



Chrome 138 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 June 18, 2025.

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

Chrome 138 release summary	2
Current Chrome browser updates	6
Current Chrome Enterprise Core updates	18
Current Chrome Enterprise Premium updates	22
Coming soon	29
Upcoming Chrome browser updates	29
Upcoming Chrome Enterprise Core updates	40
Upcoming Chrome Enterprise Premium updates	41
Previous release notes	44
Additional resources	45
Still need help?	45

Chrome 138 release summary

Current Chrome browser updates	Security / Privacy	User productivity / Apps	Management
AI Mode for search recommendations in Chrome		✓	
Bookmarks and reading list improvements on Chrome Desktop	✓	✓	
Client's LLM assistance in mitigating scams	✓		
Contextual search suggestions in Chrome Address bar		✓	
Enhanced Safe Browsing is a synced setting	✓		
Generating insights for Chrome DevTools console warnings and errors			✓
History sync opt-in via profile pill	✓		
New tab page footer	✓	✓	✓
Per-extension user script toggle	✓		
Removal of Private Network Access enterprise policies	✓		
Search your screen with Google Lens on iPad		✓	
Shared tab groups		✓	
Speculation rules prefetch for ServiceWorker		✓	
TLS 1.3 Early Data		✓	

Deprecate asynchronous range removal for Media Source extensions	✓		
Language Detector API		✓	
Summarizer API		✓	
Translator API		✓	
Web serial over Bluetooth on Android		✓	
New policies in Chrome browser			✓
Removed policies in Chrome browser			✓
Chrome Enterprise Core	Security / Privacy	User productivity / Apps	Management
Agentspace recommendations in the Chrome search bars		✓	✓
Deprecation of the Chrome browser page on the Chrome Insights report			✓
Inactive profile deletion in Chrome Enterprise Core	✓		✓
Multiple identity support on iOS		✓	
New LayerX risk assessment in the Admin console	✓		
Chrome Enterprise Premium	Security / Privacy	User productivity / Apps	Management
SecOps integration	✓		✓
DLP download support for File System Access API (FSA)	✓		✓
URL Filtering capabilities on iOS	✓		✓
Upcoming Chrome browser updates	Security / Privacy	User productivity / Apps	Management
Chrome on Android no longer supports Android Oreo or Android Pie			✓
Gemini in Chrome		✓	
Malicious APK download checks	✓		

Upcoming change for CA certificates included in the Chrome Root Store	✓		
Migrate extensions to Manifest V3 before June 2025	✓	✓	✓
Promotional notifications			✓
Remove risky extension flags in Google Chrome	✓		
Remove SwiftShader fallback	✓		
Support accounts in pending state on Chrome iOS	✓		
Chrome to remove support for macOS 11		✓	
Clear window name for cross-site navigations that switches browsing context group			✓
Fire error event instead of throwing exception for CSP blocked worker			✓
Web App Manifest: specify update eligibility, icon urls are Cache-Control: immutable		✓	
2SV enforcement for admins			✓
Happy Eyeballs V3		✓	
Isolated Web Apps		✓	
Disallow non-trustworthy plaintext HTTP prerendering	✓		
HSTS tracking prevention	✓		
IP Protection	✓		
Strict Same Origin Policy for Storage Access API	✓	✓	
Disallow spaces in non-file:// URL hosts			✓
SafeBrowsing API v4 → v5 migration	✓		

UI Automation accessibility framework provider on Windows		✓	
Upcoming Chrome Enterprise Core updates	Security / Privacy	User productivity / Apps	Management
New remote commands and CSV export for the Managed Profile list			✓
New tab page cards for Microsoft 365		✓	✓
Chrome Enterprise Overview page			✓
Upcoming Chrome Enterprise Premium updates	Security / Privacy	User productivity / Apps	Management
Chrome browser rule UX refactor	✓		✓
Copy and paste rules protection	✓		✓

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.

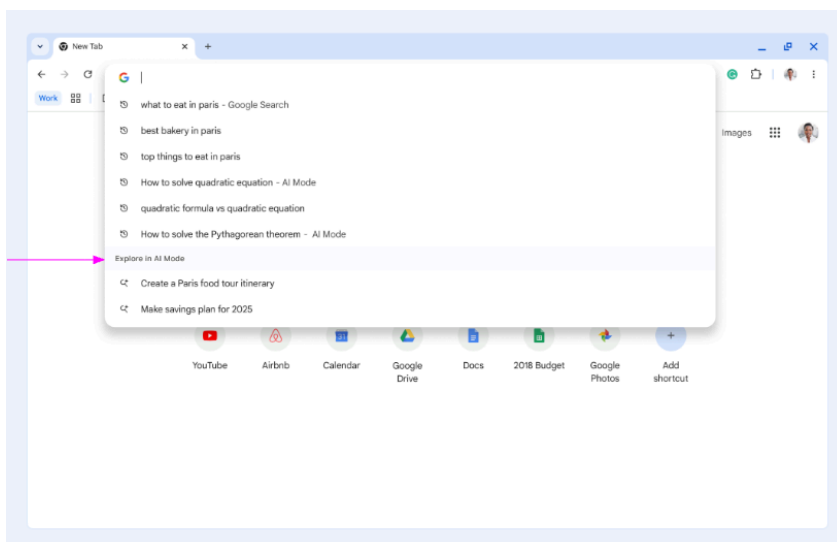
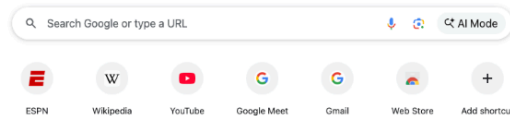
Chrome Enterprise and Education release notes are published in line with the [Chrome release schedule](#), on the Early Stable date for Chrome browser.

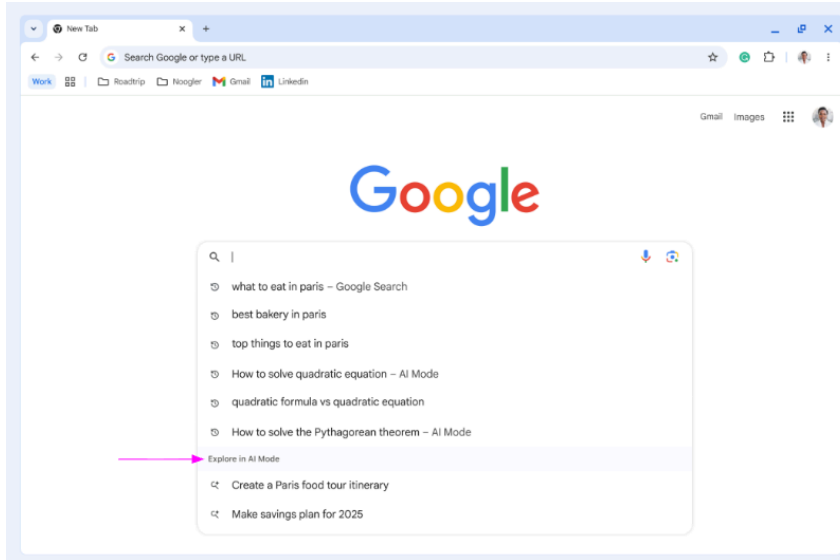
Current Chrome browser updates

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.

- **Chrome 138 on ChromeOS, Linux, macOS, Windows:** Feature starts rollout in the address bar.
- Chrome 139 on Android, iOS: Feature starts rollout in the address bar.





Bookmarks and reading list improvements on Chrome Desktop

For Chrome 138 on Desktop, some users who sign in to Chrome upon saving a new bookmark can now use and save bookmarks and reading list items in their Google Account. Relevant enterprise policies controlling bookmarks, as well as [BrowserSignin](#), [SyncDisabled](#) or [SyncTypesListDisabled](#), continue to work as before, so admins can configure whether or not users can use and save items in their Google Account. Setting [EditBookmarksEnabled](#) to false also prevents users from uploading a bookmark saved on their device to their Google Account.

- **Chrome 138 on Linux, macOS, Windows**

Client's LLM assistance in mitigating scams

Users on the web are facing significant amounts of different kinds of scams a day. To combat these scams, Chrome now uses on-device LLM to identify scam websites for Enhanced Safe Browsing users. Chrome sends the page content to an on-device LLM to infer security-related signals of the page and send these signals to the Safe Browsing server for a final verdict. When enabled, Chrome can consume more bandwidth to download the LLM.

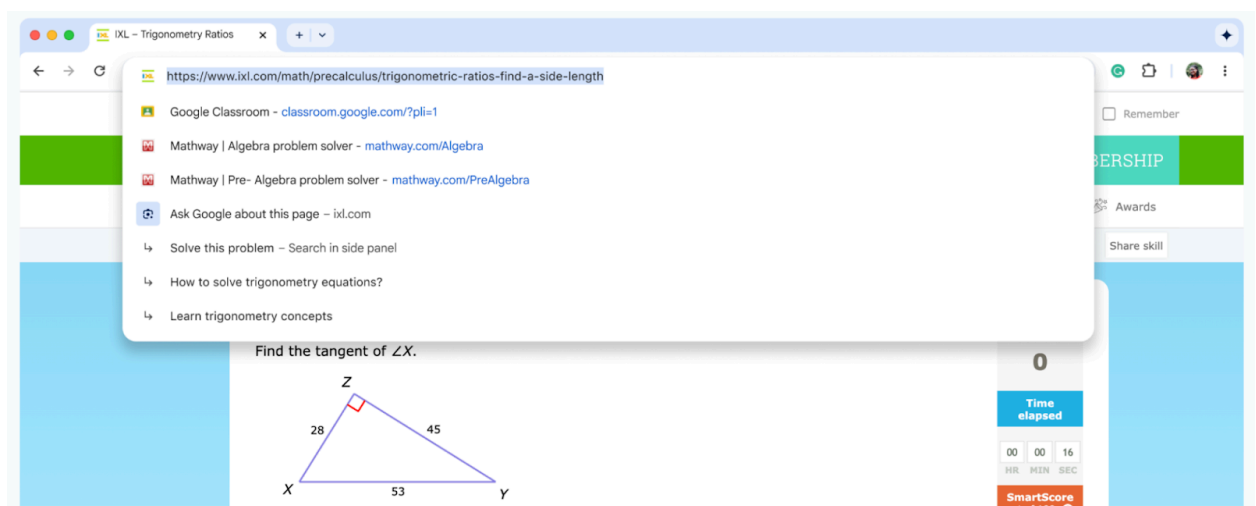
Enhanced Safe Browsing is an existing feature, controlled by the [SafeBrowsingProtectionLevel](#) policy.

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

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 Safe Browsing is a synced setting

In Chrome 138, Chrome's Enhanced Safe Browsing is a synced feature. This means that if a user opts into Enhanced Safe Browsing on one device, this protection level automatically applies across all other devices where they are signed into Chrome with the same account. The goal is to provide stronger, more consistent security protection and a standardized user experience.

Users who enable Enhanced Safe Browsing benefit from its protections, for example, proactive phishing protection, improved detection of malware and malicious extensions) consistently across their synced Chrome instances on Desktop (Windows, macOS, Linux, ChromeOS), Android, and iOS.

Users receive onscreen notifications when their Enhanced Safe Browsing setting is synced.

The Safe Browsing protection level is an existing feature, controlled by the [SafeBrowsingProtectionLevel](#) policy.

- **Chrome 138 on Android, ChromeOS, Linux, macOS, Windows**

Generating insights for Chrome DevTools console warnings and errors

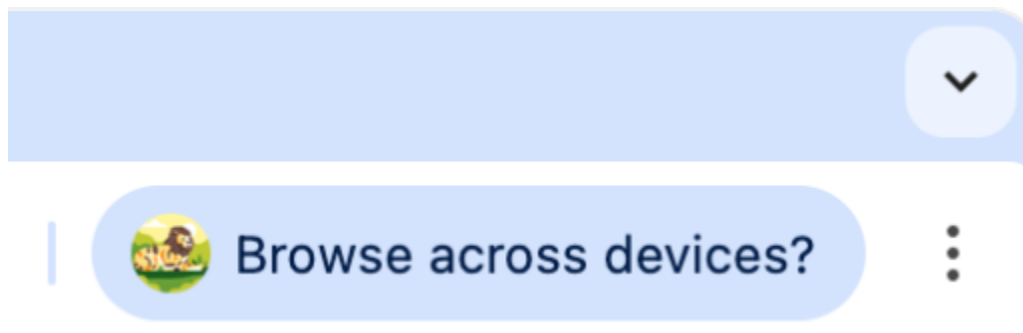
A new Generative AI (GenAI) feature is now available for unmanaged users: Generating insights for Chrome [DevTools console warnings and errors](#). These insights provide a personalized description and suggested fixes for the selected errors and warnings. Initially, this feature is available to users (18+) in English only. Admins can control this feature using the [DevToolsGenAiSettings](#) policy.

- **Chrome 131 on ChromeOS, Linux, macOS, Windows:** In Chrome 131, a new Generative AI (GenAI) feature becomes available for managed users: a dedicated *AI assistance* panel in Chrome DevTools which assists the human operator investigating & fixing styling challenges and helps debugging the CSS.
- **Chrome 132 on ChromeOS, Linux, macOS, Windows:** The AI assistance panel can now explain resources in the Performance panel, Sources panel, and Network panel, in addition to the previous support for style debugging.
- **Chrome 138 on ChromeOS, Linux, macOS, Windows:** The AI assistance panel exposes an internal API that simplifies the use of AI assistance panel features by external tools such as Model Context Protocol (MCP) servers.

History sync opt-in using the profile pill

In Chrome 138, some signed-in users see a new option to opt-in to history and tab sync. This change is designed to offer the benefits of history sync in a non-disruptive way by using the profile pill to display a short in-line message. Users who click on the profile pill are taken to their profile menu where they can choose to turn on sync. The goal is to provide users with an intuitive and contextually relevant entry point for syncing data like browsing history, separate from the sign-in flow. For Enterprise users, the expanded profile pill only appears after 4 hours of browser inactivity. Relevant enterprise policies controlling History or Tab sync ([SyncDisabled](#), [SyncTypesListDisabled](#) and [SavingBrowserHistoryDisabled](#)) continue to work as before.

- **Chrome 138 on Linux, macOS, Windows:** Feature starts gradual roll-out



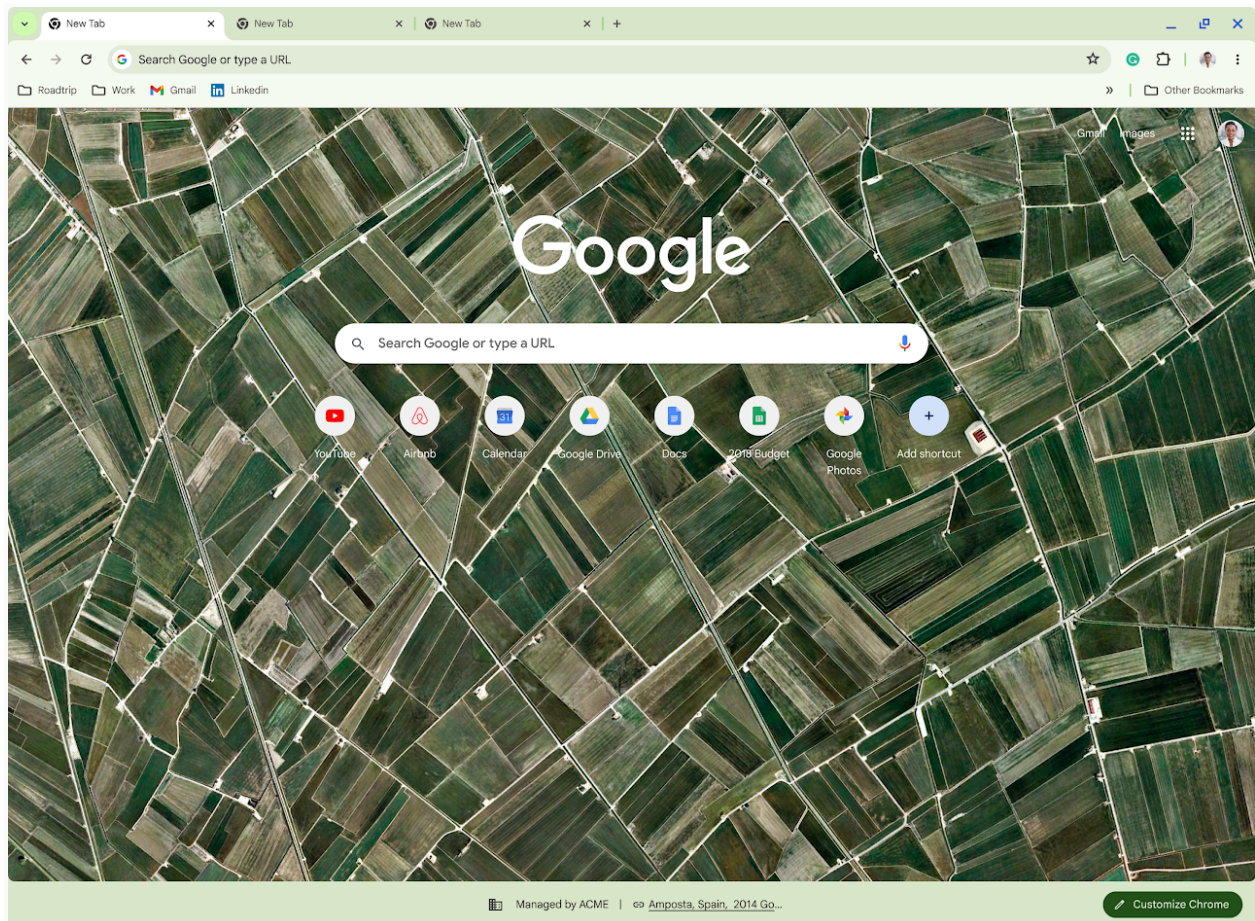
New tab page footer

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.



Per-extension user script toggle

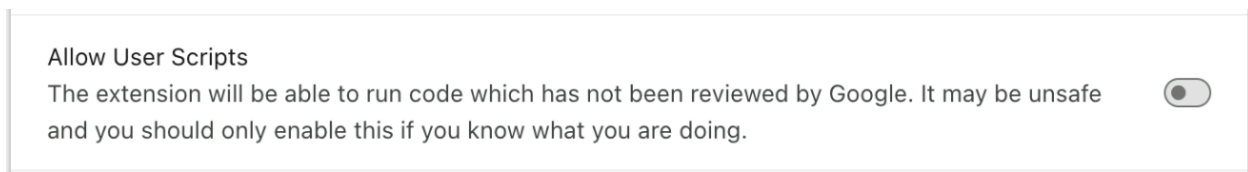
In Chrome 138, the way that users and administrators control an extension's ability to run user created scripts and use the [userScripts API](#) is changing. This change enhances security. End-users won't unintentionally grant user script permissions to every extension when enabling **Developer mode** by explicitly deciding which extensions can run these potentially powerful scripts. For more detail on the motivation for the change, see this [Chrome for developers](#) blog.

End users will now toggle this per extension on the `chrome://extensions` page via a **Allow User Scripts** toggle, replacing the global **Developer mode** toggle for more granular control. Existing extensions will have this toggle automatically enabled if **Developer mode** is on and the extension has been granted the User Scripts permission.

Administrators who currently manage user scripts by disabling developer mode should now use the [blocked_permissions field of the ExtensionSettings policy](#) or the [Google Admin console](#) to independently control the User Scripts permission and extension **Developer mode**.

Extension developers are advised to update their documentation to reflect the new toggle. See the [Chromium Extensions Google Groups](#) mailing list for more information and other changes to usage of the API.

- **Chrome 138 on ChromeOS, Linux, macOS, Windows:** Feature rolls out



Removal of Private Network Access enterprise policies

Private Network Access (PNA 1.0) is an unshipped security feature designed to limit website access to local networks. Due to deployability concerns, PNA 1.0 was never able to ship by default, as it was incompatible with too many existing devices.

PNA 1.0 required changes to devices on local networks. Instead, Chrome is implementing an updated proposal, Private Network Access 2.0 (PNA 2.0) ([Github](#)). PNA 2.0 only requires changes to sites that need to access the local network, rather than requiring changes to devices on the local

network. Sites are much easier to update than devices, and so this approach should be much more straightforward to roll out.

The only way to enforce PNA 1.0 is via enterprise policy. To avoid regressing security for enterprise customers opting-in to PNA 1.0 prior to shipping PNA 2.0, we will maintain the [PrivateNetworkAccessRestrictionsEnabled](#) policy, which causes Chrome to send special preflight messages, until such time that it becomes incompatible with PNA 2.0.

The [InsecurePrivateNetworkRequestsAllowedForUrls](#) and [InsecurePrivateNetworkRequestsAllowed](#) policies, which loosen PNA 1.0 restrictions, will be removed immediately. These policies currently have no effect, since PNA 1.0 is not shipped, and they will have no meaning once PNA 1.0 is removed.

- **Chrome 135 on Android, ChromeOS, Linux, macOS, Windows, Fuchsia:** Deprecate [InsecurePrivateNetworkRequestsAllowedForUrls](#), [InsecurePrivateNetworkRequestsAllowed](#), and [PrivateNetworkAccessRestrictionsEnabled](#) policies.
- **Chrome 138 on Android, ChromeOS, Linux, macOS, Windows, Fuchsia:** Removal of [PrivateNetworkAccessRestrictionsEnabled](#), [InsecurePrivateNetworkRequestsAllowedForUrls](#) and [InsecurePrivateNetworkRequestsAllowed](#). There should be a PNA2 replacement policy available in Chrome 138.

Search your screen with Google Lens on iPad

Expand **Search your screen with Google Lens** on iOS so it is available on iPad devices. iPad is a form factor typically associated with more complex tasks, for example, shopping, and expanding Lens functionality on iPad enables users to perform these tasks easily. Admins can control this feature using the [LensOverlaySettings](#) policy.

- **Chrome 138 on iOS:** Feature rolls out gradually.

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`, is available 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

Speculation rules prefetch for ServiceWorker

This feature enables Service Worker-controlled prefetches, that is, a speculation rules prefetch to URLs controlled by a Service Worker. Previously, the prefetch is cancelled upon detecting a controlling Service Worker, thus subsequent navigation to the prefetch target is served by the non-prefetch path. This feature enables the prefetch request to go through the Service Worker's fetch handler and the response with the Service Worker interception is cached in the prefetch cache, resulting in a subsequent navigation being served by the prefetch cache. Please use the enterprise policy [PrefetchWithServiceWorkerEnabled](#) to control this feature. For more details, see [this](#) explainer.

- **Chrome 138 on Android, ChromeOS, Linux, macOS, Windows**

TLS 1.3 Early Data

TLS 1.3 Early Data allows GET requests to be sent during the handshake when resuming a connection to a compatible TLS 1.3 server. The feature is expected to demonstrate performance improvements and will be available in Chrome 138 with a policy ([TLS13EarlyDataEnabled](#)) to control this change.

TLS 1.3 Early Data is an established protocol. Existing TLS servers, middleboxes, and security software are expected to either handle or reject TLS 1.3 Early Data without dropping the connection. However, devices that do not correctly implement the TLS standard (RFC8446) might malfunction and disconnect when TLS 1.3 Early Data is in use. If this occurs, administrators should contact the vendor for a fix.

The [TLS13EarlyDataEnabled](#) policy is a temporary measure to control the feature and will be removed in a future milestone. You can turn on the feature using the policy to allow you to test for issues and turn it off again as issues are resolved.

- **Chrome 138 on Android, ChromeOS, Linux, macOS, Windows**

Deprecate asynchronous range removal for Media Source extensions

The [Media Source standard](#) changed in the past to disallow ambiguously-defined behavior involving asynchronous range removals:

- `SourceBuffer.abort()` no longer aborts `SourceBuffer.remove()` operations
- Setting `MediaSource.duration` can no longer truncate currently buffered media

Exceptions are thrown in both of these cases now. Safari and Firefox have long shipped this behavior; Chromium is the last browser remaining with the old behavior. Use counters show ~0.001%-0.005% of page loads hit the deprecated behavior. If a site hits this issue, playback may now break. Usage of `abort()` cancelling removals is increasing, so it's prudent to resolve this deprecation before more incompatible usage appears.

- **Chrome 138 on Windows, macOS, Linux, Android**

Language Detector API

Language Detector API is a JavaScript API for detecting the language of text, with confidence levels. An important supplement to translation is language detection. This can be combined with translation, for example, taking user input in an unknown language and translating it to a specific target language. Browsers today often already have language detection capabilities, and we want to offer them to web developers through a JavaScript API, supplementing the translation API. An enterprise policy, [GenAI Local Foundational Model Settings](#), is available to disable the underlying model downloading, which would render this API unavailable.

- **Chrome 138 on Windows, macOS, Linux**

Summarizer API

Summarizer API is a JavaScript API for producing summaries of input text, backed by an AI language model. Browsers and operating systems are increasingly expected to gain access to a language model. By exposing this built-in model, we avoid every website needing to download their own multi-gigabyte language model, or send input text to third-party APIs. The Summarizer API, in particular, exposes a high-level API for interfacing with a language model to summarize inputs for a variety of use cases ([Github](#)), in a way that does not depend on a specific language model. An enterprise policy ([GenAILocalFoundationalModelSettings](#)) is available to disable the underlying model downloading, which would render this API unavailable.

- **Chrome 138 on Windows, macOS, Linux**

Translator API

Translator API is a JavaScript API to provide language translation capabilities to web pages. Browsers are increasingly offering language translation to their users. Such translation capabilities can also be useful to web developers. This is especially the case when the browser's built-in translation abilities cannot help. An enterprise policy, [GenAILocalFoundationalModelSettings](#), is available to disable the underlying model downloading, which would render this API unavailable.

- **Chrome 138 on Windows, macOS, Linux**

Web serial over Bluetooth on Android

This feature allows web pages and web apps to connect to serial ports over Bluetooth on Android devices. Chrome on Android now supports Web Serial API over Bluetooth RFCOMM. Existing enterprise policies ([DefaultSerialGuardSetting](#), [SerialAllowAllPortsForUrls](#), [SerialAllowUsbDevicesForUrls](#), [SerialAskForUrls](#) and [SerialBlockedForUrls](#)) on other platforms are enabled in future_on states for Android. All policies except [SerialAllowUsbDevicesForUrls](#) will be enabled after the feature is enabled. [SerialAllowUsbDevicesForUrls](#) will be enabled in a future launch after Android provides system level support of wired serial ports.

- **Chrome 138 on Android**

New policies in Chrome browser

Policy	Description
AIModelSettings	Settings for Google's AI Mode integrations in the address bar and New Tab page search box.
PdfAnnotationsEnabled	Enable PDF Annotations.
TLS13EarlyDataEnabled	Enable TLS 1.3 Early Data.
NTPFooterExtensionAttributionEnabled	Control the visibility of the extension attribution on the New tab page
PrefetchWithServiceWorkerEnabled	Allow SpeculationRules prefetch to ServiceWorker-controlled URLs.
EnterpriseRealTimeUrlCheckMode	Check Safe Browsing status of URLs in real time.
LocalNetworkAccessRestrictionsEnabled	Apply restrictions to requests to local network endpoints.
PrivacySandboxIpProtectionEnabled	Choose whether the IP Protection feature should be enabled.
PasswordManagerBlocklist	Configure the list of domains for which the Password Manager will be disabled.

Removed policies in Chrome browser

Policy	Description
PrivateNetworkAccessRestrictionsEnabled	Apply restrictions to requests to more-private network endpoints.
InsecurePrivateNetworkRequestsAllowed	Allow websites to make requests to more-private network endpoints in an insecure manner.
InsecurePrivateNetworkRequestsAllowedForUrls	Allow the listed sites to make requests to more-private network endpoints in an insecure manner.

Current Chrome Enterprise Core updates

Agentspace recommendations in Chrome search bars

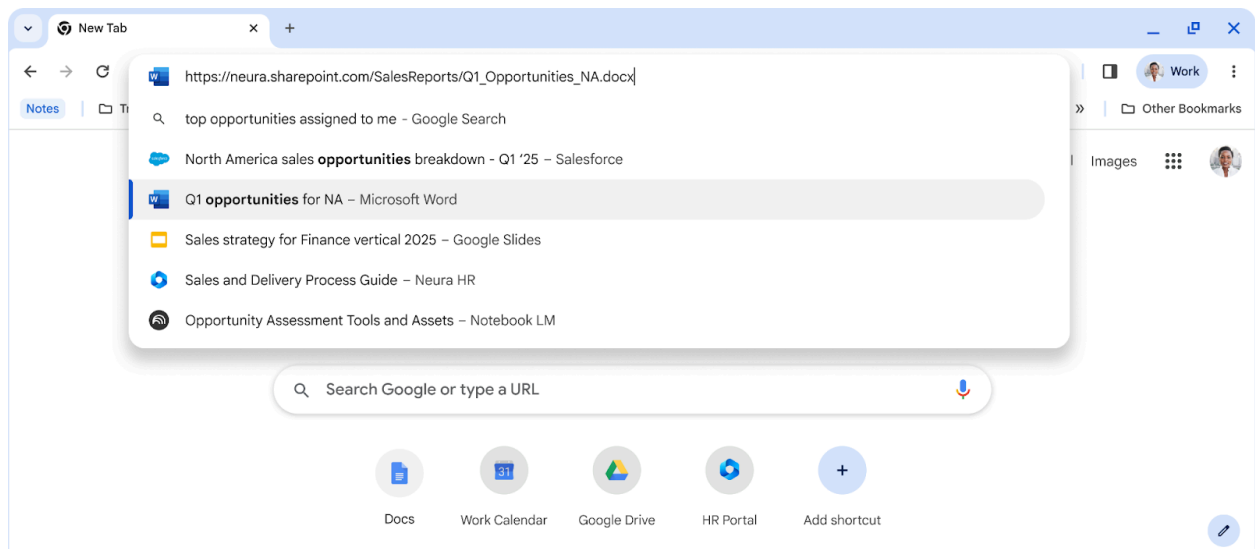
To help enterprise users with their internal information needs, you can now add enterprise search results, such as people, file, or query suggestions, from [Agentspace](#) to the Chrome address bar and realbox (search bar on the **New tab** page). Results can be shown by default or only when triggered by a custom keyword.

With keyword mode in the address bar, users can trigger actions through Agentspace, such as, "help me write an email that summarizes the current project status".

The enterprise search provider is shown when the user types @ in the address bar. The organization can customize a keyword or shortcut and the icon shown.

This can be configured via the [EnterpriseSearchAggregatorSettings](#) policy.

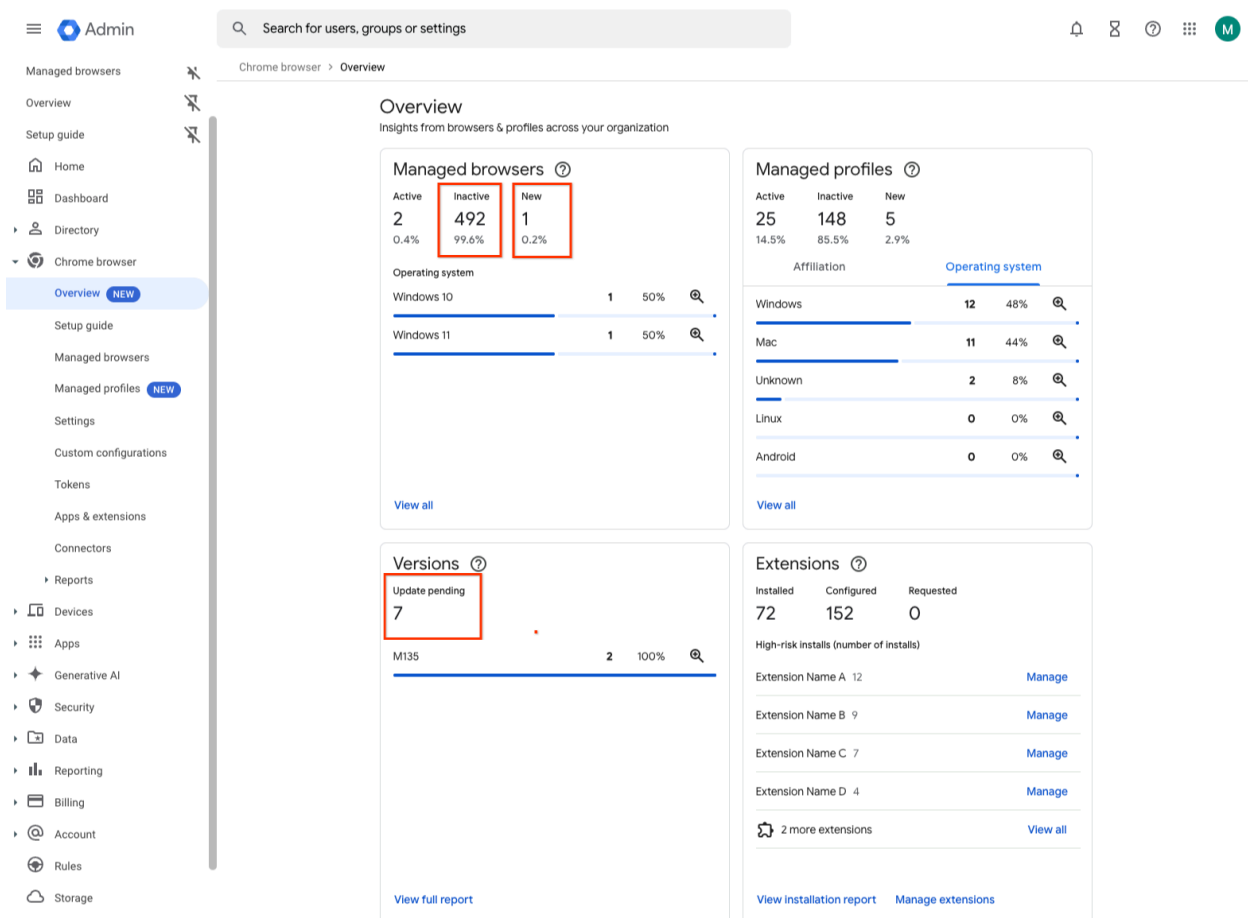
- Chrome 135 on ChromeOS, Linux, macOS, Windows: Trusted Tester
- **Chrome 138 on ChromeOS, Linux, macOS, Windows: General Availability**



Deprecation of the Chrome browser page on the Chrome Insights report

As early as July 1st, the Chrome browser page on the Chrome Insights report will be deprecated. This page is replaced by the Chrome **Overview** page that was launched in Chrome 137. The information, which was displayed on the Chrome browser page of the Chrome Insights report, can now be found on the **Overview** page.

- **Chrome 138 on Android, iOS, Linux, macOS, Windows**



Inactive profile deletion in Chrome Enterprise Core

In June 2025, the inactive period for profile deletion setting started to roll out. In July 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 you lower the set value, 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 re-activated on a device, that profile will reappear in the console.

- **Chrome 138 on Android, ChromeOS, Linux, macOS, Windows:** Policy will roll out in June. Deletion will start in July and the initial wave of deletion will complete by the end of August. After the initial deletion rollout, inactive profiles will continue to be deleted once they have reached their inactivity period.

New LayerX risk assessment in the Admin console

We are adding a new extension risk assessment provider: LayerX Security to the Admin console. This score is available to Admins in the Apps and Extensions Usage report.

- **Chrome 138 on ChromeOS, Linux, macOS, Windows:** The score would be available to admins as early as Chrome 138.

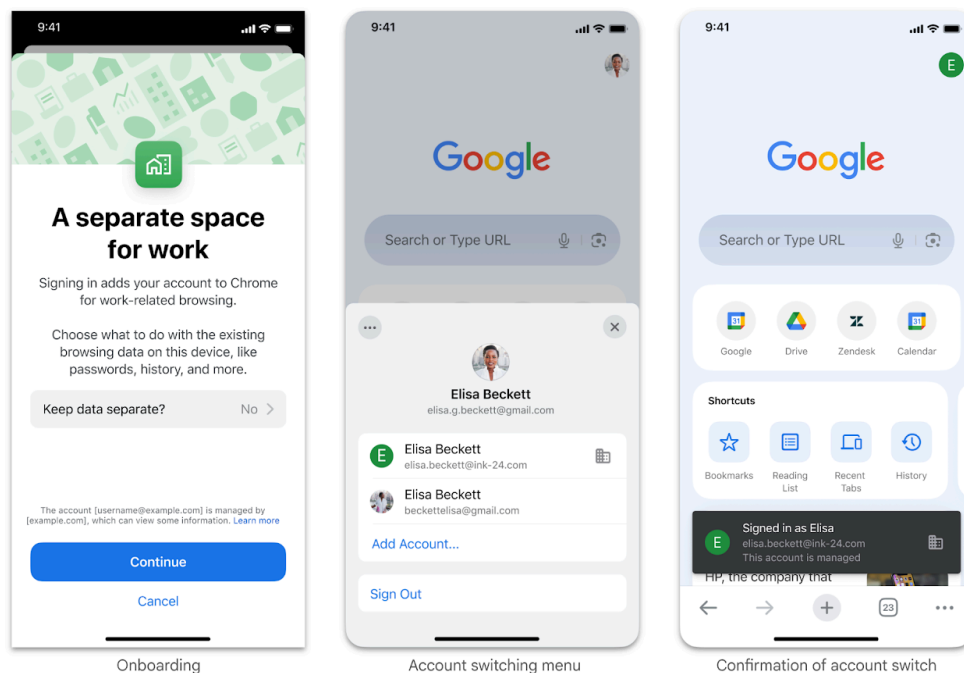
App name	App type	Install type	Chrome Web Store	Installs ↓	Permissions	Risk score									
 Application Launcher For Driv...	Chrome Extension	Sideload	Published	2	4	 Low									
<table><tr><th>Provider</th><th>Score</th><th>Version</th></tr><tr><td>LayerX</td><td> 1.5/10</td><td>3.10</td></tr><tr><td>Spin.AI</td><td> 71/100</td><td>3.10</td></tr></table>							Provider	Score	Version	LayerX	 1.5/10	3.10	Spin.AI	 71/100	3.10
Provider	Score	Version													
LayerX	 1.5/10	3.10													
Spin.AI	 71/100	3.10													
These scores are provided by 3rd party companies. Google makes no guarantees about data provided by 3rd party companies. Learn more															

Multiple identity support on iOS

Chrome on iOS now supports multiple accounts, particularly for managed (work or school) accounts. This update introduces separate browser profiles for each managed account, ensuring strict data separation between work and personal browsing. Regular accounts continue to share a single profile.

This change aims to improve Chrome's enterprise offering and provide a more secure and organized browsing experience, especially for end users with both personal and work accounts on their device. Users experience a one-time onboarding flow when adding a managed account to the device. They can switch between accounts by tapping on the account particle disk on the **New tab** page. Admins who enabled Chrome policies on iOS ([see instructions](#)) can continue to use existing policies.

- **Chrome 138 on iOS**



Current Chrome Enterprise Premium updates

SecOps integration

This feature delivers a native integration between Chrome Enterprise Premium (CEP) and Google Security Operations (SecOps), enabling organizations to send a richer set of security events and detailed browser telemetry from Chrome directly to their SecOps instance. The motivation for this change is to use the browser as a primary security sensor for web-based threats like phishing, malware, and data exfiltration. This can significantly improve an organization's ability to:

- prevent
- detect
- investigate
- and respond to web-based threats.

For administrators, this integration introduces new, enhanced security event types, including URL navigation telemetry and suspicious URL visits. These events are automatically enriched with Safe Browsing risk scores and other threat intelligence before being sent to SecOps. The launch also includes a new, streamlined "one-click" setup process in the Admin console to replace the previous manual workflow, simplifying the connection to SecOps.

To use this feature, administrators must have a Chrome Enterprise Premium subscription and will need to enable the integration through the new workflow in the Admin console. The collection of certain high-volume event types, such as URL navigation events, is an opt-in setting within the connector configuration. This feature does not add or modify any enterprise policies.

- **Chrome 137 on Linux, macOS, Windows:** Adds referrer data to `URLFilteringInterstitialEvent` and `SafeBrowseInterstitialEvent`
- **Chrome 138 on Linux, macOS, Windows:** Extends referrer data population to `SafeBrowseDangerousDownloadEvent` and `DlpSensitiveDataEvent`

URL Filtering capabilities on iOS

The current WebProtect URL Filtering capabilities on Desktop are being extended to mobile so that organizations can audit, warn, or block certain URLs or categories of URLs from loading on managed

Chrome browsers or managed user profiles on mobile devices. This feature is part of Chrome Enterprise Premium and aims to provide secure and safe internet access for enterprise users on any device. Admins can create URL filtering rules to ensure that employees can only access safe and authorized URLs on iOS devices. Chrome reports URL filtering events and unsafe site events via the Reporting Connector on mobile. This feature allows administrators to manage which URLs can be accessed on managed Chrome browsers or profiles on company-owned or BYOD iOS devices.

Key changes include:

- Admins can block, warn, or audit users when accessing certain sites or categories.
 - Users see interstitial pages when attempting to visit blocked or warned URLs.
 - Chrome reports URL filtering events.
 - Updates to the `chrome://management` page reflect the new functionality.
-
- **Chrome 138 on iOS:** The URL Filtering feature becomes available on iOS.

Rules

Google protects you by default

With **system defined rules**, you will be notified when important events occur in your organization, like phishing, malware, suspicious activities, and more.

[Learn more](#)

[View list](#)

Collaborate securely

Use **trust rules** to help your users collaborate and flexibly, both inside and outside your orga

[Learn more](#)

[View list](#)

[Create rule](#)

Rules

[Create rule](#)

[Templates](#)

[Investigate](#)

[Download](#)

+ A

Activity

Chrome action

Data protection

Trust

Name

Status

Rule type

?

Actions

Alerts

Last mo

test print

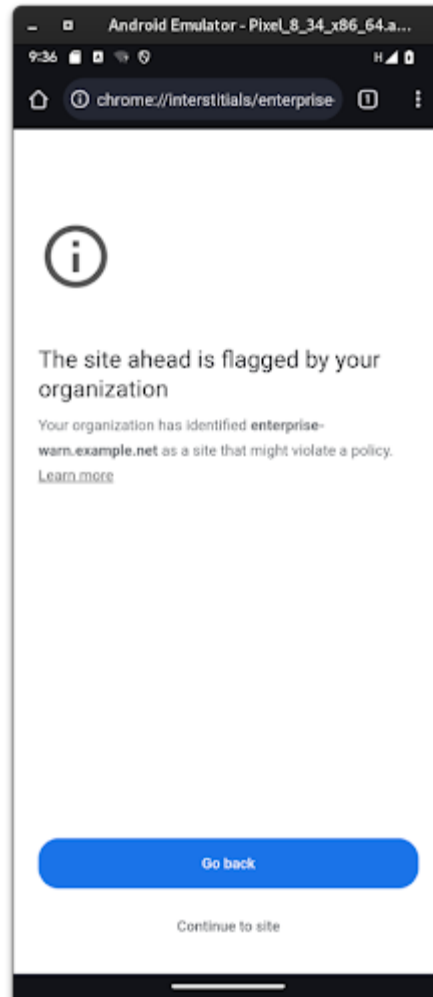
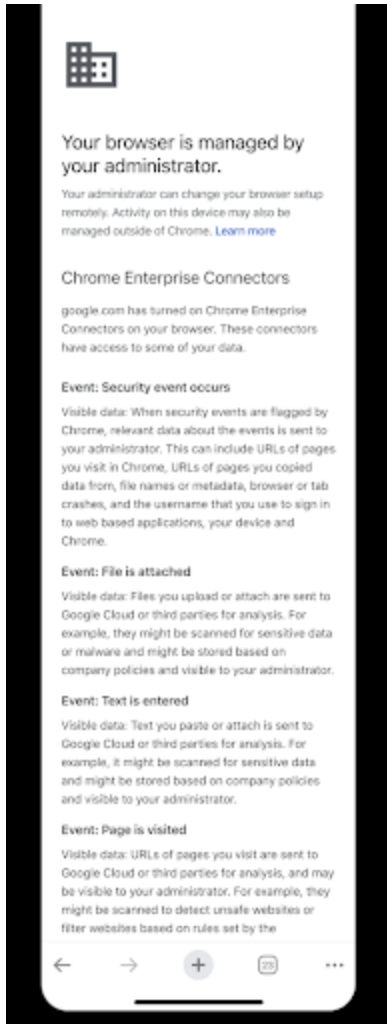
Active

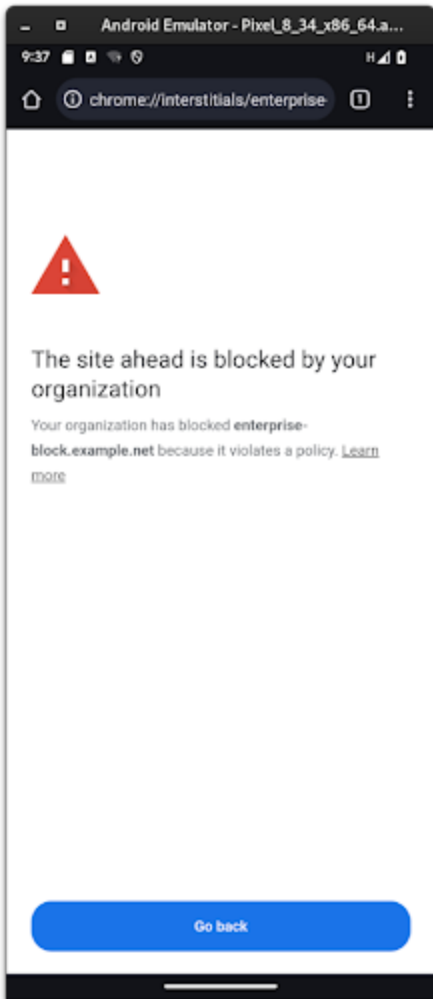
Data protection

Block

Off

5/17/20





✕ CrowdStrike Falcon Next-Gen configuration

Configuration name

new-config

Ingest Token

auheifhewihfheihwiuefhe

Host Name

cloud.google.com

[↻](#) Test connection

Events this configuration is allowed to receive

User & browser events

Default event types [Learn more](#)

Allow all ▾

Optional event types

☒ Login 

☒ Password Breach 

Device events

Default event types [Learn more](#)

Allow all ▾

SAVE CONFIGURATION

CANCEL

× Set up a provider



Google Security Operations

 Reporting

[SET UP](#) [LEARN MORE](#) 



Google Cloud Pub/Sub

 Reporting

[SET UP](#) [LEARN MORE](#) 



Splunk

 Reporting

[SET UP](#) [LEARN MORE](#) 



CrowdStrike Falcon Next-Gen

 Reporting

[SET UP](#) [LEARN MORE](#) 

DLP Download Support for File System Access API (FSA)

Data Loss Prevention (DLP) protection now covers files and directories downloaded using the [File System Access \(FSA\) API](#). This enhancement ensures that downloads from modern web applications, such as browser-based editors, are scanned according to your organization's DLP rules. Users and websites receive notifications on scan verdicts, strengthening data security and compliance. If a download violates a DLP policy, it is blocked, resulting in an empty file, and the website might indicate a "Blocked by Safe Browsing" error. This change primarily benefits security by preventing data exfiltration through this vector. Administrators should test this with web applications using the FSA API to observe the behavior with their current DLP configurations.

- **Chrome 138 on ChromeOS, Linux, macOS, Windows:** Enables DLP content analysis for downloads initiated via File System Access API on selected platforms, governed by existing enterprise policies.

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

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 newer 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.

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.

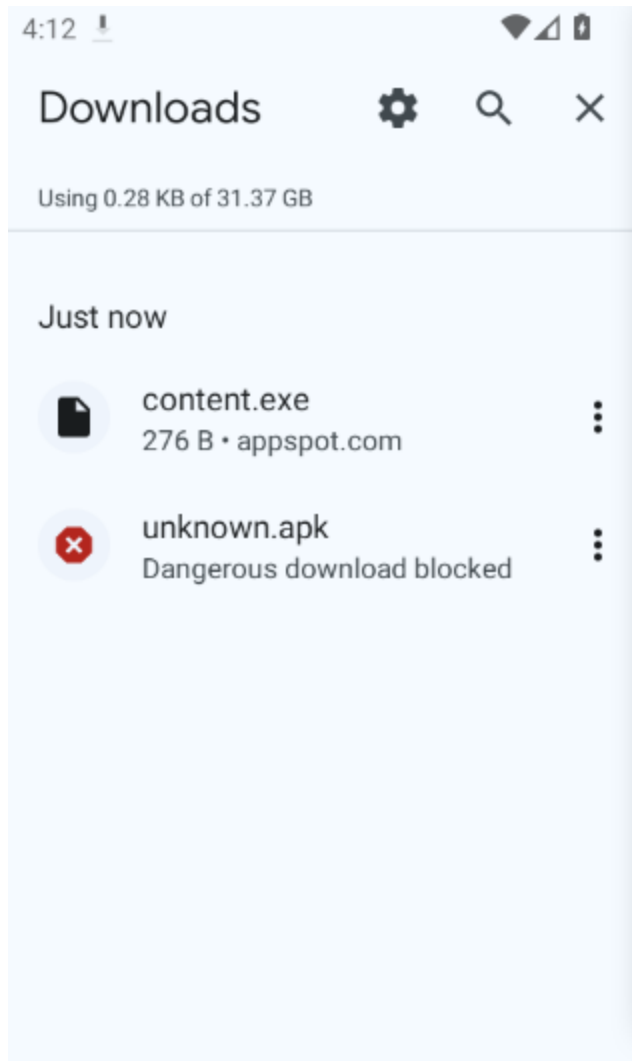
In Chrome 137, [Gemini in Chrome](#) is available for Google AI Pro and Ultra subscribers in the US. A broader rollout will come in future milestones. Admins can turn off this feature (value 1) using the [GeminiSettings](#) policy or by using the [GenAiDefaultSettings](#) (value 2). For more details, 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 139 on macOS, Windows:** Feature gradually rolls out on Stable for users signed into Chrome in the US.

Malicious APK download checks

Chrome on Android will now contact Google servers about APK files downloaded in Chrome, to get a verdict about their safety. If a downloaded APK file is determined to be dangerous, Chrome will show a warning and block the download, to protect users against mobile malware. Such download warnings will be bypassable by the user through the Chrome UI. These malicious APK download checks will be 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" via the [SafeBrowsingProtectionLevel](#) policy.

- **Chrome 139 on Android**



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.

Migrate extensions to Manifest V3 before June 2025

Extensions must be updated to leverage Manifest V3. Chrome extensions are transitioning to a new manifest version, Manifest V3. This will bring 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 will be disallowed on Manifest V3.

Beginning June 2024, Chrome will gradually disable 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 will not be subject to the disabling of Manifest V2 extensions until the following year - June 2025 - at which point the policy will 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.

Promotional notifications

In Chrome 128, new promotional OS-level notifications will be shown to users. These notifications would be governed by the `PromotionalSettings` enterprise policy

- Chrome 128 on ChromeOS, Linux, macOS, Windows
- **Chrome 139 on Windows:** In Chrome 138, promo 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:** Gradual roll-out

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. A temporary enterprise policy will be available in Chrome 138 to revert the change.

- Chrome 137 on Windows: SwiftShader will be disabled and replaced with another software WebGL fallback, WARP. Tests depending on the exact pixel values generated by SwiftShader may start failing.
- **Chrome 139 on Linux, macOS:** Swiftshader will be disabled on macOS and Linux as early as Chrome 138. Users on machines without a GPU will not be able to use WebGL.

Support accounts in pending state on Chrome iOS

Accounts whose credentials somehow became invalid will no longer be automatically signed out and removed from Chrome on iOS. Instead, these accounts will 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 will no longer be automatically deleted, but instead kept on disk. Existing policies controlling sign-in (for example, [BrowserSignin](#)) will continue to work as before.

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

Chrome to remove support for macOS 11

Chrome 138 will be the last release to support macOS 11; Chrome 139+ 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 be updated, they need to update their computer to a support version of macOS. For new installations of Chrome 139+, macOS 12+ will be required.

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

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 142.

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

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**

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

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 [Help Center article](#).

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

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**

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

Disallow non-trustworthy plaintext HTTP prerendering

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

- **Chrome 140 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 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**

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**

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 141 on Android, ChromeOS, LaCrOS, Linux, macOS, Windows, Fuchsia**

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

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

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 will be able to 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 will not need to be signed into Chrome to use this feature

Chrome Enterprise Overview page

This launch 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 140 on Android, iOS, Linux, macOS, Windows:** New filtering available on the Overview page for Organization Unit and Activity Dates

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 139 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

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

Previous release notes

Chrome version & targeted Stable channel release date
Chrome 137: May 20, 2025
Chrome 136: April 23, 2025
Chrome 135: March 26, 2025
Chrome 134: February 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.