



# Chrome 137 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 May 20, 2025.*

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

<b>Chrome 137 release summary</b>	<b>2</b>
Current Chrome browser updates	5
Current Chrome Enterprise Core updates	12
Current Chrome Enterprise Premium updates	14
<b>Coming soon</b>	<b>16</b>
Upcoming Chrome browser updates	16
Upcoming Chrome Enterprise Core updates	26
Upcoming Chrome Enterprise Premium updates	28
<b>Previous release notes</b>	<b>30</b>
<b>Additional resources</b>	<b>31</b>
<b>Still need help?</b>	<b>31</b>

# Chrome 137 release summary

Current Chrome browser updates	Security / Privacy	User productivity / Apps	Management
Gemini in Chrome		✓	
Blob URL Partitioning: Fetching/Navigation	✓		
Client's LLM assistance in mitigating scams	✓		
DTLS 1.3	✓		
Remove --load-extension command line switch in Google Chrome	✓		
Remove SwiftShader fallback	✓		
Customizing managed profiles with custom logo and label			✓
Align error type thrown for <i>payment</i> WebAuthn credential creation: <code>SecurityError =&gt; NotAllowedError</code>	✓		
HSTS tracking prevention	✓		
2SV enforcement for admins	✓		
Autofill with AI		✓	
New policies in Chrome browser			✓
Removed policies in Chrome browser			✓
Chrome Enterprise Core	Security / Privacy	User productivity / Apps	Management
IP Address Logging & Reporting			✓
Chrome Enterprise Overview page			✓

New remote commands and CSV export for the Managed Profile list			✓
New tab page cards for M365		✓	✓
<b>Chrome Enterprise Premium</b>	<b>Security / Privacy</b>	<b>User productivity / Apps</b>	<b>Management</b>
DLP download support for File System Access API (FSA)	✓		✓
Reporting Connector on Mobile	✓		✓
Reporting Safe Browsing events on iOS	✓		
<b>Upcoming Chrome browser updates</b>	<b>Security / Privacy</b>	<b>User productivity / Apps</b>	<b>Management</b>
Bookmarks and reading list improvements on Chrome Desktop	✓	✓	
Per-extension user script toggle			✓
Enhanced Safe Browsing as a synced setting	✓		
Shared tab groups		✓	
Generating insights for Chrome DevTools Console warnings and errors			✓
Removal of Private Network Access enterprise policies	✓		
TLS 1.3 Early Data		✓	
Predictable reported storage quota		✓	
Strict Same Origin Policy for Storage Access API		✓	
Summarizer API		✓	
Language Detector API		✓	
Translator API		✓	
Web serial over Bluetooth on Android			✓
Chrome on Android no longer supports Android Oreo or Android Pie			✓


Migrate extensions to Manifest V3 before June 2025	✓	✓	✓
Chrome will remove support for macOS 11			✓
Happy Eyeballs V3		✓	
Isolated Web Apps	✓		✓
Disallow spaces in non-file:// URL hosts	✓		
SafeBrowsing API v4 → v5 migration	✓		
UI Automation accessibility framework provider on Windows		✓	
<b>Upcoming Chrome Enterprise Core updates</b>	<b>Security / Privacy</b>	<b>User productivity / Apps</b>	<b>Management</b>
AgentSpace recommendations in the Chrome omnibox		✓	✓
Inactive profile deletion in Chrome Enterprise Core	✓		✓
Multiple Identity Support on iOS		✓	
<b>Upcoming Chrome Enterprise Premium updates</b>	<b>Security / Privacy</b>	<b>User productivity / Apps</b>	<b>Management</b>
URL Filtering capabilities on iOS	✓		
DLP Download Support for File System Access API (FSA)	✓		

*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

### 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. You can check the upcoming publications of these Enterprise Release Notes for availability updates.

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:** Feature becomes available for some Google AI Pro and Ultra subscribers in the US and on pre-Stable (Dev, Canary, Beta) channels in the US.
- A broader rollout will come in future milestones. You can check the upcoming publications of the Enterprise Release Notes for availability updates.

### Blob URL Partitioning: Fetching/Navigation

As a continuation of Storage Partitioning, Chrome 137 now implements partitioning of Blob URL access by Storage Key (top-level site, frame origin, and the has-cross-site-ancestor boolean), with the exception of top-level navigations which will remain partitioned only by frame origin. This behavior is similar to what’s currently implemented by both Firefox and Safari, and aligns Blob URL usage with the partitioning scheme used by other storage APIs as part of Storage Partitioning. In addition, Chrome 137 now enforces noopener on renderer-initiated top-level navigations to Blob URLs where the corresponding site is cross-site to the top-level site performing the navigation. This aligns Chrome with similar behavior in Safari, and the relevant specs have been updated to reflect these changes.

This change can be temporarily reverted by setting the [PartitionedBlobURLUsage](#) policy. The policy will be deprecated when the other storage partitioning related enterprise policies are deprecated.

- **Chrome 137** on Android, ChromeOS, 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 leverages 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 Safe Browsing server side for a final verdict. When enabled, Chrome might 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.

### **DTLS 1.3**

Chrome 137 adds support for Datagram Transport Layer Security ([DTLS](#)) 1.3 for Web Realtime Communication ([WebRTC](#)) connections. Previously, DTLS 1.2 was used for all WebRTC connections. This is required to add quantum-resistant cryptography to WebRTC.

- **Chrome 137** on Android, ChromeOS, Linux, macOS, Windows, Fuchsia

## Remove `--load-extension` command line switch in Google Chrome

To enhance the security and stability of the Chrome browser for our users, official Chrome-branded builds now deprecate the ability to load extensions via the `--load-extension` command-line flag, starting in Chrome 137. This change aims to mitigate the risks associated with harmful and unwanted extensions.

Unpacked extensions can be loaded via the **Load Unpacked** button on the extension management page (`chrome://extensions/`) with developer mode enabled. Developers can still use the `--load-extension` switch in non-branded builds such as Chromium and [Chrome For Testing](#).

- **Chrome 137 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. 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 138 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.

## Customizing managed profiles with custom logo and label

Chrome 137 has a new toolbar and profile menu customizations that help users easily identify if their Chrome profile is managed, whether they're on a work or personal device. This is especially useful for BYOD scenarios where employees use their own devices with managed accounts.

To help tailor this experience, we're adding three new policies:

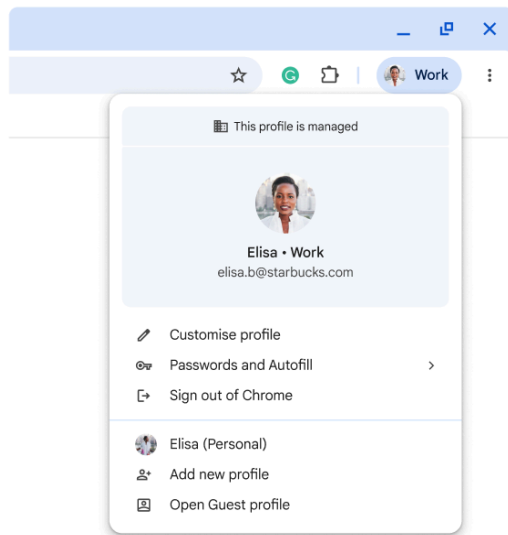
- [EnterpriseCustomLabel](#): Customize the text displayed on the toolbar element to match your organization's branding.
- [EnterpriseLogoUrl](#): Add your company logo to the profile menu.
- [EnterpriseProfileBadgeToolbarSettings](#): This policy can disable the default label for a managed profile in the Chrome toolbar.

In Chrome 134, these policies became available to customize the logo and label shown on a managed profile. Starting Chrome 137, there are updates to the default behavior of the profile label and icon overlaid on the account avatar. In Chrome 138, managed profiles will show a *work* or *school* label in addition to the profile disk. In the profile menu, there will be a building icon overlaid on the account avatar. The expanded profile disk can be disabled via [EnterpriseProfileBadgeToolbarSettings](#).

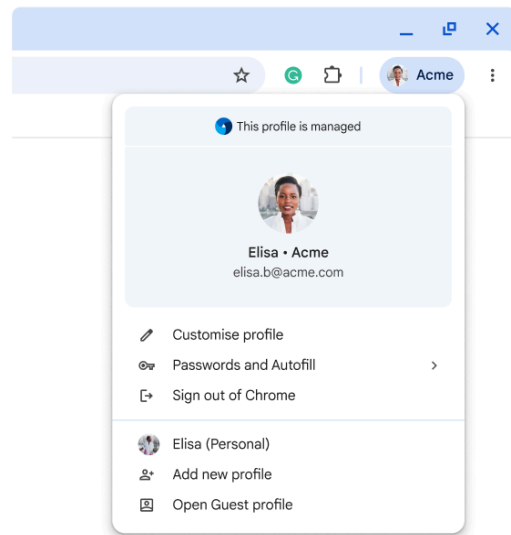
- Chrome 134 on LaCrOS, macOS, Windows: Policies to customize the toolbar label and icon (in profile menu).
- **Chrome 137 on Linux, macOS, Windows:** Rollout of *Managed by your organization* in profile menu . The logo can be customized via [EnterpriseLogoUrl](#) policy.
- Chrome 138 on Linux, macOS, Windows: Rollout of default *work* and *school* labels in Chrome toolbar. The label can be turned off via [EnterpriseProfileBadgeToolbarSettings](#).



## Default



## Customized



### Align error type thrown for *payment* WebAuthn credential creation: **SecurityError => NotAllowedError**

This change corrects the error type thrown during WebAuthn credential creation for *payment* credentials. Due to a historic specification mismatch, creating a *payment* credential in a cross-origin iframe without a user activation would throw a `SecurityError` instead of a `NotAllowedError`, which is what is thrown for non-payment credentials.

Code that previously detected the type of error thrown, for example, ``e instanceof SecurityError``, would be affected. Code that just generally handles errors during credential creation, for example, ``catch (e)``, will continue to function correctly.

- **Chrome 137 on Windows, macOS, Linux, Android**

## HSTS tracking prevention

HTTP Strict Transport Security ([HSTS](#)) tracking prevention mitigates user tracking by third-parties via the 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 137 on Windows, macOS, Linux, 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](#).

## Autofill with AI

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 Linux, macOS, Windows, ChromeOS**

### New policies in Chrome browser

Policy	Description
<a href="#">GeminiSettings</a>	Settings for Gemini integration
<a href="#">AutofillPredictionSettings</a>	Settings for Autofill with AI
<a href="#">ProvisionalNotificationsAllowed</a>	Allows the app to use provisional notification authorization on iOS
<a href="#">RelaunchFastIfOutdated</a>	Relaunch fast if outdated
<a href="#">UserSecurityAuthenticatedReporting</a>	Enable cloud reporting of security signals in managed profiles
<a href="#">BuiltInAIAPIsEnabled</a>	Allow pages to use the built-in AI APIs
<a href="#">OnSecurityEventEnterpriseConnector</a>	Configuration policy for the OnSecurityEvent Chrome Enterprise Connector (now available on iOS)
<a href="#">UserSecuritySignalsReporting</a>	Enable cloud reporting of security signals in managed profiles

### Removed policies in Chrome browser

Policy	Description
MutationEventsEnabled	Re-enable deprecated/removed Mutation Events
TabOrganizerSettings	Settings for Tab Organizer
ZstdContentEncodingEnabled	Enable zstd content-encoding support

## Current Chrome Enterprise Core updates

### IP Address Logging & Reporting

Chrome Enterprise will enhance security monitoring and incident response capabilities by collecting and reporting local and remote IP addresses and sending those IP addresses to the [Security Investigation Tool \(SIT\)](#) logs. In addition, Chrome Enterprise will allow admins to optionally send the IP addresses to first-party and third-party security information and event management (SIEM) providers via the Chrome Enterprise reporting connector. For more details, see [Manage Chrome Enterprise reporting connectors](#). This will be available for Chrome Enterprise Core and Chrome Enterprise Premium customers.

- **Chrome 137 on Windows, macOS, Linux**

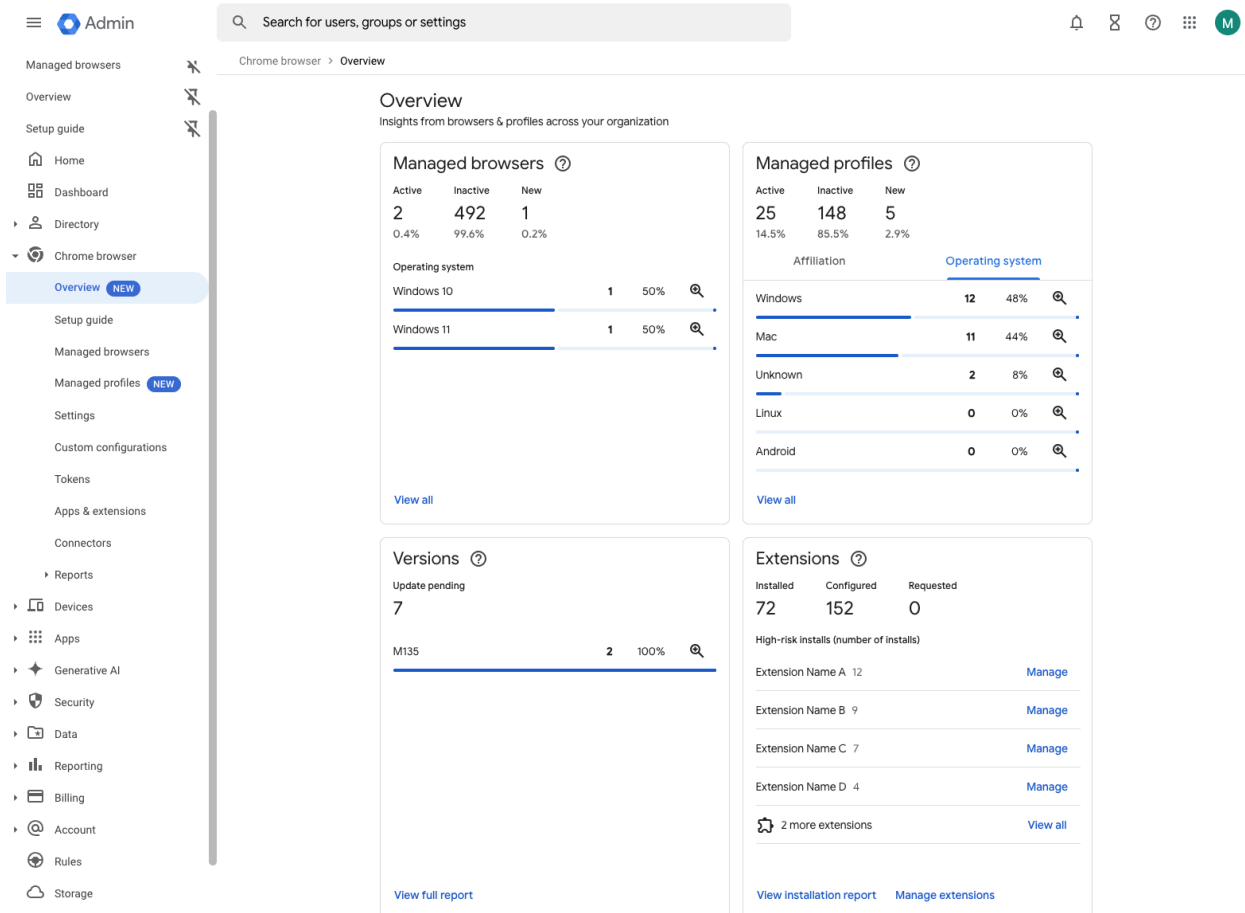
### Chrome Enterprise Overview page

Chrome Browser Enterprise 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 and 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

The Overview page also allows you to quickly access key actions, such as, managing extensions (block and allow) and accessing browser and profile lists.

- **Chrome 137 on Android, iOS, Linux, macOS, Windows**



## 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 138 on Linux, macOS, Windows:** Profile-level support for remote commands.

## New tab page cards for M365

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: Trusted Testers
- **Chrome 137 on Linux, macOS, Windows:** Rollout starts

## Current Chrome Enterprise Premium updates

### DLP download support for File System Access API (FSA)

Chrome Enterprise Premium's Data Loss Prevention (DLP) content analysis and Safe Browse deep scans now extend to folder and directory downloads initiated via the [File System Access \(FSA\) API](#), for example, in web-based IDEs. This addresses a gap, enhancing data security by applying existing DLP rules (configured via [DataLeakPreventionRulesList](#) and [SafeBrowsingDeepScanningEnabled](#) policies) to these operations.

If a download violates a DLP policy, it will be blocked, resulting in an empty file, and the website might indicate a *Blocked by Safe Browse* 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 137 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.

## Reporting Connector on Mobile

The [Chrome Enterprise Reporting Connector](#) is being updated to include security event reporting from Chrome on mobile devices (Android and iOS). This will provide IT admins with visibility into events such as unsafe site visits, sensitive data transfers (as per Data Protection rules), and URL Filtering matches occurring on mobile, achieving feature parity with existing desktop reporting. This enhancement aims to improve the organization's overall security posture by extending threat detection and data protection capabilities to mobile platforms.

For customers utilizing the Security Investigation Tool (SIT), these new mobile browser events will be available for investigation; this SIT integration is a feature of Chrome Enterprise Premium. IT admins should be aware that these additional event types from mobile will begin to flow through their configured Reporting Connector.

No new, specific enterprise policies are being introduced to control this mobile reporting extension itself; existing configurations for the Reporting Connector, Data Protection rules, and URL Filtering policies will determine the events generated and reported.

- **Chrome 137 on Android, iOS:** Enables security event reporting, for example, unsafe sites, sensitive data transfers, URL filtering, via the Reporting Connector for Chrome on Mobile

## Reporting Safe Browsing events on iOS

The feature will enable Safe Browsing events reporting on iOS to help increase the security of enterprise environments. This feature has already been implemented on Desktop and Android, we are now extending it to iOS. For details on how to turn on this feature, see this [help center article](#).

- **Chrome 137 on iOS:** Reporting Safe Browsing events become available on iOS

# 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

### Bookmarks and reading list improvements on Chrome Desktop

On 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](#), will continue to work as before, so admins can configure whether users can use and save items in their Google Account. Setting [EditBookmarksEnabled](#) to false will also prevent users from uploading a bookmark saved on their device to their Google Account.

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

### 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.

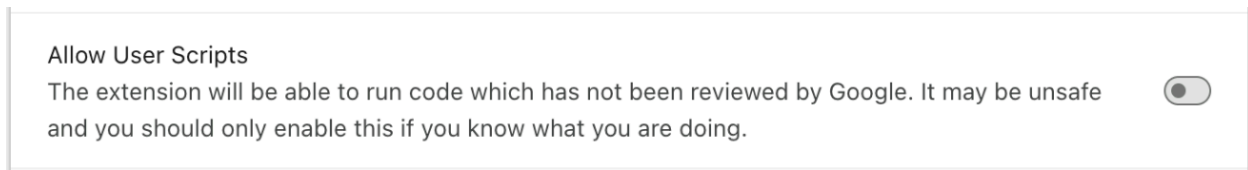
End users will now toggle this per extension on the `chrome://extensions` page via a **Allow User Scripts** toggle, replacing the global **Developer mode** toggle for more granular control. Existing extensions will have this toggle automatically enabled if **Developer mode** is on and the extension has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

Administrators who currently manage user scripts by disabling developer mode should now use the [`blocked\\_permissions` 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



### Enhanced Safe Browsing as a synced setting

Chrome's Enhanced Safe Browsing is becoming a synced feature. This means that if a user opts into Enhanced Safe Browsing on one device, this protection level will automatically apply 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 will 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 will be notified of this change via UI elements 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**

### Shared tab groups

Users will be able to collaborate on tabs via 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 will browse the same tabs on their devices. When one person changes a tab in the group, the changes are reflected across all user's browsers in the group. An enterprise policy, **TabGroupSharingSettings**, will be 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.

### 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 only available to users (18+) in English. Admins can control this feature by using the [DevToolsGenAiSettings](#) policy.

- Chrome 125 on ChromeOS, Linux, macOS, Windows: Feature becomes available to unmanaged users globally, except Europe, Russia, and China.
- Chrome 127 on ChromeOS, Linux, macOS, Windows: Feature becomes available to managed Chrome Enterprise & Education users in supported regions.
- 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.

### 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.

### 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) may malfunction and disconnect when TLS 1.3 Early Data is in use. If this occurs, administrators should contact the vendor for a fix.

This policy is a temporary measure to control the feature and will be removed in a future milestone. The policy may be enabled to allow you to test for issues and disabled while issues are being resolved.

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

### **Predictable reported storage quota**

Chrome 138 will introduce a predictable storage quota from StorageManager's estimate API for sites that do not have unlimited storage permissions.

It is possible to detect a user's browsing mode via the reported storage quota because the storage space made available is significantly smaller in incognito mode than in regular mode. This is a mitigation that prevents detection of a user's browsing mode via the storage API by reporting an artificial quota, equal to usage + min(10 GiB, disk rounded up to the nearest 1 GiB), in all browsing modes for sites with limited storage permissions. Sites with unlimited storage permissions will be unaffected. Enforced quota will also be unaffected.

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

### **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 in order to summarize inputs for a variety of use cases ([Github](#)), in a way that does not depend on the specific language model in question.

An enterprise policy ([GenAILocalFoundationalModelSettings](#)) is available to disable the underlying model downloading which would render this API unavailable.

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

### **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, [GenAILocalFoundationalModelSettings](#), is available to disable the underlying model downloading which would render this API unavailable.

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

### **Translator API**

The 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**

## 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.

## 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.

### **Chrome will 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**

### **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/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 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\\*](https://safebrowsing.googleapis.com/v4*), these should be modified to allow network requests to the whole domain instead: [safebrowsing.googleapis.com](https://safebrowsing.googleapis.com). Otherwise, rejected network requests to the v5 API will cause security regressions for users. For more details, see [Migration From V4 - Safe Browsing](#).



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

### **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

## Agentspace recommendations in the Chrome omnibox

This launch helps Enterprise users with their internal information needs by adding Enterprise Search results, such as people, file, or query suggestions, from [Agentspace](#) to the Chrome address bar.

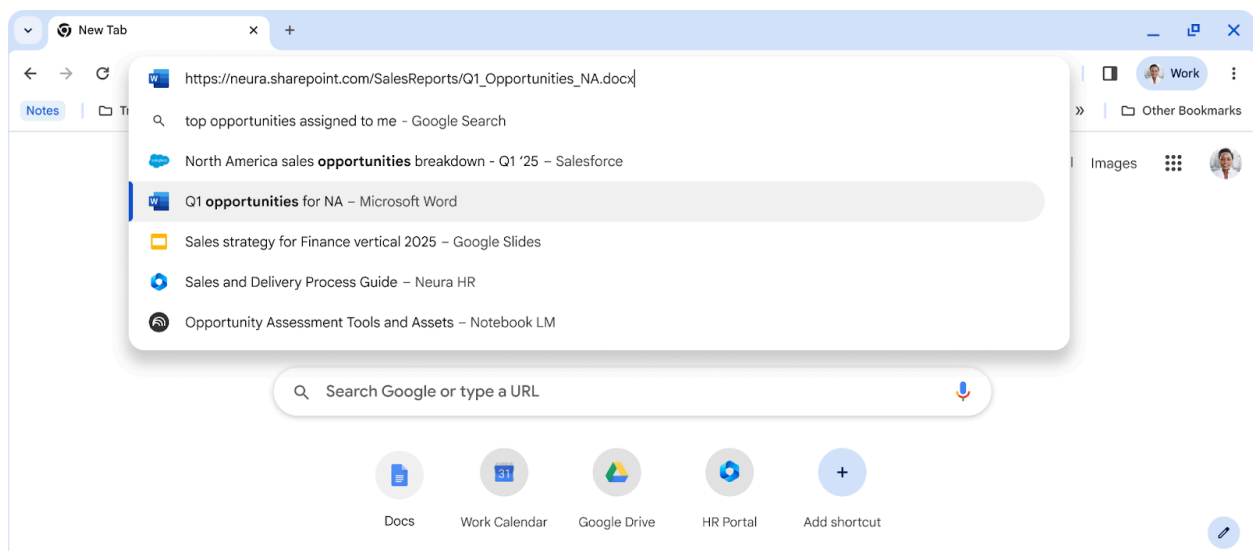
Results can be shown by default in Chrome's address bar recommendations or only when triggered by a custom keyword.

Users can also leverage the keyword mode to trigger actions through Agentspace, such as "help me write an email that summarizes the current project status".

The enterprise search provider will be shown when the user types "@" in the address bar. The organization will be able to 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**



## 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.

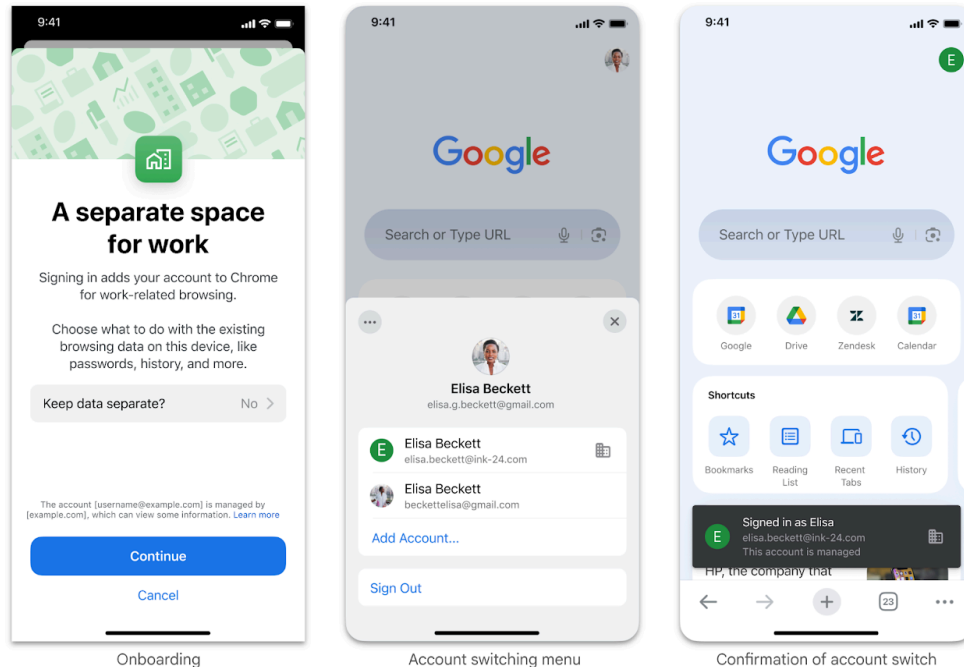
## **Multiple Identity Support on iOS**

Chrome on iOS is introducing support for multiple accounts, particularly for managed (work/school) accounts. This update introduces separate browser profiles for each managed account, ensuring strict data separation between work and personal browsing. Regular accounts will 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 will experience a one-time onboarding flow when adding a managed account to the device. They will be able to switch between accounts by tapping on the account particle disk on the **New tab** page.

Admins who enabled Chrome policies on iOS (instructions [here](#)) can continue to leverage existing policies.

- **Chrome 138 on iOS**

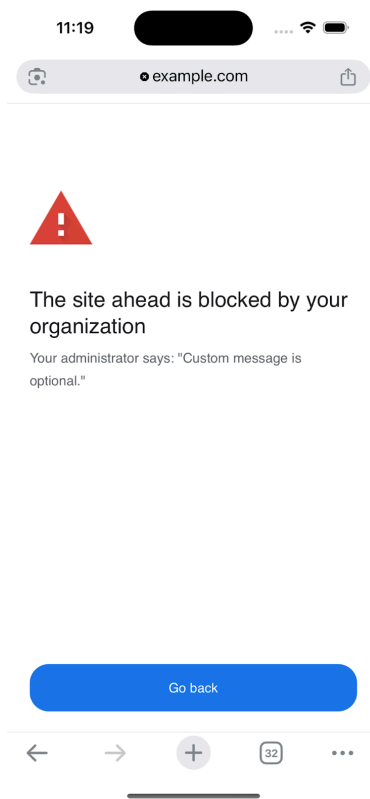
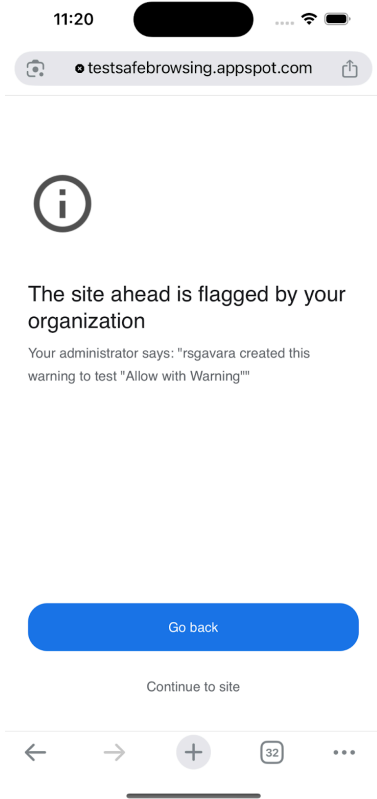


## Upcoming Chrome Enterprise Premium updates

### 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 will be able to create URL filtering rules to ensure that employees can only access safe and authorized URLs on iOS devices. Chrome will report URL filtering events and unsafe site events via the Reporting Connector on mobile.

- **Chrome 138 on iOS:** The URL Filtering feature becomes available on iOS.



## DLP Download Support for File System Access API (FSA)

Data Loss Prevention (DLP) protection will be extended to cover files and directories downloaded using the [File System Access \(FSA\) API](#). This enhancement will ensure that downloads from modern web applications, such as browser-based editors, are scanned according to your organization's DLP rules. Users and websites will receive notifications on scan verdicts, strengthening data security and compliance.

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

## Previous release notes

Chrome version & targeted Stable channel release date
<a href="#">Chrome 136: April 23, 2025</a>
<a href="#">Chrome 135: March 26, 2025</a>
<a href="#">Chrome 134: February 26, 2025</a>
<a href="#">Chrome 133: January 9, 2025</a>
<a href="#">Archived release notes</a>

## Additional resources

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

## Still need help?

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

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