



# Chrome 140 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 August 27, 2025.*

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

|  |           |
|--|-----------|
| <b>Chrome 140 release summary</b>          | <b>2</b>  |
| Current Chrome browser updates             | 5         |
| Current Chrome Enterprise Core updates     | 15        |
| Current Chrome Enterprise Premium updates  | 17        |
| <b>Coming soon</b>                         | <b>18</b> |
| Upcoming Chrome browser updates            | 18        |
| Upcoming Chrome Enterprise Core updates    | 28        |
| Upcoming Chrome Enterprise Premium updates | 30        |
| <b>Previous release notes</b>              | <b>34</b> |
| <b>Additional resources</b>                | <b>35</b> |
| <b>Still need help?</b>                    | <b>35</b> |

# Chrome 140 release summary

| Current Chrome browser updates  | Security / Privacy | User productivity / Apps | Management |
|---|--------------------|--------------------------|------------|
| Automated password change   | ✓                  |                          |            |
| Contextual Search suggestions in Chrome address bar                         |                    | ✓                        |            |
| DSE Prewarming  |                    | ✓                        |            |
| Enhanced autofill   |                    | ✓                        |            |
| Gemini in Chrome  |                    | ✓                        |            |
| Launch Chrome into a new Profile using command line                         | ✓                  |                          | ✓          |
| Signed-in users: Autofill & settings from Google Account.                   | ✓                  |                          |            |
| ServiceWorkerAutoPreload mode   |                    |                          | ✓          |
| Shared tab groups   |                    | ✓                        |            |
| Update to <i>No HTTPS</i> warning   | ✓                  |                          |            |
| Stop sending <i>Purpose: prefetch</i> header from prefetches and prerenders | ✓                  |                          | ✓          |
| Deprecate special font size rules for H1 within some elements               |                    |                          | ✓          |
| IP Protection   | ✓                  |                          | ✓          |
| Probabilistic Reveal Tokens   | ✓                  |                          | ✓          |
| Script blocking in Incognito  | ✓                  |                          | ✓          |

|   |                           |                                 |                   |
|---|---------------------------|---------------------------------|-------------------|
| SharedWorker inherits controller for blob URL                       |                           |                                 | ✓                 |
| New policies in Chrome browser                                      |                           |                                 | ✓                 |
| <b>Chrome Enterprise Core updates</b>                               | <b>Security / Privacy</b> | <b>User productivity / Apps</b> | <b>Management</b> |
| New filters on the Chrome Enterprise Overview page                  |                           |                                 | ✓                 |
| Regionalize covered Chrome Enterprise data                          |                           |                                 | ✓                 |
| <b>Chrome Enterprise Premium updates</b>                            | <b>Security / Privacy</b> | <b>User productivity / Apps</b> | <b>Management</b> |
| Copy/Paste rules protection   | ✓                         |                                 | ✓                 |
| DLP support for iFrames   | ✓                         |                                 | ✓                 |
| <b>Upcoming Chrome browser updates</b>                              | <b>Security / Privacy</b> | <b>User productivity / Apps</b> | <b>Management</b> |
| Add a search hijacking heuristic signal to extension telemetry      | ✓                         |                                 |                   |
| New Tab page footer   | ✓                         | ✓                               | ✓                 |
| PostQuantum cryptography for DTLS in WebRTC                         | ✓                         |                                 |                   |
| CSS find-in-page highlight pseudos                                  |                           | ✓                               | ✓                 |
| Local network access restrictions                                   | ✓                         |                                 | ✓                 |
| Origin-bound cookies (by default)                                   | ✓                         |                                 |                   |
| Permissions policy for Device Attributes API                        | ✓                         |                                 | ✓                 |
| Strict Same Origin policy for Storage Access API                    | ✓                         |                                 |                   |
| window.name property no longer preserved for cross-site navigations | ✓                         |                                 |                   |

|   |                           |                                 |                   |
|---|---------------------------|---------------------------------|-------------------|
| Deprecating <i>savedTabGroups</i> as individual value in <i>SyncTypesListDisabled</i> |                           |                                 | ✓                 |
| Disallow non-trustworthy plaintext HTTP prerendering                                  | ✓                         |                                 |                   |
| HSTS tracking prevention  | ✓                         |                                 |                   |
| Web App manifest: update eligibility algorithm  |                           |                                 | ✓                 |
| Happy Eyeballs V3   | ✓                         |                                 | ✓                 |
| 2SV enforcement for admins  |                           |                                 | ✓                 |
| Disallow spaces in non-file:// URL hosts  | ✓                         |                                 |                   |
| Remove third-party storage partitioning policies                                      | ✓                         |                                 |                   |
| SafeBrowsing API v4 → v5 migration  | ✓                         |                                 |                   |
| X25519Kyber768 key encapsulation for TLS  | ✓                         |                                 |                   |
| Isolated Web Apps   |                           |                                 | ✓                 |
| UI Automation accessibility framework provider on Windows                             |                           | ✓                               |                   |
| <b>Upcoming Chrome Enterprise Core updates</b>  | <b>Security / Privacy</b> | <b>User productivity / Apps</b> | <b>Management</b> |
| Enrolled browsers support for the Enterprise Chrome Web Store customizations          |                           | ✓                               |                   |
| Inactive profile deletion in Chrome Enterprise Core                                   | ✓                         |                                 | ✓                 |
| <b>Upcoming Chrome Enterprise Premium updates</b>                                     | <b>Security / Privacy</b> | <b>User productivity / Apps</b> | <b>Management</b> |
| Chrome browser rule UX refactor   | ✓                         |                                 | ✓                 |

|   |   |  |   |
|---|---|--|---|
| Increased file size support for DLP scans | ✓ |  | ✓ |
| Watermarking customization                | ✓ |  | ✓ |

*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.*

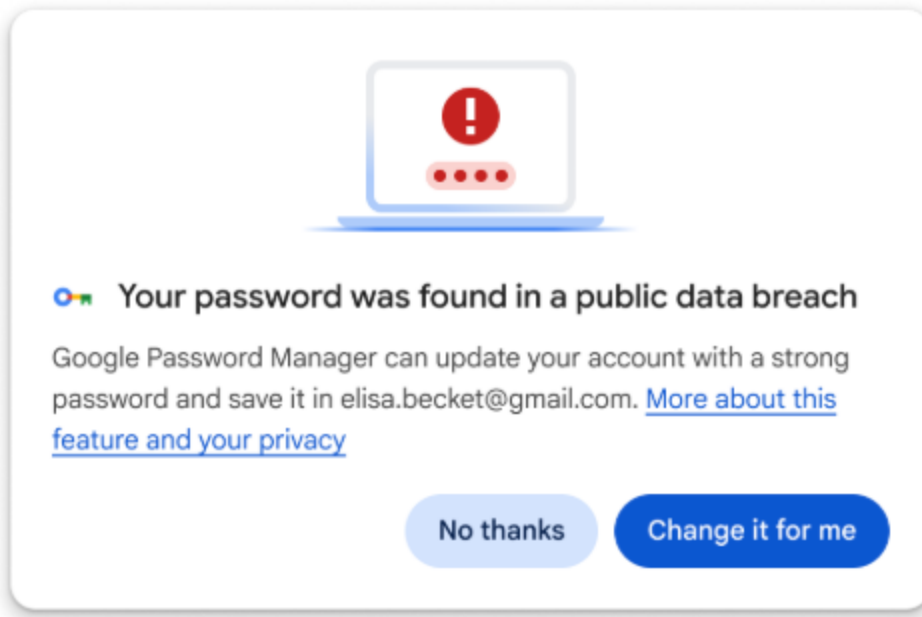
*Chrome Enterprise and Education release notes are published in line with the [Chrome release schedule](#), on the Early Stable date for Chrome browser.*

## Current Chrome browser updates

### Automated password change

When Chrome detects that a user has signed into a website with a known compromised password, it now offers to change it automatically. This feature is available on a set of eligible sites. The feature uses AI, and admins can control it using the [AutomatedPasswordChangeSettings](#) enterprise policy.

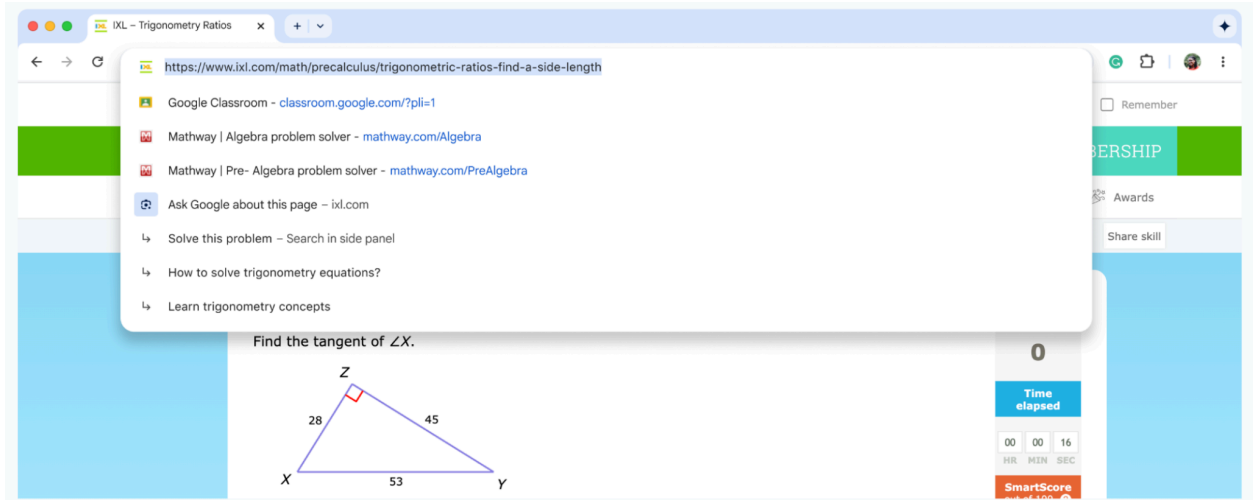
- **Chrome 140 on ChromeOS, Linux, macOS, Windows**



### Contextual search suggestions in Chrome address bar

With this feature, you can ask anything about the page you're on, directly in context. Building on the existing Search habit of the address bar, users can ask a question with Google Lens by selecting anything on screen or asking with words. A Google Lens action in the address bar and contextual suggestions guide people to the feature when it's most helpful. Admins can control this feature with the existing [LensOverlaySettings](#) policy.

- Chrome 138 on ChromeOS, Linux, macOS, Windows: Feature starts rollout
- **Chrome 140 on ChromeOS, Linux, macOS, Windows:** If the [LensOverlaySettings](#) policy is not set, this feature will respect the [GenAiDefaultSettings](#) policy if present.



## DSE Prewarming

DSE Prewarming optimizes the default search provider integration in the Omnibox. When the Omnibox gets a focus, Chrome starts prerendering the prewarm page that preload required resources for the search result page, and reuses the resources to accelerate navigating to the search result page in the next query. Admins can control this feature with the, [NetworkPredictionOptions](#) enterprise policy.

- **Chrome 140 on ChromeOS, Linux, macOS, Windows:** Gradual roll-out

## Enhanced autofill

Starting in Chrome 137, some users can turn on Autofill with AI, a new feature that helps users fill out online forms more easily. On relevant forms, Chrome can use AI to better understand the form and offer users to automatically fill in previously-saved info. Admins can control the feature using the existing [GenAiDefaultSettings](#) policy and a new [AutofillPredictionSettings](#) policy.

- Chrome 137 on ChromeOS, Linux, macOS, Windows
- **Chrome 140 on ChromeOS, Linux, macOS, Windows:** The existing "Autofill with AI" feature will be renamed to "Enhanced autofill", allow users to save and fill additional types of info, and become available in more countries and languages.

## 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 140, [Gemini in Chrome](#) becomes available for users signed into Chrome 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.

- 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 140 on macOS, Windows:** Feature gradually rolls out on Stable for users signed into Chrome in the US.

## Launch Chrome into new profile via command line

This feature is designed for our enterprise partners and admins who need to launch web applications from their native app catalogs directly into a specific managed Chrome profile using `Chrome-Cli`. Currently, if the designated profile does not exist, Chrome defaults to the last-used profile, creating a disjointed user experience. With this new feature, when a specified profile is not found, Chrome initiates the existing profile creation flow, pre-populating the user's email address to streamline the setup process. This is a key technical enabler for admins aiming to onboard their enterprise users to Chrome Enterprise via managed profiles.

- **Chrome 140 on Linux, macOS, Windows**

## Signed-in users: Autofill & settings from Google Account

As part of our effort to streamline Chrome's identity model on Desktop, managed accounts that originally signed in to Chrome implicitly by signing in to a Google web property, and who are in a



managed profile with user policies, can now save and use Autofill, settings and themes from their Google Account while signed in. Existing user policies continue to work as before, including [SyncDisabled](#), [SyncTypesListDisabled](#), [BrowserSignin](#), [AutofillAddressEnabled](#), [AutofillCreditCardEnabled](#) and [PasswordManagerEnabled](#).

- **Chrome 140 on 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

### **Shared tab groups**

Users can now collaborate on tabs using the shared tab groups feature. With this feature, users can create and use a set of tabs on their desktop or mobile device and their collaborative partners can browse the same tabs on their devices. When one person changes a tab in the group, the changes are reflected across all users' browsers in the group. Admins can control this feature using an enterprise policy, [TabGroupSharingSettings](#), in Chrome 140.

- Chrome 138 on Android, ChromeOS, Linux, macOS, Windows: Rollout of the ability to join and use a shared tab group. Users on Stable Chrome will not be able to create a shared

tab group (the entry point will not be available) - this part of the feature will only be available on Beta/Dev/Canary for this phase of rollout.

- Chrome 139 on iOS: As early as Chrome 139, support for iOS will rollout

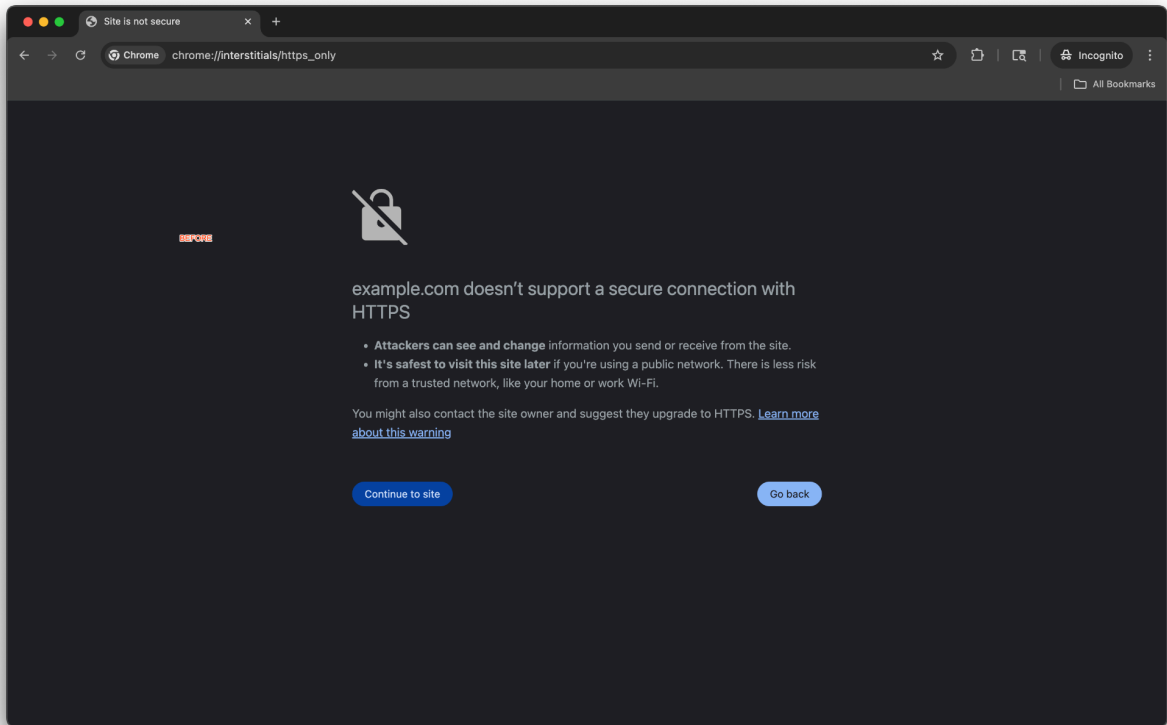
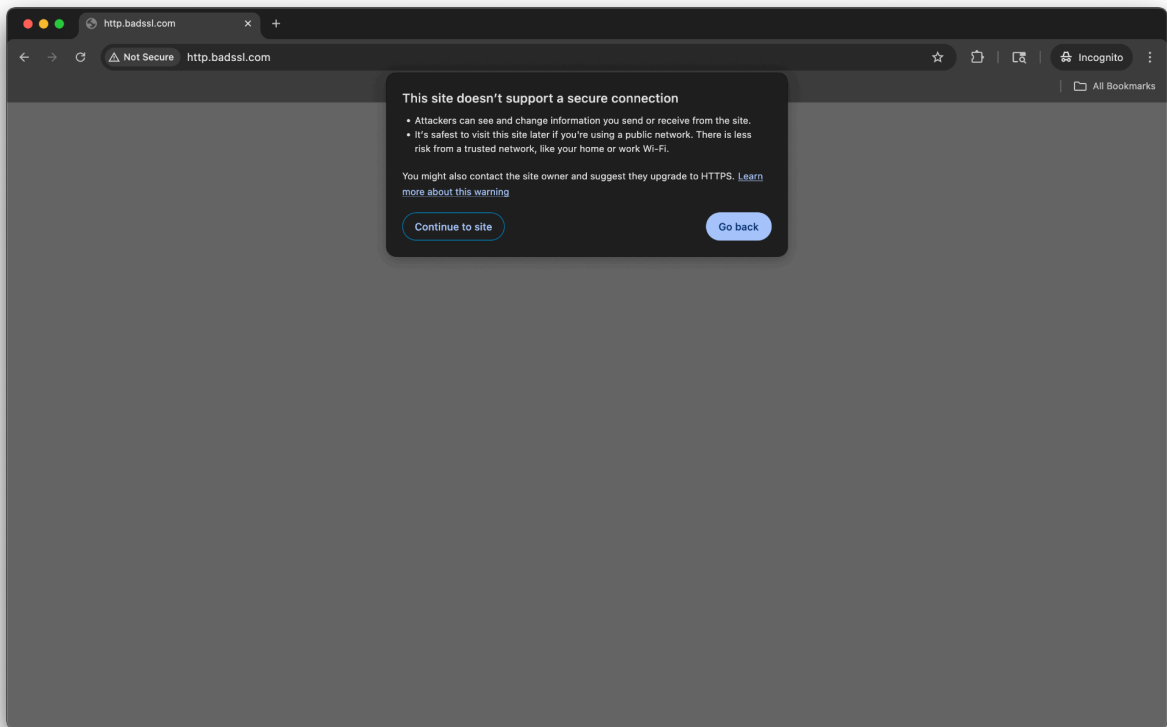
- **Chrome 140 on Android, iOS, ChromeOS, Linux, macOS, Windows:**

[TabGroupSharingSettings](#) enterprise policy will be available to the enterprise owner in the admin console. 100% of users on Stable will be able to join and use a shared tab group. However, the ability to create a shared tab group will remain exclusive to users on Beta/Dev/Canary, implying that only users on those channels could initiate a group (their friends and coworkers on Stable can then join).

### **Update to *No HTTPS* warning**

Chrome 140 updates 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 141 on Android: New warning design on Android



## Stop sending *Purpose: prefetch* header from prefetches and prerenders

Now that prefetches and prerenders are using the Sec-Purpose header for prefetches and prerenders, this change removes the legacy *Purpose: prefetch* header that is still currently passed. This update is behind a feature flag or kill switch to prevent compatibility issues.

The scope includes speculation rules prefetch, speculation rules prerender, *<link rel=prefetch>*, and Chromium's non-standard *<link rel=prerender>*.

- **Chrome 140 on Windows, macOS, Linux, Android**

## Deprecate special font size rules for H1 within some elements

The HTML spec contains a list of [special rules for <h1> tags](#) nested within <article>, <aside>, <nav>, or <section> tags. Chrome 140 deprecates these special rules, because they can cause accessibility issues. For example, they can visually reduce the font size for nested <h1> tags so that they look like <h2> tags, but nothing in the accessibility tree reflects this demotion.

- **Chrome 140 on Windows, macOS, Linux, Android**

## IP protection

This feature limits availability of a user's original IP address in third-party contexts in **Incognito mode**, enhancing Incognito's protections against cross-site tracking when users choose to browse in this mode. IP addresses facilitate a range of use cases, including routing traffic and preventing fraud and spam. However, they can also be used for tracking. For Chrome users who choose to browse in Incognito mode, we want to provide additional control over their IP address, without breaking essential web functionality. To strike this balance between protection and usability, this proposal focuses on limiting the use of IP addresses in a third-party context in Incognito mode. To that end, this proposal uses a list-based approach, where only domains on the [Masked Domain List \(MDL\)](#) in a third-party context will be impacted. For enterprises, this feature can be controlled via the [PrivacySandboxIpProtectionEnabled](#) enterprise policy.

- **Chrome 140 on Windows, macOS, Linux, Android**

### **Probabilistic Reveal Tokens**

To ensure that all businesses can continue to estimate the amount of fraud on their systems, train models to defend against fraud, and analyze emerging fraudulent behavior while still mitigating the ability to track users at scale using IP addresses, Chrome 140 introduces a delayed IP sampling mechanism called Probabilistic Reveal Tokens (PRTs) alongside IP Protection, for use in protected traffic.

PRTs are now included on proxied requests in a new HTTP header added by the browser for domains that indicate they want to receive them via a signup process. Each PRT contains a ciphertext, generated by an Issuer and re-randomized for unlinkability by the browser prior to the request, that the recipient can decrypt after a delay. Google will be the issuer for Chrome's implementation. A minority of the decrypted PRTs contain the client's pre-proxy IP address (that is, non-masked, and as observed by the token issuer), while the remaining PRTs provide no information about the client's original IP address. This results in only a small percent of PRTs containing and revealing the user's IP. Since PRTs will only be attached when IP Protection is enabled, admins can use the [PrivacySandboxIpProtectionEnabled](#) policy to control IP Protection and PRTs.

- **Chrome 140 on Windows, macOS, Linux, Android**

### **Script blocking in Incognito**

Mitigating API Misuse for Browser Re-Identification, otherwise known as *Script blocking*, is a feature that blocks scripts engaging in known, prevalent techniques for browser re-identification in third-party contexts. These techniques typically involve the misuse of existing browser APIs to extract additional information about the user's browser or device characteristics.

This feature uses a list-based approach, where only domains marked as *Impacted by Script Blocking* on the Masked Domain List (MDL) in a third-party context will be impacted. When the feature is enabled, Chrome checks network requests against the blocklist. Chromium's

[subresource\\_filter component](#) is reused, which is responsible for tagging and filtering subresource requests based on page-level activation signals, and a ruleset is used to match URLs for filtering. The enterprise policy name is [PrivacySandboxFingerprintingProtectionEnabled](#).

- **Chrome 140 on Windows, macOS, Linux, Android**

### **SharedWorker inherits controller for blob URL**

According to [Worker client case \(github\)](#), workers should inherit controllers for the blob URL. However, existing code allows only dedicated workers to inherit the controller, and shared workers do not inherit the controller. This is the fix to make Chromium behavior adjust to the specification. An enterprise policy [SharedWorkerBlobURLFixEnabled](#) is available to control this feature.

- **Chrome 140 on Windows, macOS, Linux, Android**

## New policies in Chrome browser

| Policy  | Description  |
|---|--|
| <a href="#">DataControlsRules</a>                             | Sets a list of Data Controls rules.  |
| <a href="#">LiveCaptionEnabled</a>                            | Enable Live Caption  |
| <a href="#">ProtectedContentIdentifiersAllowed</a>            | Allows web pages to use identifiers for the purpose of protected content playback                        |
| <a href="#">TabGroupSharingSettings</a>                       | Tab group sharing settings   |
| <a href="#">RestrictCoreSharingOnRenderer</a>                 | Restrict CPU core sharing for renderer process   |
| <a href="#">OriginKeyedProcessesEnabled</a>                   | Enable origin-keyed process isolation by default.  |
| <a href="#">AutomatedPasswordChangeSettings</a>               | Enable automated password change   |
| <a href="#">ServiceWorkerAutoPreloadEnabled</a>               | Allow ServiceWorker to dispatch navigation requests without waiting for its startup                      |
| <a href="#">PrivacySandboxFingerprintingProtectionEnabled</a> | Choose whether the Privacy Sandbox Fingerprinting Protection feature is to be enabled in Incognito mode. |
| <a href="#">WebRtcPostQuantumKeyAgreement</a>                 | Enable post-quantum key agreement for WebRTC   |
| <a href="#">SerialAskForUrls</a>                              | Allow the Serial API on these sites  |
| <a href="#">SerialBlockedForUrls</a>                          | Block the Serial API on these sites  |
| <a href="#">DefaultSerialGuardSetting</a>                     | Control use of the Serial API  |
| <a href="#">SerialAllowAllPortsForUrls</a>                    | Automatically grant permission to sites to connect all serial ports.                                     |
| <a href="#">LocalNetworkAccessAllowedForUrls</a>              | Allow sites to make requests to local network endpoints.   |

| Policy   | Description  |
|--|--|
| <a href="#">LocalNetworkAccessBlockedForUrls</a> | Block sites from making requests to local network endpoints. |

## Current Chrome Enterprise Core updates

### New filters on the Chrome Enterprise Overview page

The Chrome Overview page now includes new filters that allows admins to refine data by last activity date and organizational unit. This Overview page was originally introduced in Chrome 137 as part of the Chrome browser Enterprise section within the Google Admin console.

- **Chrome 140 on Android, iOS, Linux, macOS, Windows:** As early as Chrome 140, new filters will be available on the Overview page.

The screenshot shows the Chrome Enterprise Overview page. At the top right, there are two filters: "Global Organization" and "Past 28 days", which are highlighted with a red box. The main content area is divided into several sections:

- Managed browsers:** A table showing 0 Active, 1 Inactive, and 0 New browsers. Below the table, it says "No active browsers.".
- Managed profiles:** A table showing 6 Active (25%), 18 Inactive (75%), and 1 New (4.2%) profiles. Below the table, there is a section for "Operating system" with a list of operating systems and their counts and percentages: Mac (5, 83.3%), Windows (1, 16.7%), Linux (0, 0%), Android (0, 0%), and Unknown (0, 0%).
- Versions:** A table showing 0 Update pending.
- Extensions:** A table showing 0 Installed, 4 Configured, and 0 Requested extensions.



## Regionalize covered Chrome Enterprise data

With Chrome 139, administrators gained the ability to designate a specific geographic location for storing users' covered Chrome Enterprise data. Options include the United States, European Union (displayed as **Europe** in the Google Admin console), or **No preference**. The full migration is anticipated to conclude by the end of Chrome 140. This setting is configurable within the Google Admin console under **Data > Compliance > Data regions > Region > Data at rest**. For details on the types of data covered, refer to the [Chrome Enterprise Service Specific Terms](#).

- **Chrome 139 on Android, iOS, ChromeOS, Linux, macOS, Windows:** Rollout will begin. Admins may be able to set a region; however, data may not be fully regionalized until the end of Chrome 140.
- **Chrome 140 on Android, iOS, ChromeOS, Linux, macOS, Windows:** The initial migration will be fully regionalized.

## Current Chrome Enterprise Premium updates

### Copy/Paste rules protection

To help organizations better prevent data exfiltration on mobile devices, Chrome is extending its existing desktop clipboard data controls. Administrators can now use the [DataControlsRules](#) policy to set rules that block or warn users when they attempt to copy or paste content that violates organizational policies. This feature allows admins to define data boundaries and prevent sensitive information from being pasted from a work context into personal apps or websites on their mobile fleet. This addresses a significant security gap and a frequently requested feature from enterprise customers who have cited the lack of mobile data controls as a concern.

To use this feature, administrators can configure clipboard restrictions within the [DataControlsRules](#) policy, providing a consistent management experience across desktop and mobile to strengthen their organization's overall security posture. [This help center article](#) provides further context on how administrators can configure and manage Chrome Enterprise reporting connectors to forward browser security and data protection events to third-party services for analysis.

- **Chrome 140 on Android:** Copy/Paste Rules Protection becomes available on Android

## DLP support for iFrames

To enhance security and prevent data exfiltration, Chrome 140 extends Data Loss Prevention (DLP) capabilities to content within iFrames. With this change, when a user performs a DLP-triggering action (such as uploading a file) from a site loaded in an iFrame, Chrome now sends the entire URL hierarchy, from the source iFrame up to the top-level page, to be evaluated against all applicable DLP rules.

No new enterprise policies are required to enable this functionality; it works with existing DLP rules configured via the [Connector policies](#). Administrators should be aware that their existing rules now apply to iFrame contexts, which might block user actions that were previously permitted.

- **Chrome 139 on Linux, macOS, Windows:** Initial launch of Data Loss Prevention support for iFrames. This phase adds enforcement for file upload events originating from within an iFrame context and it will work with existing DLP rules configured via the [OnFileAttachedEnterpriseConnector](#) policy
- **Chrome 140 on Linux, macOS, Windows:** This expanded phase combines two feature rollouts, extending DLP iFrame support to include enforcement for both file download and printing actions.

# 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

### Add a search hijacking heuristic signal to 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**

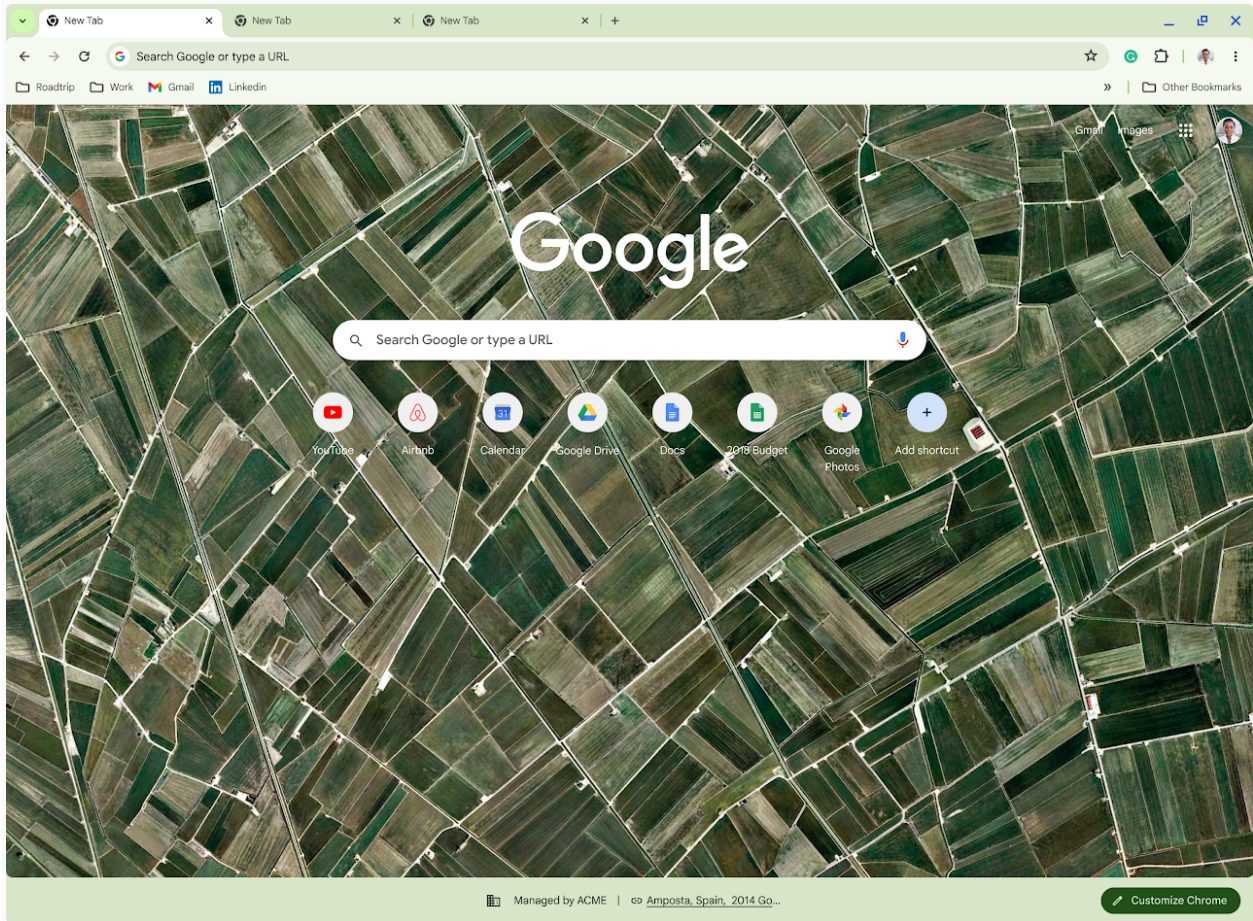
### New tab page footer

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 start to be shown in the **New tab** page footer for all managed browsers. Visibility can be changed with the [NTPFooterManagementNoticeEnabled](#) policy.



## 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.

This feature will be controllable by 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 151.

- **Chrome 141 on Android, ChromeOS, Linux, macOS, Windows, Fuchsia**
- Chrome 151 on Android, ChromeOS, Linux, macOS, Windows, Fuchsia: Remove Enterprise Policy

## 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 141 on Windows, macOS, Linux, Android**

## Local network access restrictions

Chrome 140 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-bound cookies (by default)

In Chrome 141, 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 141 on Windows, macOS, Linux, Android, iOS:** policy will be made available
- Chrome 150 on Windows, macOS, Linux, Android, iOS: policy will be removed

### Permissions policy for Device Attributes API

The new Permissions policy enables restricting access to the Device Attributes API, which is available only for policy-installed kiosk web apps and policy-installed Isolated Web Apps, both only on managed ChromeOS devices.

Additionally, the feature is controlled by content settings. 2 new policies are introduced:

[DeviceAttributesBlockedForOrigins](#) and [DefaultDeviceAttributesSetting](#), to complement the previously-introduced [DeviceAttributesAllowedForOrigins](#) policy. The feature is enabled by default for the supported scenarios described above.

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

### Strict Same Origin policy for Storage Access API

We plan to adjust the [Storage Access API](#) semantics to 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**



## **window.name property no longer preserved for cross-site navigations**

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**

## **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 142, 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 142 on Windows, macOS, Linux**

## Disallow non-trustworthy plaintext HTTP prerendering

This launch will provide the capability to disallow non-trustworthy plaintext HTTP prerendering.

- **Chrome 142 on Windows, macOS, Linux, 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 in order to track users across the web.

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

## Web App manifest: update eligibility algorithm

As early as Chrome 139, 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

## 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**

## **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 → 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\\*](https://safebrowsing.googleapis.com/v4*), these should be modified to allow network requests to the whole domain instead: [safebrowsing.googleapis.com](https://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

Starting in Chrome 124, Chrome enables 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 this 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

### Enrolled browsers support for the Enterprise Chrome Web Store customizations

The Customized Chrome Web Store will support managed browsers enrolled in [Chrome Enterprise Core](#) (Cloud machine settings). This will allow 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).

### Chrome Enterprise Overview page

Chrome 137 introduced a new **Overview** page in the Chrome browser section of the Google Admin console. The Overview page allows IT administrators to quickly find key information about their deployment:

- Active & inactive profiles and enrolled browsers
- Identify browsers out-of-date and with pending updates
- Identify high-risk extensions (according to [Spin.AI](#)) and get a preview of most requested extensions
- Security Insights (for example, sensitive file uploads or downloads)

The Overview page also allows admins to quickly access key actions such as managing extensions, accessing the browser or profile list and setting update policies, to name a few.

- Chrome 137 on Android, iOS, Linux, macOS, Windows: Publicly Available to IT administrators
- **Chrome 141 on Android, iOS, Linux, macOS, Windows:** New filtering available on the Overview page for Organization Unit and Activity Dates

### **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 will begin 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](#). The maximum value to determine the profile inactivity period is 730 days and the 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 September. After the initial deletion rollout, inactive profiles will continue to be deleted once they have reached their inactivity period.



## 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 first 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.

- **Chrome 141 on ChromeOS, Linux, macOS, Windows:** Enables mutually exclusive app selection for DLP rule configuration in Admin Console

×

Edit Rule

✓ Name and scope

2 Apps

3 Conditions

4 Actions

5 Review


Apps

Select the apps that you want to protect data in. There may be some files that can't be scanned for data protection rules, due to size or other issues. [Learn more about scan limits](#)

i


To scan for text in images and PDFs, check that Optical Character Recognition (OCR) is on. [Check](#)

☐ Workspace


 Google Chat

☐ Message sent

☐ File uploaded


 Google Drive

☐ Drive files

 Gmail NEW

☐ Message sent

☒ Chrome

 Chrome

☒ File uploaded


☒ File downloaded

☐ Content pasted

☐ Content printed

☐ URL visited

☐ ChromeOS

 ChromeOS

☐ File transfer

BACK

CANCEL

CONTINUE

## 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.

- **Chrome 140 on Linux, macOS, Windows:** Feature is rolled out

### **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.

## Previous release notes

| Chrome version & targeted Stable channel release date |
|---|
| <a href="#">Chrome 139: July 30, 2025</a>             |
| <a href="#">Chrome 138: June 18, 2025</a>             |
| <a href="#">Chrome 137: May 20, 2025</a>              |
| <a href="#">Chrome 136: April 23, 2025</a>            |
| <a href="#">Archived release notes</a>                |

## 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.*