, ChromeOS, Linux, macOS, Windows:** Policy was rolled out in June. Deletion will start in September and the initial wave of deletion will complete by the end of October. After the initial deletion rollout, inactive profiles will continue to be deleted once they have reached their inactivity period.

Current Chrome Enterprise Premium updates

Watermarking customization

Chrome Enterprise Premium now allows administrators to customize the appearance of watermarks. This enhancement is motivated by the need to improve user experience, addressing concerns such as eyestrain and readability on pages with existing watermarks.

To control the watermark's appearance, administrators can use the new [WatermarkStyle](#) policy. Within this policy, admins can configure the following:

- `font_size`: Sets the font size of the text in pixels.
- `fill_opacity`: Sets the fill opacity of the text, from 0 (transparent) to 100 (opaque).
- `outline_opacity`: Sets the outline opacity of the text, from 0 (transparent) to 100 (opaque).

This provides administrators with greater flexibility to balance security requirements with user productivity.

- **Chrome 141 on ChromeOS, Linux, macOS, Windows:** This launch enables administrators to customize watermark font size and opacity using the new [WatermarkStyle](#) policy in the Google Admin console.

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

Local network access restrictions

Chrome 142 will restrict 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. Enterprises that need to disable or auto-grant the permission can do so using the [LocalNetworkAccessAllowedForUrls]() and [LocalNetworkAccessBlockedForUrls]() policies. The value of '*' can be used to allow local network access on all URLs, matching the behavior prior to rolling out the restrictions.

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

Chrome on iOS multi-profile support in Share extension

As early as Chrome 142 on iOS, Chrome Share extension now 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**
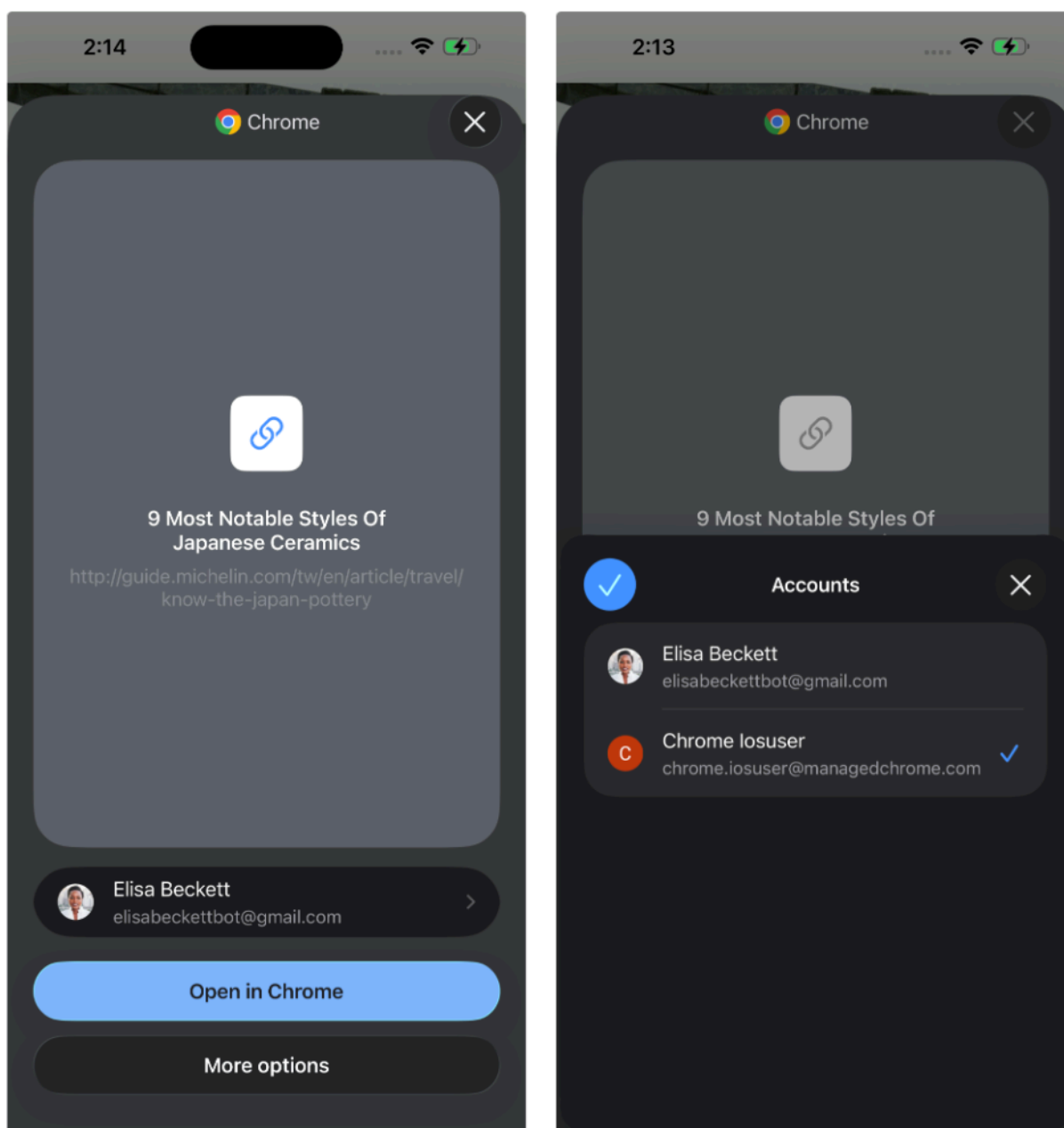
A simplified sign-in and sync experience on Chrome Desktop

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

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 142 on ChromeOS, Linux, macOS, Windows**

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 142 on Windows, macOS, Linux, Android, iOS:** Enterprise policy would be available
- Chrome 146 on Windows, macOS, Linux, Android, iOS: Enterprise policy would be removed

Client's LLM assistance in mitigating scams

Users on the webs are facing significant amounts of several kinds of scams a day. To combat these scams, Chrome will leverage on-device LLM to identify scam websites for Enhanced Safe Browsing (ESB) users. Chrome will send 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**

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 142 on Windows, macOS, Linux, Android**

Interoperable pointerrawupdate events exposed only in secure contexts

The PointerEvents spec restricted `pointerrawupdate` to secure contexts in 2020, hiding both the event firing and the global event listeners from insecure contexts. Through this feature, Chrome will match the updated spec and become interoperable with other major browsers.

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

Origin-Bound Cookies (by default)

In Chrome 142, 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 142 on Android, iOS, Linux, macOS, Windows**: Enterprise policies will be available
- Chrome 150 on Android, iOS, Linux, macOS, Windows: Enterprise policies would be removed

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 **WebRtcPostQuantumKeyAgreementEnabled**, 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

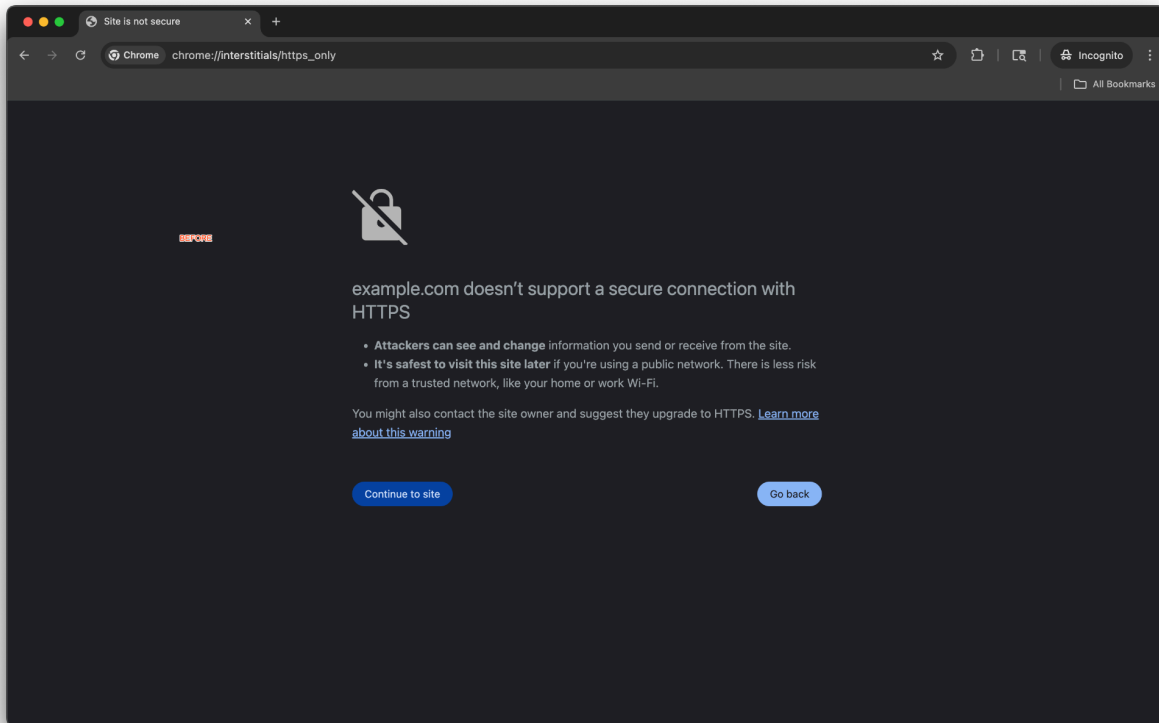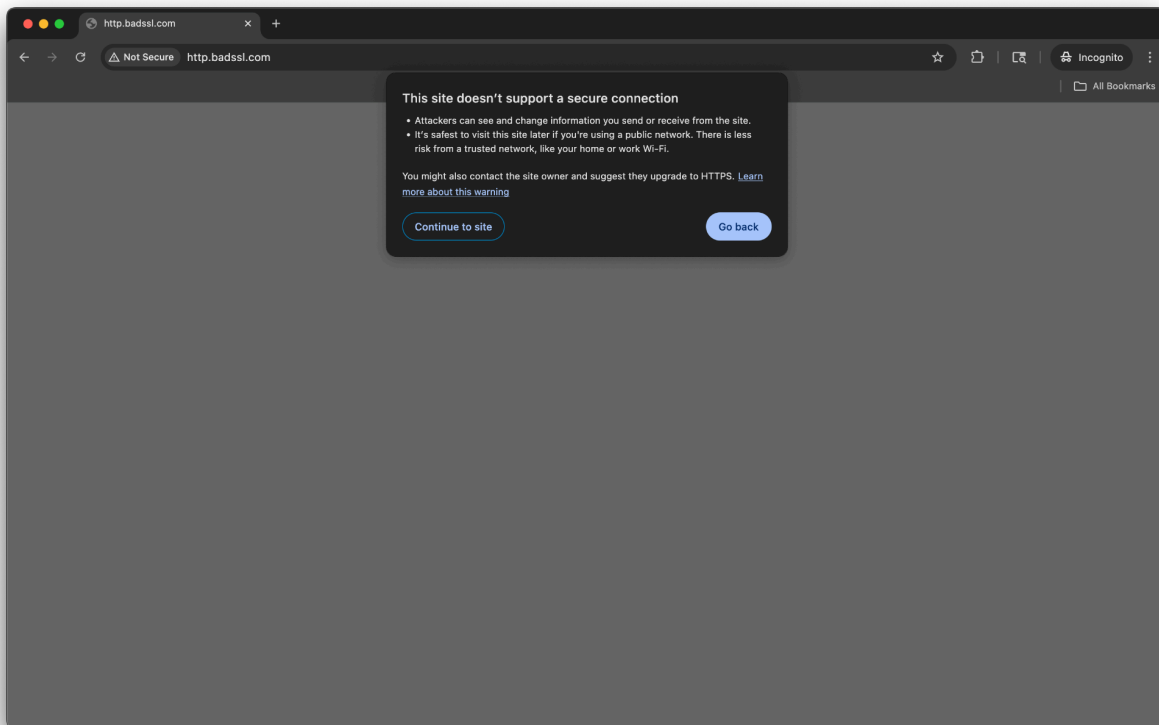**Sticky user activation across same-origin navigations**

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**

Update to *No HTTPS* warning

Chrome 140 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 140 on ChromeOS, Linux, macOS, Windows: New warning design on desktop platforms
- **Chrome 142 on Android: New warning design on Android**

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

---

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

Web App manifest: update eligibility algorithm

As early as Chrome 142, the Web App manifest will specify an update eligibility algorithm. This makes the update process more deterministic and predictable, giving the developer more control over whether (and when) updates should apply to existing installations, and allowing removal of the *update check throttle* that user agents currently need to implement to avoid wasting network resources.

- **Chrome 142 on Windows, macOS, Linux**
- Chrome 143 on Android

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 143 on Windows, macOS, Linux, Android**

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 143, 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 143 on Windows, macOS, Linux**

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**

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

Change in *Early Stable* 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. To view the new planned Early Stable dates, 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.

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**

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](#)

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

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 146 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.

Upcoming Chrome Enterprise Core updates

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 142 on iOS**: Feature would rollout gradually

Upcoming 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

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

Google and related marks and logos are trademarks of Google LLC. All other company and product names are trademarks of the companies with which they are associated.