



Chrome 139 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 July 30, 2025.

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

Chrome 139 release summary	2
Current Chrome browser updates	6
Current Chrome Enterprise Core updates	21
Current Chrome Enterprise Premium updates	25
Coming soon	28
Upcoming Chrome browser updates	28
Upcoming Chrome Enterprise Core updates	40
Upcoming Chrome Enterprise Premium updates	41
Previous release notes	45
Additional resources	46
Still need help?	46

Chrome 139 release summary

Current Chrome browser updates	Security / Privacy	User productivity / Apps	Management
AI Mode for search recommendations in Chrome		✓	
Admin-configurable site search		✓	✓
Chrome on Android no longer supports Android Oreo or Android Pie			✓
Malicious APK download checks	✓		
Migrate extensions to Manifest V3 before June 2025	✓	✓	✓
New tab page footer	✓	✓	✓
Prevent accidental password deletions on Chrome	✓		
Promotional notifications			✓
Remove risky extension flags in Chrome	✓		
Remove SwiftShader fallback	✓		
Shared tab groups		✓	
Support accounts in pending state on Chrome iOS	✓		
Upcoming change for CA certificates included in the Chrome Root Store	✓		
Stop sending Purpose: prefetch header from prefetches and prerenders	✓		✓
Chrome removes support for macOS 11			✓
Fire error event instead of throwing exception for CSP blocked worker			✓

Randomizing TCP port allocation on Windows			✓
New policies in Chrome browser			✓
Removed policies in Chrome browser			✓
Chrome Enterprise Core	Security / Privacy	User productivity / Apps	Management
Group based policies for connector configuration selection			✓
New remote commands and CSV export for the Managed Profile List			✓
New tab page cards for Microsoft 365		✓	✓
Regionalize covered Chrome Enterprise data			✓
Chrome Enterprise Premium	Security / Privacy	User productivity / Apps	Management
Active account detection	✓		✓
Chrome Enterprise Connectors API	✓		✓
Copy and paste rules protection	✓		✓
Data Loss Prevention support for iFrames	✓		✓
Enable watermarking on Single Page Applications	✓		✓
Upcoming Chrome browser updates	Security / Privacy	User productivity / Apps	Management
2SV enforcement for admins			✓
Automated password change	✓		
Contextual search suggestions in Chrome address bar		✓	
Enhanced autofill		✓	
Gemini in Chrome		✓	

Happy Eyeballs V3	✓		✓
Launch Chrome into new profile from command line	✓		✓
PostQuantum cryptography for DTLS in WebRTC	✓		
ServiceWorkerAutoPreload			✓
CSS find-in-page highlight pseudos		✓	✓
Deprecate special font size rules for H1 within some elements			✓
IP protection	✓		✓
Local network access restrictions	✓		✓
Probabilistic reveal tokens	✓		✓
Propagate Viewport overscroll-behavior from Root	✓		✓
Script blocking in Incognito	✓		✓
SharedWorker script inherit controller for blob script URL			✓
Strict Same Origin Policy for Storage Access API	✓		
Web App Manifest: specify update eligibility, icon urls are Cache-Control: immutable			✓
Clear window name for cross-site navigations that switches browsing context group	✓		
Disallow non-trustworthy plaintext HTTP prerendering	✓		
HSTS tracking prevention	✓		
Disallow spaces in non-file:// URL hosts			✓
Remove third-party storage partitioning policies	✓		

SafeBrowsing API v4 → v5 migration	✓		
Isolated Web Apps			✓
UI Automation accessibility framework provider on Windows		✓	
Upcoming Chrome Enterprise Core updates	Security / Privacy	User productivity / Apps	Management
Inactive profile deletion in Chrome Enterprise Core	✓		✓
Chrome Enterprise Overview page			✓
Upcoming Chrome Enterprise Premium updates	Security / Privacy	User productivity / Apps	Management
Increased file size support for Data Loss Prevention scans	✓		✓
Watermarking customization	✓		✓
Chrome browser rule UX refactor	✓		✓

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.

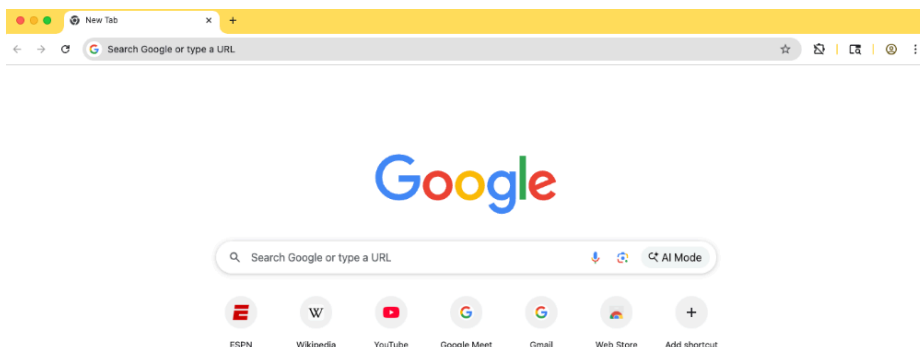
Chrome Enterprise and Education release notes are published in line with the [Chrome release schedule](#) on the Early Stable date for Chrome browser.

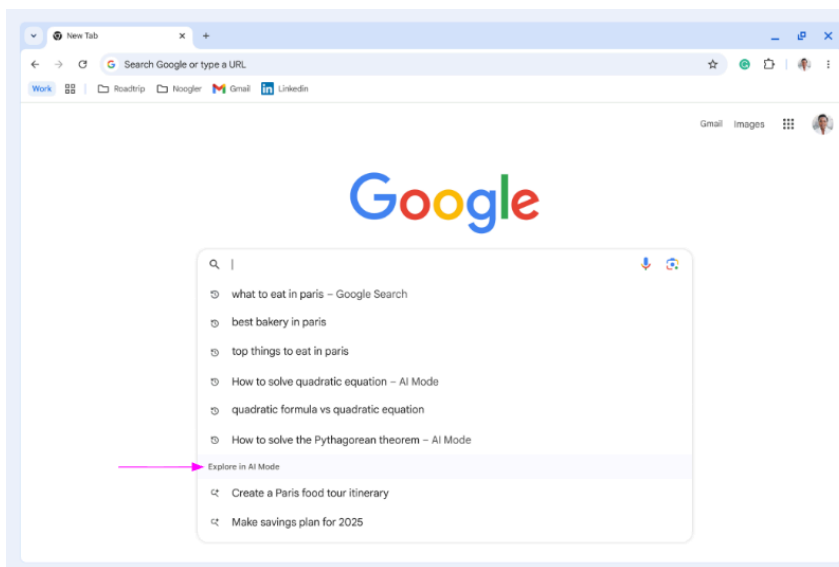
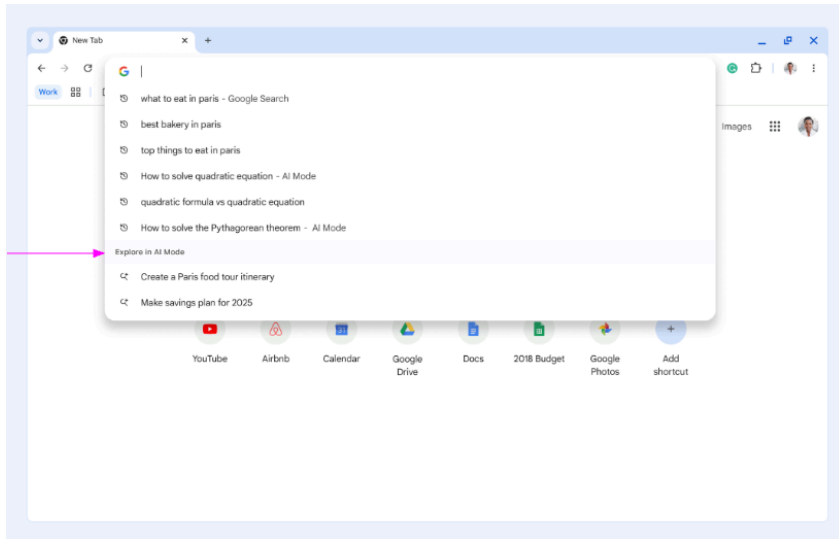
Current Chrome browser updates

AI Mode for search recommendations in Chrome

AI Mode is a feature that helps users dive deeper into topics they care about by showing AI Mode for search recommendations in Chrome. A new policy, [AI Mode Settings](#), is available to control search recommendations in the address bar and **New tab** page search box. This policy also controls AI Mode recommendations in the address bar and the new tab page omnibox.

- Chrome 138 on ChromeOS, Linux, macOS, Windows: AI Mode recommendations starts rolling out in the address bar and the new tab page search box. The AI Mode entry point is also rolled out in the new tab page search box.
- **Chrome 139**
 - **on Windows, macOS, Linux and ChromeOS:** The AI Mode entrypoint button in the address bar begins rollout. AI Mode inline compose box in new tab page omnibox begins rollout.
 - **on Android, iOS:** The AI Mode entrypoint in the new tab page omnibox begins to roll out. And for iOS the AI Mode recommendations starts rollout in the address bar as well.





Admin-configurable site search

Site search shortcuts are a way to use the address bar (omnibox) as a search box for a specific site without navigating directly to the site's URL, similar to how you can use the omnibox to perform a broad Google search of the web. Administrators can now create site shortcuts for users to shortcut to the most critical enterprise sites. Users can initiate a search by typing the shortcut or @shortcut (for example, @work), followed by Space or Tab, in the address bar.

Admins control these shortcut settings using the [SiteSearchSettings](#) policy.

- Chrome 128 on ChromeOS, Linux, macOS, Windows: Gradual rollout
- **Chrome 139 on ChromeOS, Linux, macOS, Windows:** Adding an additional policy parameter allowing admins to specify **Allow user override**, which allows users to edit, disable, or delete admin-set shortcuts

About this setting

Provides a list of sites that users can quickly search using predefined shortcuts in their address bar. For example, you can create predefined shortcuts to your organization's company intranet, most used tools, and so on. Users trigger a search by typing **@shortcut**, or just **shortcut**, followed by Space bar or Tab key in their address bar.

Enter details for the shortcuts you want to configure:

- **Site or page**—The name that is shown to the user in their address bar. For example, enter **Workspace**.
- **Shortcut**—The keyword that the user enters to trigger the search. The shortcut can include plain words and characters, but cannot include spaces or start with the @ symbol. Shortcuts must be unique. For example, enter **ws**. Then, users type **ws** in their address bar to trigger the search.
- **URL**—The URL on which to search. Enter the web address for the search engine's results page, and use **{searchTerms}** in place of the query. For example, enter **https://drive.google.com/corp/drive/search?q={searchTerms}**.
- **Featured**—When selected as **Featured**, the shortcut appears as a recommendation when users type @ in their address bar. Up to three entries can be selected as **Featured**.

Chromium name

[SiteSearchSettings](#)

Supported on

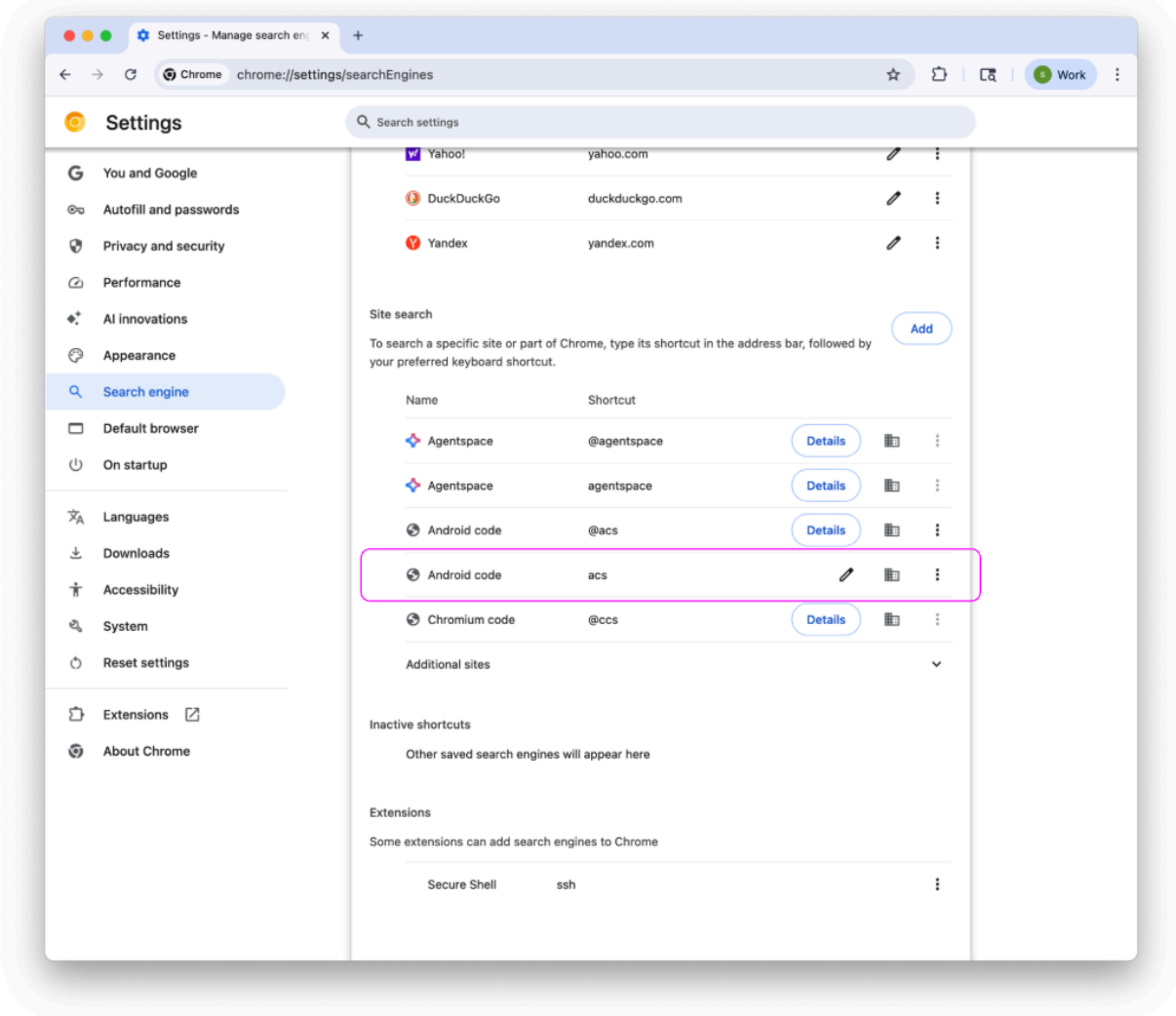
Chrome (Windows, Mac, Linux) since version 128
ChromeOS since version 128

Inheritance

Locally applied

Configuration

Site or page	Shortcut	URL	Featured	Allow user override
Android Code	asc	https://cs.android.com/search?q=test&sq={searchTerms}	Featured	Allow user override
+ Add item				



Chrome on Android no longer supports Android Oreo or Android Pie

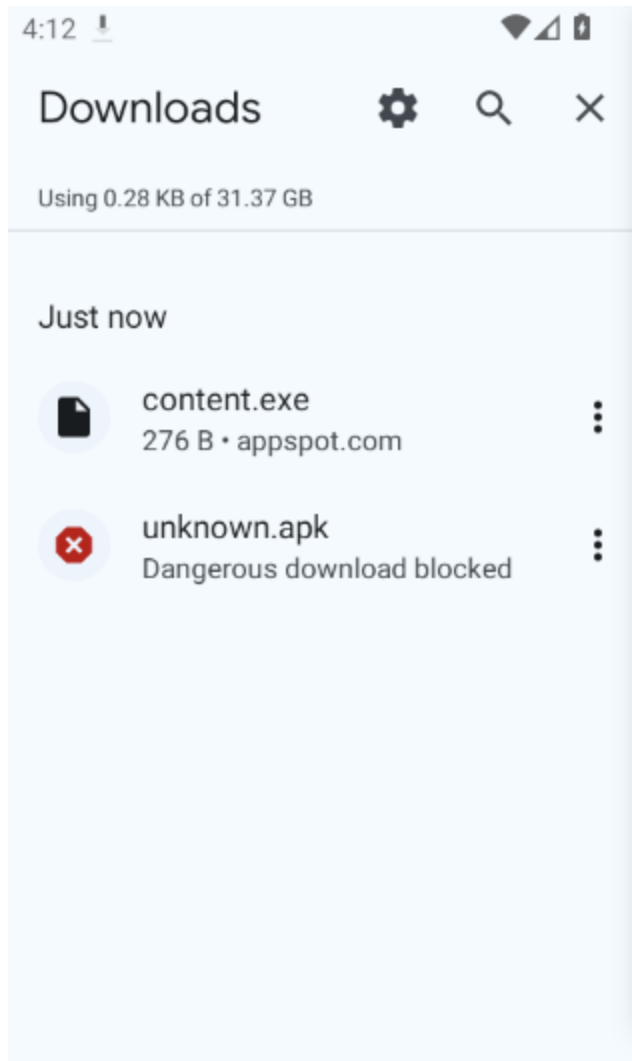
The last version of Chrome that supports Android Oreo or Android Pie is Chrome 138, and it includes a message to affected users informing them to upgrade their operating system. Chrome 139 and later versions will not be supported on, nor shipped or available to, users running Android Oreo or Android Pie.

- **Chrome 139 on Android:** Chrome on Android no longer supports Android Oreo or Android Pie.

Malicious APK download checks

Chrome on Android now contacts Google servers about Android Package Kit (APK) files downloaded in Chrome, to get a verdict about their safety. If a downloaded APK file is determined to be dangerous, Chrome shows a warning and blocks the download, to protect users against mobile malware. Such download warnings are bypassable by the user through the Chrome UI. These malicious APK download checks are performed for users enrolled in Standard Protection or Enhanced Protection from Google Safe Browsing. This feature can be disabled by setting the Safe Browsing mode to *No Protection* using the [SafeBrowsingProtectionLevel](#) policy.

- **Chrome 139 on Android**



Migrate extensions to Manifest V3 before June 2025

Extensions must be updated to use Manifest V3. Chrome extensions are transitioning to a new manifest version, Manifest V3. This brings improved privacy for your users—for example, by moving to a model where extensions modify requests declaratively, without the ability to see individual requests. This also improves extension security, as remotely-hosted code is disallowed on Manifest V3.

Beginning June 2024, Chrome gradually disables Manifest V2 extensions running in the browser. An enterprise policy - [ExtensionManifestV2Availability](#) - can be used to test Manifest V3 in your organization ahead of the migration. Additionally, machines on which the policy is

enabled are not subject to the disabling of Manifest V2 extensions until June 2025 - at which point the policy is to be removed.

You can see which Manifest version is being used by all Chrome extensions running on your fleet using the **Apps & extensions** usage page in Chrome Enterprise Core.

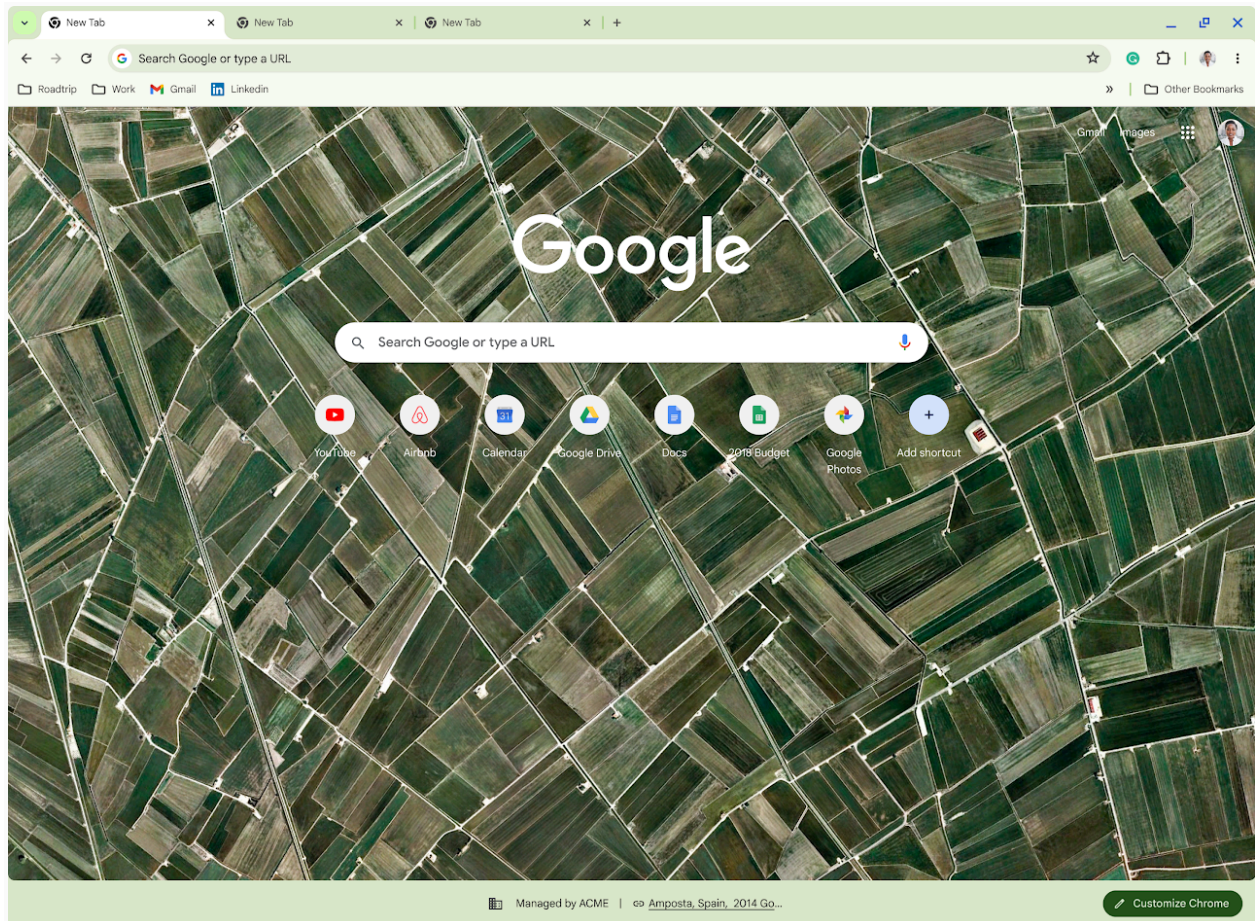
- Chrome 127 on ChromeOS, LaCrOS, Linux, macOS, Windows: Chrome will gradually disable Manifest V2 extensions on user devices. Only those with the [ExtensionManifestV2Availability](#) enterprise policy enabled would be able to continue using Manifest V2 extensions in their organization.
- **Chrome 139 on ChromeOS, Linux, macOS, Windows:** Remove [ExtensionManifestV2Availability](#) policy.

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 140 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.



Prevent accidental password deletions on Chrome

To reduce the risk of accidental deletion of passwords on [Delete browsing data](#), Chrome 139 now points users to Google Password Manager settings, where they can better manage and delete passwords and passkeys. The feature removes the **Passwords and other sign-in data** selection in

⋮ > **Delete browsing data** and instead directs users to Google Password Manager where they can delete individually or in bulk.

This feature does not impact the existing enterprise policies [ClearBrowsingDataOnExitList](#) and [BrowsingDataLifetime](#).

- **Chrome 139 on ChromeOS, Linux, macOS, Windows:** Feature will gradually roll out

Delete browsing data

Last 15 min

✓ Last hour

Last 24 hours

Last 7 days

More ▾



Browsing history

example.com + 195 items on this device, plus items on synced devices



Cookies and other site data

From 83 sites. To delete Google cookies from this device, [sign out of Chrome](#).



Cached images and files

288 MB



Download history

17 items



Autofill form data

None



Site settings

3 sites

Manage other Google data

Search history and passwords can be deleted in their management settings



Elisa Beckett

elisa.g.beckett@gmail.com

Cancel

Delete data

Promotional notifications

In Chrome 128, new promotional OS-level notifications began to be shown to users. These notifications are governed by the [PromotionsEnabled](#) enterprise policy.

- Chrome 128 on ChromeOS, Linux, macOS, Windows
- **Chrome 139 on Windows:** In Chrome 138, promotional notifications were only activated on Chrome clients when upgrading from Windows 10 to Windows 11. From Chrome 139, this is being extended to all Windows Chrome installations. Notifications will still be only shown to a subset of low-engaged users, and these can be disabled through the [PromotionsEnabled](#) enterprise policy.

Remove risky extension flags in Google Chrome

To enhance the security and stability of the Chrome browser for our users, official Chrome branded builds will be removing `--extensions-on-chrome-urls` and `--disable-extensions-except` command-line flags starting in Chrome 139. This change aims to mitigate the risks associated with harmful and unwanted extensions. Developers can still use the both flags in non-branded builds such as [Chromium and Chrome For Testing](#).

- **Chrome 139 on Linux, macOS, Windows**

Remove SwiftShader fallback

Allowing automatic fallback to [WebGL](#) backed by [SwiftShader](#) is deprecated and WebGL context creation now fails instead of falling back to SwiftShader. This was done for two primary reasons:

1. SwiftShader is a high security risk due to JIT-ed code running in Chromium's GPU process.
2. Users have a poor experience when falling back from a high-performance GPU-backed WebGL to a CPU-backed implementation. Users have no control over this behavior and it is difficult to describe in bug reports.

SwiftShader is a useful tool for web developers to test their sites on systems that are headless or do not have a supported GPU. This use case will still be supported by opting in but is not intended for running untrusted content. To opt in to lower security guarantees and allow SwiftShader for WebGL, run the chrome executable with the `--enable-unsafe-swiftshader` command-line switch.

During the deprecation period, a warning will appear in the javascript console when a WebGL context is created and backed with SwiftShader. Passing `--enable-unsafe-swiftshader` will remove this warning message.

Chromium and other browsers do not guarantee WebGL availability. It is important to test and handle WebGL context creation failure and fall back to other web APIs such as Canvas2D or an appropriate message to the user.

- **Chrome 139**

- **on Linux, macOS:** Swiftshader will be disabled on macOS and Linux. Users on machines without a GPU will not be able to use WebGL.
- **On Windows:** The fallback to Swiftshader after three out-of-memory (OOM) errors will be disabled on Windows. Swiftshader usage will be limited to devices without a GPU or those with a GPU on the blocklist.

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. An enterprise policy, **TabGroupSharingSettings**, will be available in Chrome 140 to control this feature.

- 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.

Support accounts in pending state on Chrome iOS

Accounts whose credentials somehow became invalid are no longer automatically signed out and removed from Chrome on iOS. Instead, these accounts stay signed in to the browser, in a newly introduced *pending state* associated with a persistent error indication in the UI so users are encouraged to resolve it. This also means that local data associated with these accounts are no longer automatically deleted, but instead kept on disk. Existing policies controlling sign-in (for example, [BrowserSignin](#)) continue to work as before.

- **Chrome 139 on iOS:** Feature will gradually roll out

Upcoming change for CA certificates included in the Chrome Root Store

In response to sustained compliance failures, Chrome 139 changes how publicly-trusted TLS server authentication, that is, websites or certificates issued by Chunghwa Telecom and Netlock, are trusted by default. This applies to Chrome 139 and later on Windows, macOS, ChromeOS, Android, and Linux; iOS policies do not allow use of the Chrome Root Store in Chrome for iOS.

Specifically, TLS certificates validating to the Chunghwa Telecom or Netlock root CA certificates included in the Chrome Root Store and issued:

- after July 31, 2025, will no longer be trusted by default.
- on or before July 31, 2025, will be unaffected by this change.

If a Chrome user or an enterprise explicitly trusts any of the affected Chunghwa Telecom or Netlock certificates on a platform and version of Chrome relying on the Chrome Root Store, for example, when explicit trust is conveyed through a Windows Group Policy Object, the Signed Certificate Timestamp (SCT) constraints described above will be overridden and certificates will function as they do today.

For additional information and testing resources, see [Sustaining Digital Certificate Security - Upcoming Changes to the Chrome Root Store](#).

To learn more about the Chrome Root Store, see this [FAQ](#).

- **Chrome 139 on Android, ChromeOS, Linux, macOS, Windows:** All versions of Chrome 139 and higher that rely on the Chrome Root Store will honor the blocking action, but the blocking action will only begin for certificates issued after July 31, 2025.

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 139 on Windows, macOS, Linux, Android**

Chrome to remove support for macOS 11

Chrome 138 is the last release to support macOS 11; Chrome 139 and later will no longer support macOS 11, which is outside of its support window with Apple. Running on a supported operating system is essential to maintaining security.

On Macs running macOS 11, Chrome will continue to work, showing a warning infobar, but will not update any further. If a user wishes to have their Chrome updated, they need to update their computer to a support version of macOS. For new installations of Chrome 139 and later, macOS 12 and later will be required.

- **Chrome 139 on Windows, macOS, Linux**

Fire error event instead of throwing exception for CSP blocked worker

When blocked by [Content Security Policy \(CSP\)](#), Chromium currently throws a `SecurityError` from the constructor of `Worker` and `SharedWorker`. To be spec-compliant, the CSP needs to be checked as part of fetch and then fire error events asynchronously instead of throwing an exception when the script runs `new Worker(url)` or `new SharedWorker(url)`.

This update aims to make Chromium spec-conformant, which is, it no longer throws exceptions following constructor calls, and fires error events asynchronously.

- **Chrome 139 on Windows, macOS, Linux, Android**

Randomizing TCP port allocation on Windows

This feature enables TCP port randomization on Windows versions 2020 H1 and later. We do not anticipate issues with rapid re-use of prior ports (which can cause rejections due to port re-use timeouts) on these versions. The rapid port re-use issue stems from [the Birthday](#)

[problem](#), where the probability of randomly re-picking an already used port quickly approaches 100% with each new port chosen, unlike sequential port re-use models.

- **Chrome 139 on Windows, macOS, Linux**

New policies in Chrome browser

Policy	Description
GeminiSettings	Settings for Gemini integration
WatermarkStyle	Configure Custom Watermark Settings
EnableUnsafeSwiftShader	Allow software WebGL fallback using SwiftShader
NTPFooterManagementNoticeEnabled	Control the visibility of the management notice on the New Tab Page for managed browsers
EnterpriseLogoUrlForBrowser	Enterprise Logo URL for a managed browser
EnterpriseCustomLabelForBrowser	Set a custom enterprise label for a managed browser
LocalNetworkAccessRestrictionsEnabled	Specifies whether to apply restrictions to requests to local network endpoints
LocalNetworkAccessAllowedForUrls	Allow sites to make requests to local network endpoints.
LocalNetworkAccessBlockedForUrls	Block sites from making requests to local network endpoints.

Removed policies in Chrome browser

Policy	Description
ExtensionManifestV2Availability	Control Manifest v2 extension availability
SelectParserRelaxationEnabled	Controls whether the new HTML parser behavior for the <select> element is enabled
KeyboardFocusableScrollersEnabled	Enable keyboard focusable scrollers

Current Chrome Enterprise Core updates

Group based policies for connector configuration selection

Reporting connector configurations that receive events sent by managed browsers can now be [configured by groups](#) in addition to organizational units.

- **Chrome 139 on ChromeOS, Linux, macOS, Windows**

The image displays two screenshots of the Google Admin console's 'Connectors' page, illustrating the new group-based policy configuration options for reporting connectors.

Top Screenshot: All browsers & devices

- The left sidebar shows the 'Connectors' menu item highlighted.
- The main content area shows the 'All browsers & devices' tab.
- A red box highlights the 'Groups' dropdown menu in the 'All browsers & devices' section.
- A red arrow points from the 'Groups' dropdown to the 'Google Security Operations' connector configuration.
- The 'Google Security Operations' connector configuration shows a list of connectors with their status (e.g., 'Connected to 3 org units', 'Not connected to any org unit', 'Connection lost').
- A red arrow points from the 'Group setting available' label to the 'Groups' dropdown.

Bottom Screenshot: Reporting connectors

- The left sidebar shows the 'Connectors' menu item highlighted.
- The main content area shows the 'Reporting connectors' tab.
- A red box highlights the 'Groups' dropdown menu in the 'Reporting connectors' section.
- A red arrow points from the 'Groups' dropdown to the 'Google Security Operations' connector configuration.
- The 'Reporting connectors' section shows a list of connectors with their status (e.g., 'Locally applied', 'Connection lost').
- A red arrow points from the 'Click on a particular group to set the value for that group' label to the 'Groups' dropdown.
- A red arrow points from the 'Set precedence for the order in which settings are applied if a user is in multiple groups' label to the 'Groups' dropdown.

New remote commands and CSV export for the Managed profiles list

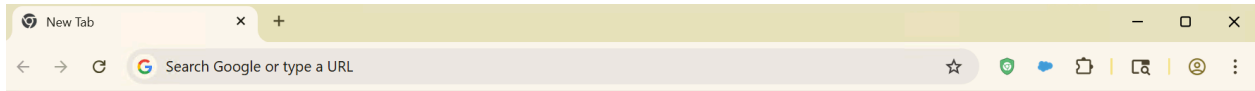
The Admin console will support profile-level "Clear cache" and "Clear cookies" remote commands, and CSV export for the Managed Profiles list. You can select one or multiple profiles and perform a remote command.

- Chrome 137 on Android, Linux, macOS, Windows: Adding CSV export for Managed profiles.
- **Chrome 139 on Linux, macOS, Windows:** Profile-level support for remote commands.

New tab page cards for Microsoft 365

Enterprise users with Outlook or SharePoint can now access their upcoming meetings or suggested files directly from the **New tab** page. This streamlined experience eliminates the need to switch tabs or waste time searching for your next meeting, allowing you to focus on what matters most. Admins can enable the cards with [NTPSharepointCardVisible](#) and [NTPOutlookCardVisible](#). For Microsoft tenants who do not allow for self-authorization, the admin must also consent to the app permissions during first authentication or approve the app for use in Microsoft Entra.

- Chrome 134 on Linux, macOS, Windows: Available to Trusted Testers
- Chrome 137 on Linux, macOS, Windows: Gradual rollout to all customers
- **Chrome 139 on ChromeOS, Linux, macOS, Windows:** Users do not need to be signed into Chrome to use this feature



Gmail Images  

Google

 Search Google or type a URL  




Google Search



Web Store




Add shortcut

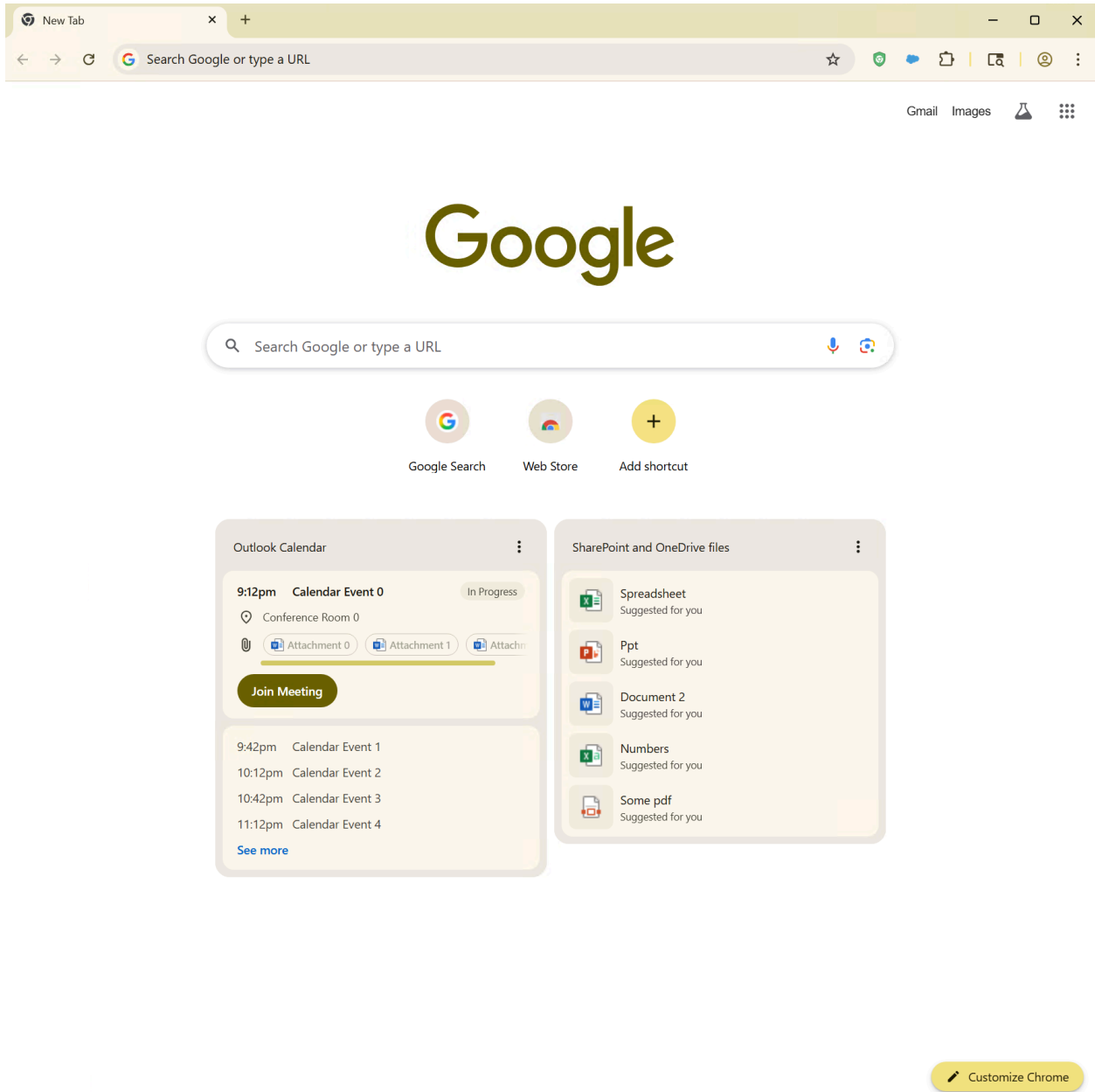


See your Outlook Calendar and SharePoint and OneDrive files

Easily access recent documents and upcoming calendar events

[Sign in with Microsoft](#)

 Customize Chrome



Regionalize covered Chrome Enterprise data

Starting in Chrome 139, Admins can use data regions to store users' covered Chrome Enterprise data in a specific geographic location. The location options are United States, European Union (labeled Europe in the Google Admin console), or No preference. The initial migration will not complete until the end of Chrome 140. This can be set in the Google Admin console via **Data > Compliance > Data regions > Region > Data at rest**. For more information about the types of data covered, see 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

Active account detection

Chrome Enterprise can now detect whether an employee is using their corporate or personal Google account on Google Workspace pages like Google Drive, Docs, or Gmail. This allows administrators to create more granular Data Loss Prevention (DLP) rules to prevent sensitive data from being moved to personal accounts, addressing a critical data exfiltration risk. For instance, an administrator can now configure a policy in the Google Admin console to block a file upload to a personal Google Drive account while still allowing it to a corporate account. To use this feature, administrators should create or update their DLP rules to include the new **Google Workspace Web app signed-in account** condition. There is no single enterprise policy to enable or disable this feature; control is managed through the creation of these specific DLP rules.

- **Chrome 139 on ChromeOS, Linux, macOS, Windows:** The Chrome browser can detect the active user account on Google Workspace pages and sends this information as a new signal with Data Loss Prevention (DLP) scan requests.

Chrome Enterprise Connectors API

Chrome Enterprise is introducing programmatic management for Chrome Enterprise Connectors. This update exposes connector settings as new and updated policies within the existing Chrome Policy API, allowing IT administrators and technology partners to manage these configurations at scale. Previously, this was a manual process in the Google Admin

console. This update enables automation, which helps reduce manual errors and improve the efficiency of managing integrations with third-party security solutions.

Administrators can use the Chrome Policy API to programmatically control settings for event reporting, content analysis, and real-time URL checks. This launch includes updates to the [OnSecurityEventEnterpriseConnector](#) policy and adds new policies such as [OnFileAttachedEnterpriseConnector](#), [OnFileDownloadedEnterpriseConnector](#), [OnFileTransferEnterpriseConnector](#), [OnBulkDataEntryEnterpriseConnector](#), [OnPrintEnterpriseConnector](#), and [EnterpriseRealTimeUrlCheckMode](#).

For technical details, developers should refer to the main [Chrome Policy API documentation](#)

- **Chrome 139 on Android, iOS, Linux, macOS, Windows:** This rollout adds support for programmatic management of Chrome Enterprise Connectors via a new API

Copy and 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.

- **Chrome 139 on Android:** Copy and Paste rules protection becomes available on Android

Data Loss Prevention support for iFrames

To enhance security and prevent data exfiltration, Chrome's Data Loss Prevention (DLP) capabilities are being extended to the content within iFrames. Currently, DLP rules configured by administrators do not apply to content inside an iFrame, which allows a potential security loophole where users can bypass restrictions. This feature closes that gap. With this change, when a user performs a DLP-triggering action (such as uploading a file) from a site loaded in an iFrame, Chrome will send the entire URL hierarchy, from the source iFrame up to the top-level page, to be evaluated against all applicable DLP rules.

The motivation for this change is to provide a more robust security posture and eliminate a known method for bypassing data protection policies. No new enterprise policies are required to enable this functionality; it will work with existing DLP rules configured via the [Connector policies](#). Administrators should be aware that their existing rules will now apply to iFrame contexts, which may 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.

Enable watermarking on Single Page Applications

To enhance data security, Chrome Enterprise Premium's watermarking feature now supports Single Page Applications (SPAs). This addresses a significant customer request, as watermarks previously only applied to traditional websites. This capability is controlled by your existing Data Loss Prevention (DLP) policies in the Google Admin Console; no new policy configuration is required for this enhancement.

IT administrators should be aware of a key technical limitation. SPAs utilize same-document navigations, which cannot be paused for a security scan like a standard page load.

Consequently, there may be a brief delay before a watermark appears after navigating within an SPA. Additionally, DLP rules set to *Warn* or *Block* will not display an interstitial page for these SPA navigations; the action would only trigger on a full page reload.

- **Chrome 139 on ChromeOS, Linux, macOS, Windows:** This rollout adds support for watermarking on Single Page Applications (SPAs)

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

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](#).

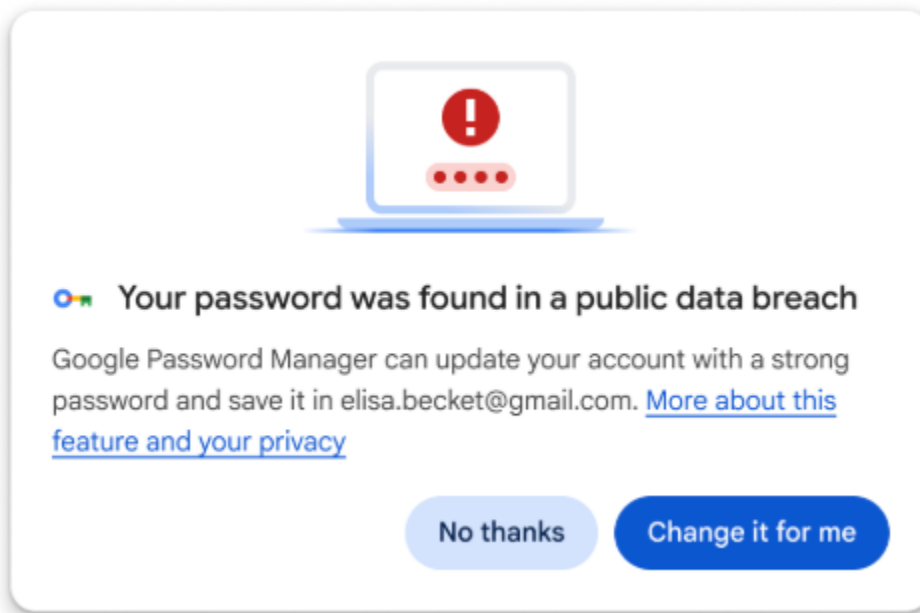
- Chrome 137 on ChromeOS, Linux, macOS, Windows: 2SV enforcement starts
- **Chrome 140 on ChromeOS, Linux, macOS, Windows: 2SV mandatory**

Automated password change

When Chrome detects that a user has signed into a website with a known compromised password, it will offer the user to change it automatically. This feature will be available on a set of eligible sites. The feature uses AI, and can be controlled via the Enterprise policy

AutomatedPasswordChangeSettings.

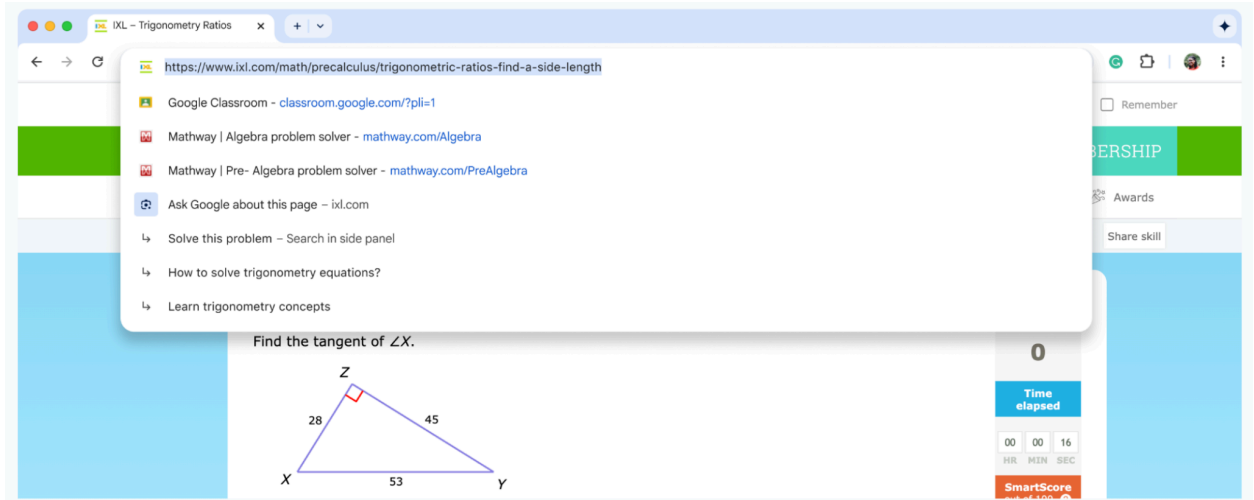
- **Chrome 140 on ChromeOS, Linux, macOS, Windows**



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. This feature is gated by 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.



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, with which users can interact with Gemini via voice.

In Chrome 140, [Gemini in Chrome](#) will become 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.

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 140 on Android, ChromeOS, Linux, macOS, Windows**

Launch Chrome into new profile via command line

This enhancement addresses a critical gap for our enterprise partners and admin who need to launch web applications from their native app catalogs directly into a specific managed Chrome profile using Chrome CLI (command line interface). Currently, if the designated profile does not exist, Chrome defaults to the last-used profile, creating a disjointed and insecure user experience. With this new feature, when a specified profile is not found, Chrome will initiate 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**

PostQuantum cryptography for DTLS in WebRTC

This feature enables 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 150.

- **Chrome 140 on Android, ChromeOS, Linux, macOS, Windows, Fuchsia**
- Chrome 150 on Android, ChromeOS, Linux, macOS, Windows, Fuchsia: Remove Enterprise Policy

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.

A temporary enterprise policy called **ServiceWorkerAutoPreloadEnabled** will be added to control this feature.

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

CSS find-in-page highlight pseudos

Exposes 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 UA defaults have insufficient contrast with the page colors or are otherwise unsuitable.

- **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. These special rules are deprecated, because they cause accessibility issues. Namely, they visually reduce the font size for nested <h1>s so that they "look" like <h2>s, 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**

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 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, we propose to introduce a delayed IP sampling mechanism called Probabilistic Reveal Tokens (PRTs) alongside IP Protection for use in protected traffic.

PRTs will be 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 will contain 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**

Propagate Viewport overscroll-behavior from Root

This feature will propagate overscroll-behavior from the root instead of the body. The [CSS working group resolved](#) on not propagating properties from the body to the viewport. Rather, properties of the viewport are to be propagated from the root element e.g. [scroll-behavior](#), [scroll-snap-type](#), [scroll-padding](#). As such, overscroll-behavior should be propagated from the root element. However, Chrome has had a longstanding issue of propagating overscroll-behavior from the body rather than the root, which deviates from the behavior of Safari(WebKit) and Firefox(Gecko). This feature intends to fix this by propagating overscroll-behavior from the root rather than the body.

- **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 will block 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 will check network requests against the blocklist. The Chromium's subresource_filter component will be 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 script inherit controller for blob script 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**

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 140 on Windows, macOS, Linux, Android**

Web App Manifest: specify update eligibility, icon URLs are Cache-Control: immutable

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

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. Clear the `window.name` property in this case addresses 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**

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**

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*`, 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

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

Inactive profile deletion in Chrome Enterprise Core

In June 2025, the inactive period for profile deletion setting started to roll out. In August 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 140 on Android, ChromeOS, Linux, macOS, Windows:** Policy was rolled out in June. Deletion will start in August and the initial wave of deletion will complete by the

beginning of September. After the initial deletion rollout, inactive profiles will continue to be deleted once they have reached their inactivity period.

Chrome Enterprise Overview page

This feature is introducing 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
- **Chrome 141 on Android, iOS, Linux, macOS, Windows:** New filtering available on the Overview page for Organization Unit and Activity Dates

Upcoming Chrome Enterprise Premium updates

Increased file size support for Data Loss Prevention 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 should 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 end-user productivity.

- **Chrome 140 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.
- **Chrome 141 on ChromeOS, Linux, macOS, Windows:** As an enhancement, a new chrome:// enterprise page is introduced that allows administrators to preview their configured watermark style before deployment.

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

Previous release notes

Chrome version & targeted Stable channel release date
Chrome 138: June 18, 2025
Chrome 137: May 20, 2025
Chrome 136: April 23, 2025
Chrome 135: March 26, 2025
Archived release notes

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.