chrome enterprise

Chrome 134 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 Feb 26, 2025, updated March 3, 2025.

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

Chrome 134 release summary

Current Chrome browser updates	Security / Privacy	User productivity / Apps	Management
Search your screen with Google Lens on Desktop and iOS		✓	
Security & Privacy panel in Chrome DevTools	✓	✓	
Better password form detection with ML	✓		
Client’s LLM assistance in mitigating scams	✓		
LLM-powered on-device detection of abusive notifications on Android			✓
Customizing managed profiles with custom logo and label		✓	✓
Device Bound Session Credentials google.com prototype	✓		
Password change	✓		
Read aloud in Reading mode in Chrome 134		✓	
Restrict unpacked extensions to developer mode	✓		
Show settings for AI features in policy level 2 in settings			✓
Customizable <select> element		✓	
HTML parser relaxation for <select>	✓		
Remove nonstandard getUserMedia audio constraints	✓		
Updates to Chrome sign-in flows for managed users	✓		
New tab page cards for Microsoft Outlook and Sharepoint		✓	
New policies in Chrome browser			✓

Removed policies in Chrome browser			✓
Chrome Enterprise Core	**Security / Privacy**	**User productivity / Apps**	**Management**
Chrome Enterprise Companion			✓
DownloadRestrictions policy support on iOS	✓		
Recommended policies (User override)			✓
Chrome Enterprise Premium	**Security / Privacy**	**User productivity / Apps**	**Management**
Evidence Locker	✓		
Screenshot prevention	✓		
Upcoming Chrome browser updates	**Security / Privacy**	**User productivity / Apps**	**Management**
Deprecate mutation events		✓	
Extensions improvements on Chrome Desktop	✓	✓	
Removal of Private Network Access enterprise policies	✓		
Remove ThirdPartyBlockingEnabled policy			✓
Settings, site shortcuts, and themes improvements on Chrome Desktop	✓		
Sunsetting the legacy Password Manager in Chrome on Android	✓		
Third-party cookies always blocked in Incognito mode	✓		
Blob URL Partitioning: Fetching/Navigation	✓		
Create service worker client and inherit service worker controller for srcdoc iframe	✓		
Deprecate getters of Intl Locale Info	✓		
Partitioning :visited links history	✓		
HSTS tracking prevention	✓		

Remove deprecated navigator.xr.supportsSession method	✓		
Strict same-origin policy for Storage Access API	✓		
UI Automation accessibility framework provider on Windows		✓	
Remove SwiftShader fallback	✓		
Disallow spaces in non-file:// URL hosts	✓		
SafeBrowsing API v4 → v5 migration	✓		
Upcoming Chrome Enterprise Core updates	**Security / Privacy**	**User productivity / Apps**	**Management**
Apple Extensible SSO support for Chrome on macOS		✓	✓
Isolated Web Apps	✓		
Upcoming Chrome Enterprise Premium updates	**Security / Privacy**	**User productivity / Apps**	**Management**
Refactor DLP rules user experience	✓		
URL filtering on iOS and Android	✓		
Reporting connector for mobile	✓		
Connectors API	✓		

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

Search your screen with Google Lens on Desktop and iOS

Admins can control all elements of this feature through a policy called LensOverlaySettings. To perform the search, a screenshot of the screen is sent to Google servers but it is not linked to any IDs or accounts, it is not viewed by any human, and data about its contents is not logged. To contextualize the search to the document or website the user is viewing, the PDF bytes or website HTML is sent to Google servers but is not linked to any IDs or accounts, not viewable by any human, and the data or data generated about its contents is not logged.

Desktop

Since Chrome 126, users can search any images or text they see on their Desktop screen with Google Lens. To use this feature, go to a website and click the **Google Lens** chip on the on-focus omnibox or right-click an image and select **Search with Google Lens**. Users can select anywhere on the screen to search its contents, and refine their search by adding questions to the search box. Starting in Chrome 132, users can also ask questions about entire web pages or PDF documents and answers will reference their current document and the web. To use this feature, invoke **Search with Google Lens** as described above and enter queries into the search box on the top right corner of the Chrome window. A side panel will open on the right side of the browser window with search results.

iOS

Since Chrome 131, users can search any images or text they see on their iOS Chrome screen with Google Lens. To use this feature, go to a website and click on the **3-dot menu > Search with Google Lens**. Starting in Chrome 134, users can also invoke this feature by clicking the **Google Lens** icon on the left side of the omnibox. Users can click, highlight, or drag anywhere on the screen to search its contents, and refine their search by adding keywords or questions to the search box.

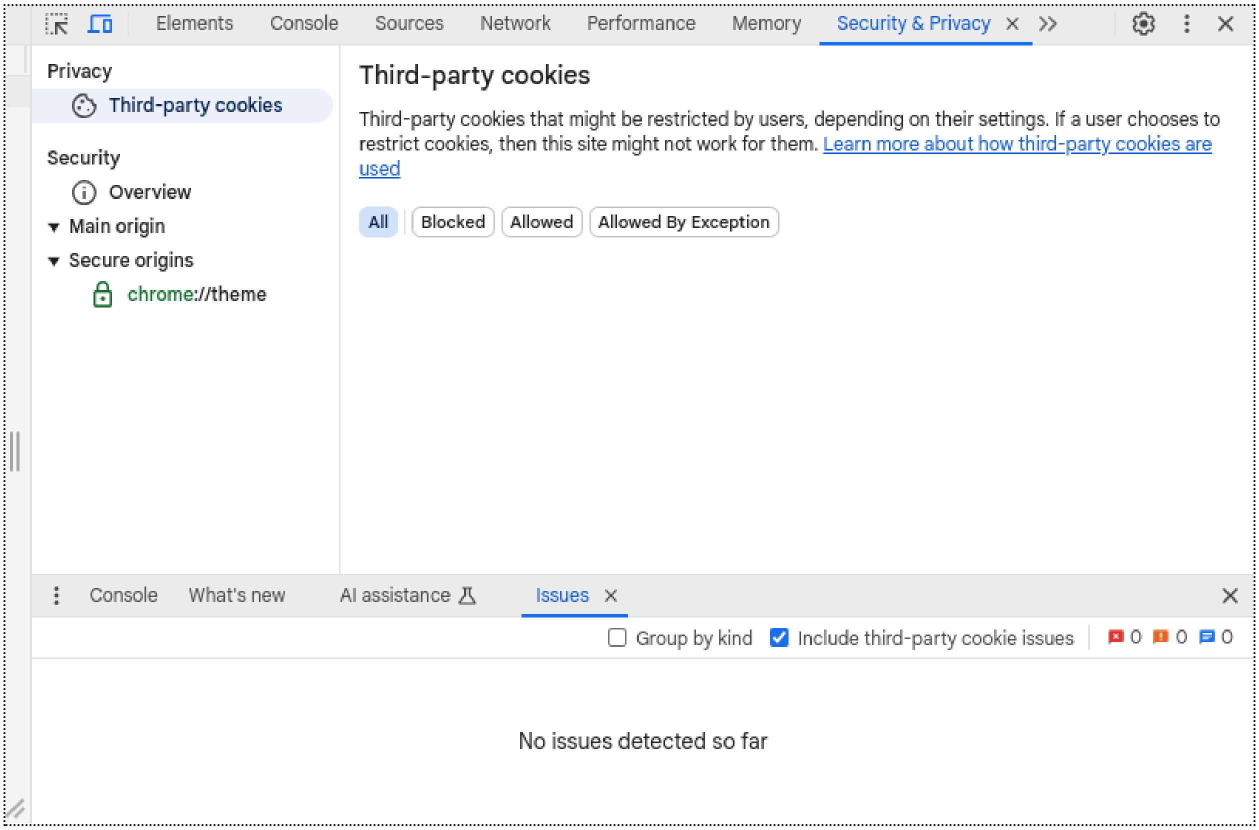
Rollout details:

- Chrome 126 on ChromeOS, Linux, macOS, Windows: Rollout of the feature to 1% Stable
- Chrome 127 on ChromeOS, Linux, macOS, Windows: Rollout to 100% Stable
- Chrome 131 on iOS: Rollout of the feature to 1% Stable

- Chrome 132 on ChromeOS, Linux, macOS, Windows: Rollout of the expanded feature to 1% Stable
- Chrome 133 on iOS: Rollout to 100% Stable
- **Chrome 134 on iOS: Rollout of the expanded feature to 100% Stable**

Security & Privacy panel in Chrome DevTools

Starting in Chrome 134, developers can use the new **Security & Privacy** panel in Chrome DevTools to test how their site behaves when third-party cookies are limited. Developers can temporarily limit third-party cookies, observe how their site behaves, and review the status of third-party cookies on their site.



Third-party cookies

Third-party cookies that might be restricted by users, depending on their settings. If a user chooses to restrict cookies, then this site might not work for them. Learn more about how third-party cookies are used

☐ Group by kind ☑ Include third-party cookie issues

No issues detected so far

This feature does not make any permanent changes to existing enterprise policies, but it lets third-party cookie related enterprise policies (that is, BlockThirdPartyCookies and CookiesAllowedForUrls) be temporarily overridden, to test enhanced restrictions. If your enterprise policy already blocks third-party cookies using BlockThirdPartyCookies, this feature will be disabled.

The new **Security & Privacy** panel replaces the existing **Security** panel. TLS connection and certificate information continue to be available on the **Security** menu on the left, within the **Security & Privacy** panel.

- **Chrome 134 on ChromeOS, Linux, macOS, Windows**

Better password form detection with ML

Chrome 134 introduces a new client-side Machine Learning (ML) model to better parse password forms on the web to increase detection and filling accuracy. You can control this feature using the PasswordManagerEnabled policy.

- **Chrome 134 on Android, iOS, ChromeOS, Linux, macOS, Windows**

Client's LLM assistance in mitigating scams

Users on the webs are facing enormous amounts of several kinds of scams a day. To combat these scams, Chrome will leverage on-device Large Language Model (LLM) to identify scam websites for Enhanced Safe Browsing (ESB) users. Chrome will send the page content to an on-device LLM to infer security-related signals of the page and send these signals to Safe Browsing server side for a final verdict. When enabled, Chrome may consume more bandwidth to download the LLM.
An enterprise policy SafeBrowsingProtectionLevel is available to control safe browsing and the mode it operates in.

- **Chrome 134 on Linux, macOS, Windows**
  Gather the brand name and intent summary of the page that requested keyboard lock API to identify scam websites.

LLM-powered on-device detection of abusive notifications on Android

This launch aims to hide the contents of notifications that are suspected to be abusive. The user then has the options to dismiss, show the notification, or unsubscribe from the origin. This detection is to be done by an on-device model.

- **Chrome 134 on Android**

Customizing managed profiles with custom logo and label

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 scenarios where employees use their own devices with managed accounts.
To help tailor this experience, we're adding three new policies:

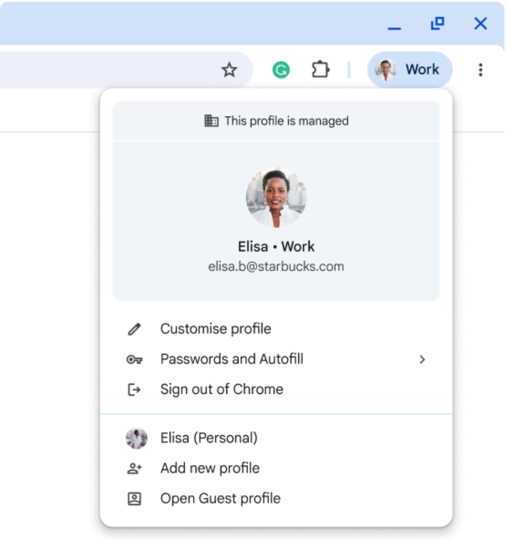
- EnterpriseCustomLabel: Customize the text displayed on the toolbar element to match your organization's branding.
- EnterpriseLogoUrl: Add your company logo to the profile menu.
- EnterpriseProfileBadgeToolbarSettings: This policy can disable the default label for a managed profile in the Chrome toolbar.

In Chrome 134, these policies will be available to customize the logo and label shown on a managed profile. The policies will take effect on user's managed profiles.

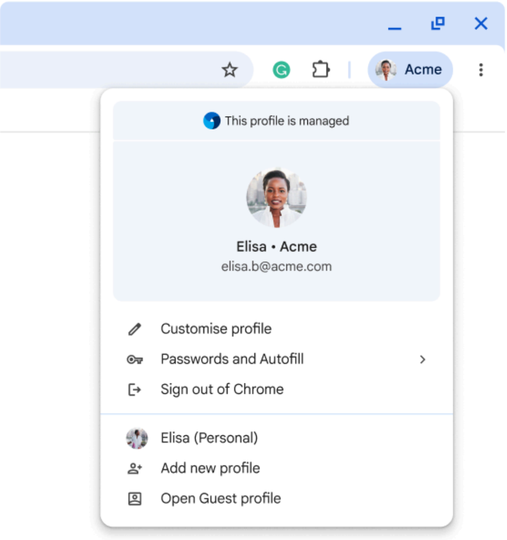
Starting Chrome 135, there will be updates to the default behavior of the profile label and icon overlaid on the account avatar. Managed profiles will show a *work* or *school* label in addition to the profile disk. In the profile menu, there will be a building icon overlaid on the account avatar. The expanded profile disk can be disabled via EnterpriseProfileBadgeToolbarSettings.

- **Chrome 134 on macOS, Windows, Linux**
  Policies to customize the toolbar label and icon (in profile menu) are available in the Admin console. If policies have already been set, the user will see the customized logo and label.
- Chrome 135: Starting rollout of defaults including:
  - 1) *work* or *school* label shown in toolbar, next to user avatar
  - 2) A building icon overlayed on the user's account photo in the profile menu. The label can be turned off via EnterpriseProfileBadgeToolbarSettings. Starting with 1% and gradual slow rollout thereafter.

Default



Customized



Device Bound Session Credentials google.com prototype

The Device Bound Session Credentials (DBSC) project is intended to move the web away from long-lived bearer credentials like cookies, which can be stolen and reused, to credentials which are either short-lived or cryptographically bound to a device.

The feature aims at protecting users against credential theft which is typically performed by malware running on the user's device.

The current launch is a proof-of-concept targeting the **google.com** website. In the future, we plan to standardize this approach for other websites and web browsers.

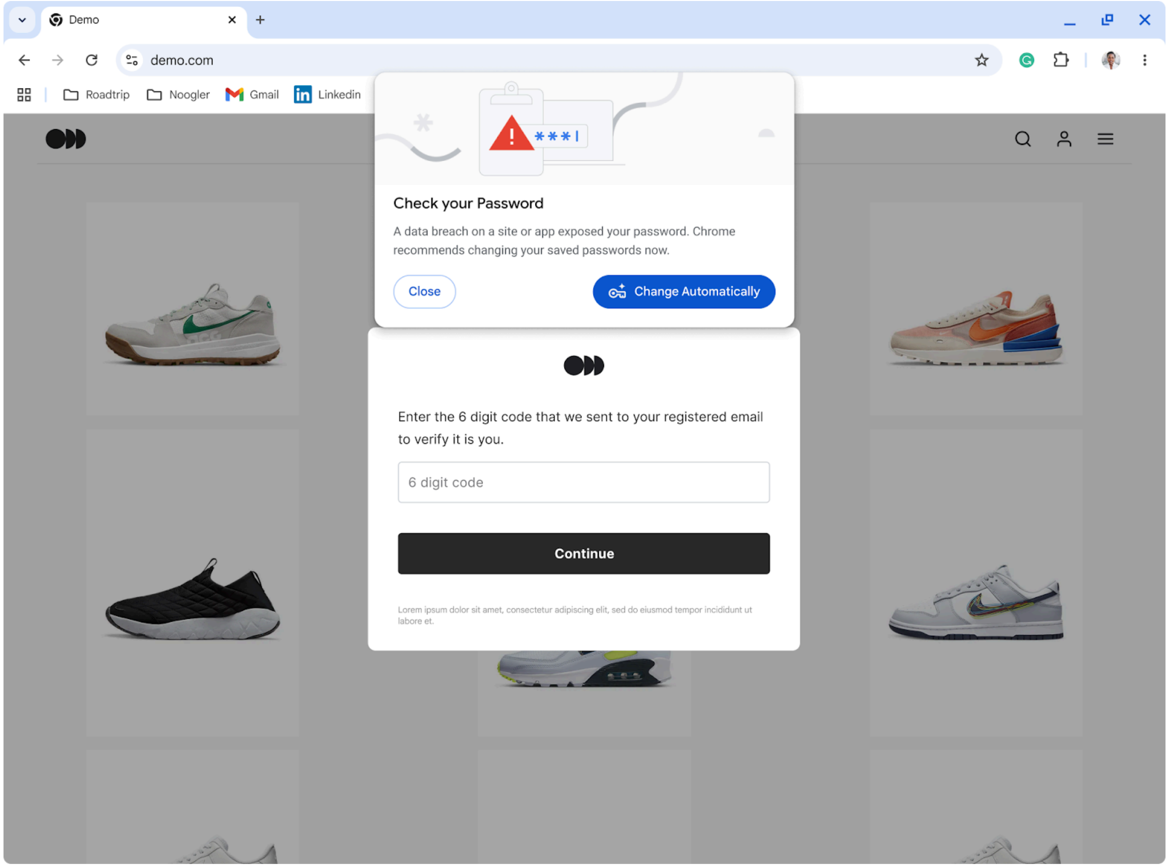
Enterprise admins can control the feature state using the BoundSessionCredentialsEnabled boolean policy.

- Chrome 124 on Windows
  Planned 1% rollout on Chrome stable for google.com cookie binding for the general population.
- **Chrome 134 on Windows**
  Added binding support for OAuth2.0 refresh tokens that are used for Chrome sign-in.

Password change

This feature gives users the option to change leaked credentials immediately. The feature can only be triggered from the **Check your Password** dialog. When users see a warning for an eligible website, they can change the password there and then.

- **Chrome 134 on Linux, macOS, Windows**



Check your Password

A data breach on a site or app exposed your password. Chrome recommends changing your saved passwords now.

Enter the 6 digit code that we sent to your registered email to verify it is you.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et.

Read aloud in Reading mode in Chrome 134

Reading mode is a side-panel feature that provides a simplified view of text-dense web pages. Reading mode now includes a **Read aloud** feature that allows users to hear the text they are reading spoken out loud. You can choose different natural voices and speeds, and see visual highlights as the text is spoken.

- **Chrome 134 on Linux, macOS, Windows**

Restrict unpacked extensions to developer mode

Starting in Chrome 134, unpacked extensions loaded from the `chrome://extensions` page will only be enabled if the developer mode switch is turned on. This change is intended to improve security by mitigating the risks associated with harmful unpacked extensions and developer mode tampering exploitation. An enterprise policy, ExtensionDeveloperModeSettings, is available to gate the existing developer mode switch.

- **Chrome 134 on ChromeOS, Linux, macOS, Windows**
  The feature will roll out to 100% of users on Chrome 134.

Show enterprise settings for AI features

Previously, AI features were hidden from settings when they are disabled by enterprise policy. Now, we will keep showing the features and show a *Disabled by your organization* notice, similar to other settings when they are disabled by policy.

- **Chrome 134 on ChromeOS, Linux, macOS, Windows**

Customizable <select> element

Customizable `<select>` allows developers to take complete control of the rendering of `<select>` elements by adding the appearance:base-select CSS property.
This feature relies on the `SelectParserRelaxation` flag, which changes the HTML parser to allow more tags within the `<select>` tag. Sites that include additional tags inside `<select>`, which were getting removed before, such as `<span>` tags, or sites that include an extremely large number of `<option>` tags in their `<select>`, might be affected by `SelectParserRelaxation`. This feature and `SelectParserRelaxation` can be controlled with the SelectParserRelaxation enterprise policy. Some issues that have come up in prior launches of `SelectParserRelaxation`

include `<select>` elements taking a very long time to open or <option> tags not showing up anymore.

- **Chrome 134 on Windows, macOS, Linux, Android**

HTML parser relaxation for <select>

In Chrome 134, the HTML parser allows more tags in `<select>` in addition to `<option>`, `<optgroup>`, and `<hr>`.
This supports the customizable `<select>` feature but is being shipped first because it can be done separately and has some compatibility risk.
This feature is gated by the temporary policy SelectParserRelaxationEnabled. This is a temporary transition period, and the policy will stop working by Chrome 141.
For more details, see the Customizable Select Element (Explainer).

- **Chrome 134 on Windows, macOS, Linux, Android**

Remove nonstandard getUserMedia audio constraints

Chrome 134 removes a number of nonstandard goog-prefixed constraints for `getUserMedia`, which existed before audio constraints were properly standardized.

Usage has gone down significantly ~0.000001% to 0.0009% (depending on the constraint) and some of them do not even have an effect due to changes in the Chromium audio-capture stack. Soon none of them will have any effect due to other upcoming changes.

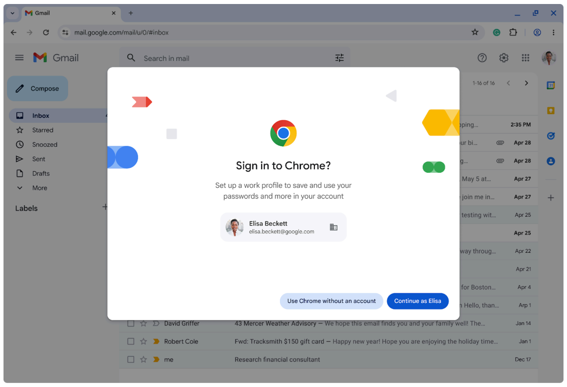
We do not expect any major regressions due to this change. Applications using these constraints will continue to work, but will get audio with default settings (as if no constraints were passed). They can easily migrate to standard constraints.

- **Chrome 134 on Windows, macOS, Linux, Android**

Updates to Chrome sign-in flows for managed users

Enterprise users signing into the web or Chrome now see refreshed sign-in flows and management disclosures. In addition, the user might be prompted to create a new profile or continue working in the existing profile. Admins can continue to use [BrowserSignIn]() or [ProfileSeparationSettings]() to enforce a managed profile.

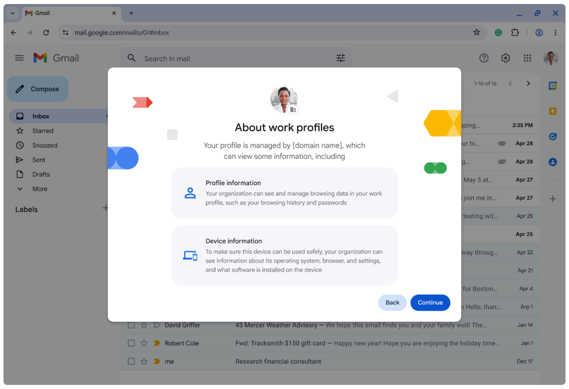
- **Chrome 134 on Linux, macOS, Windows** Roll-out continues



Sign in to Chrome?

Set up a work profile to save and use your passwords and more in your account

Elisa Beckett
elisa.beckett@google.com

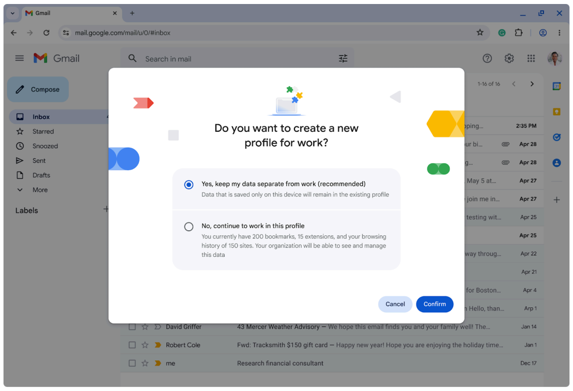


About work profiles

Your profile is managed by [domain name], which can view some information, including

Profile information
Your organization can see and manage browsing data in your work profile, such as your browsing history and passwords

Device information
To make sure this device can be used safely, your organization can see information about its operating system, browser, and settings, and what software is installed on the device



Do you want to create a new profile for work?

● Yes, keep my data separate from work (recommended)
Data that is saved only on this device will remain in the existing profile

○ No, continue to work in this profile
You currently have 200 bookmarks, 15 extensions, and your browsing history of 150 sites. Your organization will be able to see and manage this data

New tab page cards for Microsoft Outlook and Sharepoint

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 who are interested in testing out this feature can [Sign up to become a Trusted Tester]().

- **Available to Trusted Testers Chrome 134 on Windows, macOS, Linux**

New policies in Chrome browser

Policy	Description
ProfileSeparationDataMigrationSettings	Profile separation data migration settings
NTPSharepointCardVisible	Show SharePoint and OneDrive File Card on the New Tab Page
NTPOutlookCardVisible	Show Outlook Calendar card on the New Tab Page
ServiceWorkerToControlSrcdocIframeEnabled	Allow ServiceWorker to control srcdoc iframes
PasswordManagerPasskeysEnabled	Enable saving passkeys to the password manager

Removed policies in Chrome browser

Policy	Description
N/A	

Current Chrome Enterprise Core updates

Chrome Enterprise Companion

Chrome Enterprise Companion is a new administrative binary that will be automatically installed with Chrome browsers enrolled into Chrome Enterprise Core or Chrome Enterprise Premium. It is meant to support Enterprise use cases, policies, and reporting.

- **Chrome 134 on Windows, macOS**

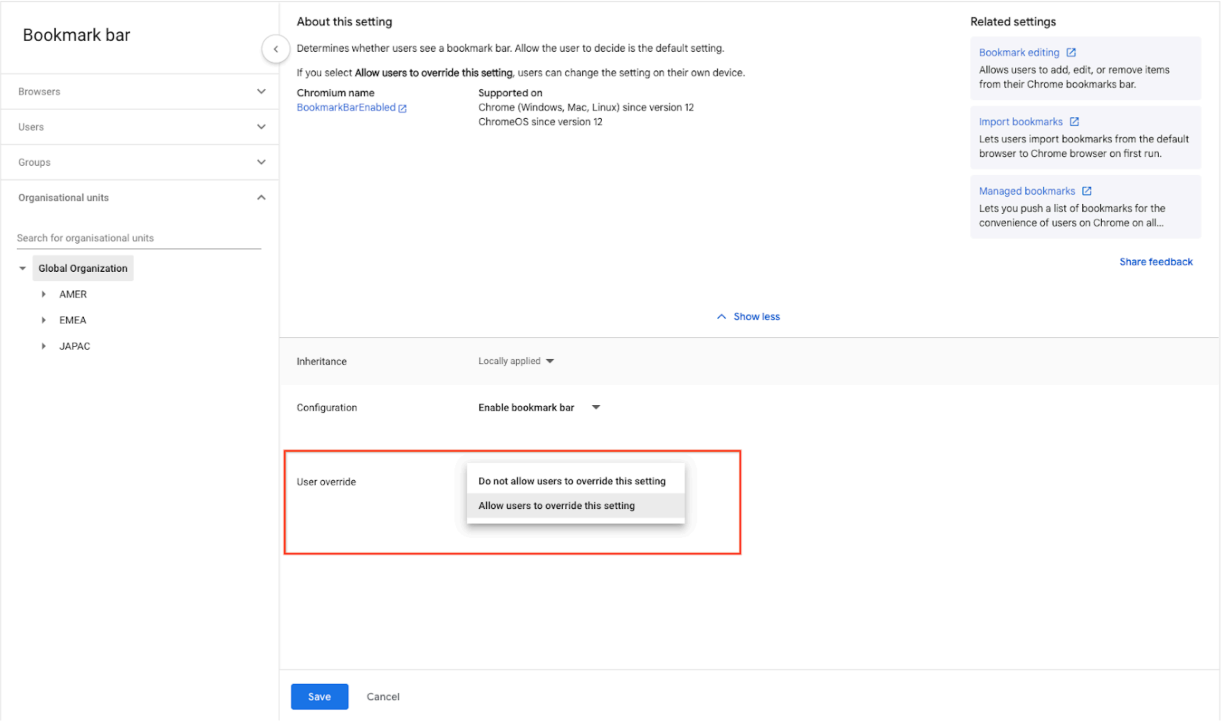
DownloadRestrictions policy support on iOS

DownloadRestrictions is a universal policy available to Chrome Enterprise Core users on Desktop platforms and on Android. The DownloadRestrictions policy is now supported on iOS. This allows admins to block all downloads on mobile Chrome on iOS.

- **Chrome 135 on iOS**

Recommended policies (User override)

Chrome has introduced the **User override** configuration in the Google Admin console for policies that can be set as recommended. This means that IT administrators can apply a policy value and allow users to override the policy value.



About this setting

Determines whether users see a bookmark bar. Allow the user to decide is the default setting.

If you select **Allow users to override this setting**, users can change the setting on their own device.

Chromium name: BookmarkBarEnabled

Supported on: Chrome (Windows, Mac, Linux) since version 12
ChromeOS since version 12

Related settings

Bookmark editing: Allows users to add, edit, or remove items from their Chrome bookmarks bar.

Import bookmarks: Lets users import bookmarks from the default browser to Chrome browser on first run.

Managed bookmarks: Lets you push a list of bookmarks for the convenience of users on Chrome on all...

Share feedback

Inheritance: Locally applied

Configuration: Enable bookmark bar

User override:
- Do not allow users to override this setting
- Allow users to override this setting

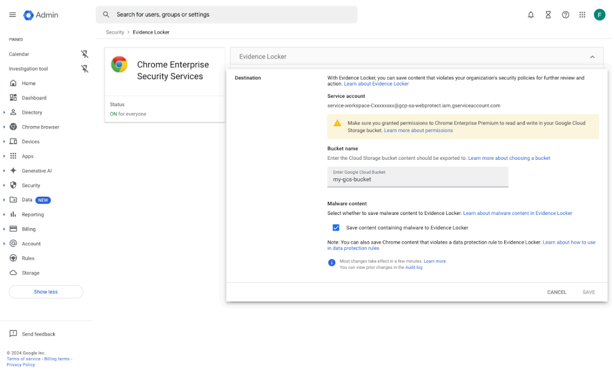
- **On Chrome 134**: the following policies are supported: BookmarkBarEnabled, PasswordManagerEnabled, PinUnlockAutosubmitEnabled, SchedulerConfiguration, PrintHeaderFooter, TranslateEnabled, SpellCheckServiceEnabled, ShowFullUrlsInAddressBar

Current Chrome Enterprise Premium updates

Evidence Locker

Evidence Locker allows Chrome Enterprise Premium administrators to store and inspect files that are flagged as malware or those that violate a Data Protection rule. A copy of the file is saved to the Google Cloud Storage bucket that is owned and specified by the organization. The security administrator can investigate the incidents using the security investigation tool and download the files that triggered the incident to analyze further. For more details, see Investigate and take action on suspicious files.

- **Chrome 134 on ChromeOS, Linux, macOS, Windows**



Status
ON for everyone

Destination

With Evidence Locker, you can save content that violates your organization's security policies for further review and action. Learn about Evidence Locker

Service account

service-workspace-Cxxxxxxxx@gcp-sa-webprotect.iam.gserviceaccount.com

Make sure you granted permissions to Chrome Enterprise Premium to read and write in your Google Cloud Storage bucket. Learn more about permissions

Bucket name

Enter the Cloud Storage bucket content should be exported to. Learn more about choosing a bucket

Enter Google Cloud Bucket: my-gcs-bucket

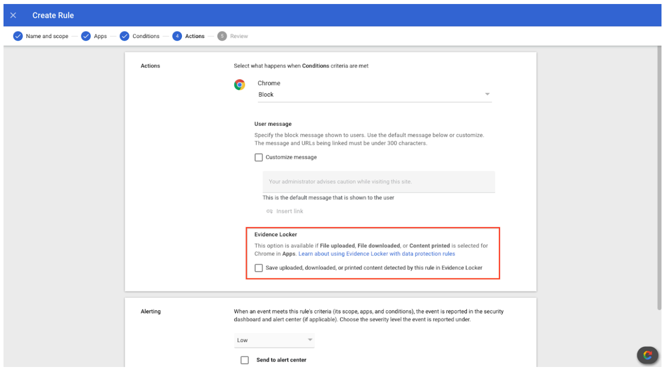
Malware content

Select whether to save malware content to Evidence Locker. Learn about malware content in Evidence Locker

☑ Save content containing malware to Evidence Locker

Note: You can also save Chrome content that violates a data protection rule to Evidence Locker. Learn about how to use in data protection rules

Most changes take effect in a few minutes. Learn more
You can view prior changes in the Audit log



Actions

Select what happens when **Conditions** criteria are met

Chrome
Block

User message

Specify the block message shown to users. Use the default message below or customize. The message and URLs being linked must be under 300 characters.

☐ Customize message

Your administrator advises caution while visiting this site.

This is the default message that is shown to the user

Evidence Locker

This option is available if **File uploaded**, **File downloaded**, or **Content printed** is selected for Chrome in **Apps**. Learn about using Evidence Locker with data protection rules

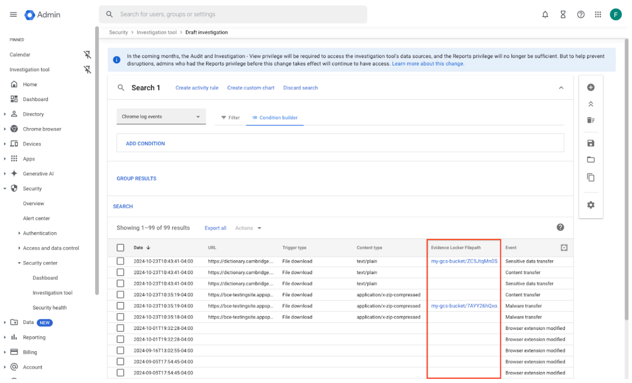
☐ Save uploaded, downloaded, or printed content detected by this rule in Evidence Locker

Alerting

When an event meets this rule's criteria (its scope, apps, and conditions), the event is reported in the security dashboard and alert center (if applicable). Choose the severity level the event is reported under.

Low

☐ **Send to alert center**



In the coming months, the Audit and Investigation - View privilege will be required to access the investigation tool's data sources, and the Reports privilege will no longer be sufficient. But to help prevent disruptions, admins who had the Reports privilege before this change takes effect will continue to have access. Learn more about this change.

Showing 1–99 of 99 results

□	Date ↓	URL	Trigger type	Content type	Evidence Locker Filepath	Event
□	2024-10-23T10:43:41-04:00	https://dictionary.cambridge....	File download	text/plain	my-gcs-bucket/ZC5JtqMn0S.	Sensitive data transfer
□	2024-10-23T10:43:41-04:00	https://dictionary.cambridge....	File download	text/plain		Content transfer
□	2024-10-23T10:43:41-04:00	https://dictionary.cambridge....	File download	text/plain		Sensitive data transfer
□	2024-10-23T10:35:19-04:00	https://bce-testingsite.appsp...	File download	application/x-zip-compressed		Content transfer
□	2024-10-23T10:35:19-04:00	https://bce-testingsite.appsp...	File download	application/x-zip-compressed	my-gcs-bucket/7AYY26hQxo.	Malware transfer
□	2024-10-23T10:35:18-04:00	https://bce-testingsite.appsp...	File download	application/x-zip-compressed		Malware transfer
□	2024-10-01T19:32:28-04:00					Browser extension modified
□	2024-10-01T19:32:28-04:00					Browser extension modified
□	2024-09-16T13:02:55-04:00					Browser extension modified
□	2024-09-05T17:54:45-04:00					Browser extension modified
□	2024-09-05T17:54:45-04:00					Browser extension modified

Screenshot prevention

Chrome 134 enhances the existing screenshot prevention feature by extending screen-sharing blocking to meeting apps like Google Meet, Zoom, Teams, and Slack. With this update, we build upon the successful release of data protection controls by adding key features and addressing gaps and user feedback.

- **Chrome 134 on Windows, macOS**

Read more about the differences between Chrome Enterprise Core and Chrome Enterprise Premium.

Coming soon

Note: The items listed below are experimental or planned updates. They might change, be delayed, or canceled before launching to the Stable channel.

Upcoming Chrome browser updates

Deprecate mutation events

Synchronous mutation events, including DOMSubtreeModified, DOMNodeInserted, DOMNodeRemoved, DOMNodeRemovedFromDocument, DOMNodeInsertedIntoDocument, and DOMCharacterDataModified, negatively affect page performance, and also significantly increase the complexity of adding new features to the Web. These APIs were deprecated from the spec in 2011, and were replaced (in 2012) by the much better-behaved Mutation Observer API. Usage of the obsolete mutation events must be removed or migrated to Mutation Observer.

Since Chrome 124, a temporary enterprise policy, MutationEventsEnabled, is available to re-enable deprecated or removed mutation events. To read more, see this Chrome for Developers blog post. If you encounter any issues, you can file a Chromium bug.

Mutation event support is disabled by default, since Chrome 127, or around July 30, 2024. Code should have been migrated before that date to avoid site breakage. If more time is needed, there are a few options:

- The Mutation Events Deprecation Trial can be used to re-enable the feature for a limited time on a given site. This can be used up until Chrome 134, ending March 25, 2025.
- A MutationEventsEnabled enterprise policy can also be used for the same purpose, also through Chrome 134.
- **Chrome 135 on Android, Linux, macOS, Windows:** The MutationEventsEnabled enterprise policy will be deprecated.

Extensions improvements on Chrome Desktop

On Chrome 135 on Desktop, some users who sign in to Chrome when installing a new extension can now use and save extensions in their Google Account.
Relevant enterprise policies controlling extensions, 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.
For more information about how to use extensions on any computer, see Install and manage extensions in the Chrome Web Store help center.

Note: this change is a follow-up to the launch of the new identity model on Chrome Desktop.

- **Chrome 135 on Linux, macOS, Windows**

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). 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 in Chrome 135. 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.

PNA 2.0 is described in this explainer on GitHub.

- **Chrome 135 on Android, ChromeOS, Linux, macOS, Windows, Fuchsia**
  Removal of InsecurePrivateNetworkRequestsAllowedForUrls and InsecurePrivateNetworkRequestsAllowed policies.
- Chrome 137 on Android, ChromeOS, Linux, macOS, Windows, Fuchsia
  Removal of PrivateNetworkAccessRestrictionsEnabled.

Remove ThirdPartyBlockingEnabled policy

Due to unexpected issues, ThirdPartyBlockingEnabled will be removed in Chrome 135. If you have feedback about this removal, you can file a Chromium bug.

- Chrome 132 on Windows
  Deprecation of ThirdPartyBlockingEnabled policy
- **Chrome 135 on Windows**
  Removal of ThirdPartyBlockingEnabled policy

Settings, site shortcuts, and themes improvements on Chrome Desktop

On Chrome 135 on Desktop, for users who newly sign in to Chrome or who have Sync enabled, settings, site shortcuts and themes synced to their Google Account will now be kept separate from the local ones, that is, settings from when they're signed out or when Sync is turned off.
This allows for strictly less data sharing than previously: local settings don't get automatically uploaded when signing in or turning on Sync, and no settings from the account are left behind on the device when Sync is turned off.
Existing enterprise policies SyncDisabled and SyncTypesListDisabled will continue to apply so admins can restrict or disable the Sync feature if they want to.

Note: This change is a follow-up to the launch of the new identity model on Chrome Desktop. For more details, see Chrome Platform Status.

- **Chrome 135 on Linux, macOS, Windows**

Sunsetting the legacy Password Manager in Chrome on Android

Users with old versions of Google Play Services will lose Password Manager functionality in Chrome. This is a step towards sunsetting the legacy Password Manager in Chrome on Android. These users can download a CSV file with their passwords from Chrome Settings and import it to their preferred Password Manager. The new Google Password Manager is available on devices with a recent version of Google Play Services.

- **Chrome 135 on Android**

Third-party cookies always blocked in Incognito mode

Starting in Chrome 135, users will start having third-party cookies blocked in Incognito mode with no way to globally re-enable them. Site-level controls for allowing third-party cookies will not be changed.

With this launch, the BlockThirdPartyCookies policy will only apply to regular mode when set to false, not Incognito mode. There will be no changes when the policy is true or unset. There will also be no changes to the CookieAllowedForUrls policy, which will continue to apply in both regular and Incognito modes, as it applies at the site level and not globally.

- **Chrome 135 on Android, ChromeOS, Linux, macOS, Windows**

Blob URL Partitioning: Fetching/Navigation

As a continuation of Storage Partitioning, Chromium will implement 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, Chromium will enforce 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 Chromium 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 135 on Windows, macOS, Linux**

Create service worker client and inherit service worker controller for srcdoc iframe

Srcdoc context documents are currently not service worker clients and are not covered by their parent page's service worker. This results in some discrepancies (for example, Resource Timing reports the URLs that these documents load, but the service worker doesn't intercept them). We aim to fix the discrepancies by creating service worker clients for `srcdoc` iframes and make them inherit the parent page's service worker controller.

- **Chrome 135 on Windows, macOS, Linux, Android**

Deprecate getters of Intl Locale Info API

Intl Locale Info API is a Stage 3 ECMAScript TC39 proposal to enhance the `Intl.Locale` object by exposing locale information, such as week data (first day in a week, weekend start day, weekend end day, minimum day in the first week), and text direction hour cycle used in the locale.
We shipped our implementation in Chrome 99 but later on the proposal made some changes in Stage 3 and moved several getters to functions. We need to remove the deprecated getters and relaunch the renamed functions.

- **Chrome 135 on Windows, macOS, Linux, Android**

Partitioning :visited links history

To eliminate user browsing history leaks, anchor elements are styled as `:visited` only if they have been clicked from this top-level site and frame origin before. On the browser-side, this means that the VisitedLinks hashtable is now partitioned by triple-keying, or by storing the following for each visited link: `<link URL, top-level site, frame origin>`. By only styling links that have been clicked on this site and frame before, the many side-channel attacks that have been developed to obtain `:visited` links styling information are now obsolete, as they no longer provide sites with new information about users.

There is an exception for *self-links*, where links to a site's own pages can be styled as `:visited` even if they have not been clicked on in this exact top-level site and frame origin before. This exemption is only enabled in top-level frames or subframes, which are same-origin with the top-level frame. The privacy benefits above are still achieved because sites already know which of its subpages a user has visited, so no new information is exposed. This was a community-requested exception that improves user experience as well.

- **Chrome 135 on Windows, macOS, Linux, Android**

HSTS tracking prevention

HTTP Strict Transport Security (HSTS) allows sites to declare themselves accessible through secure connections only. As early as Chrome 135, HSTS tracking prevention will mitigate user tracking by third-parties using the HSTS cache. It only allows HSTS upgrades for top-level navigations and blocks HSTS upgrades for sub-resource requests. This will prevent third-party sites using the HSTS cache to track users across the web. For more information, see this HSTS Tracking Prevention explainer on Github.

- **Chrome 135 on Windows, macOS, Linux, Android**

Remove deprecated navigator.xr.supportsSession method

`navigator.xr.supportsSession` was replaced in the WebXR spec by the `navigator.xr.isSessionSupported` method in September of 2019 after receiving feedback on the API shape from the TAG. It has been marked as deprecated in Chromium since then, producing a console warning redirecting developers to the updated API.

Usage of the call is very low, as shown by Chrome Status usage metrics. Additionally, all major frameworks that are used to build WebXR content have been confirmed to have been updated to use the newer call.

- **Chrome 135 on Windows, macOS, Linux, Android**

Strict Same Origin Policy for Storage Access API

Chrome 135 will adjust Storage Access API semantics to strictly follow the Same Origin Policy, to enhance security. This means that using `document.requestStorageAccess()` in a frame will only attach cookies to requests to the iframe's origin (not site) by default.
Note: the CookiesAllowedForUrls policy or Storage Access headers can still be used to unblock cross-site cookies.

- **Chrome 135 on Windows, macOS, Linux, Android**

UI Automation accessibility framework provider on Windows

Starting in Chrome 126, Chrome started 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.
Admins might use the UiAutomationProviderEnabled enterprise policy, available from 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 136, and will be removed in Chrome 137. 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 admins 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 admins may continue to use the UiAutomationProviderEnabled policy to either opt-in early to the new behavior, or to temporarily opt-out through Chrome 136.

- **Chrome 137 on Windows:** The UiAutomationProviderEnabled policy will be removed from Chrome. All clients will use the browser's UI Automation accessibility framework provider.

Remove SwiftShader fallback

As early as Chrome 137, we plan to deprecate automatic fallback to WebGL backed by SwiftShader. WebGL context creation will fail instead of falling back to SwiftShader. We plan to remove SwiftShader fallback 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. You can test and handle WebGL context creation failure and fall back to other web APIs such as Canvas2D or an appropriate message to the user.

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

Disallow spaces in non-file:// URL host

As stated in the WhatWG.org spec, 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. To read more, see the discussion on Github.
This feature will be part of the ongoing work to bring Chromium closer to spec compliance by forbidding spaces in non-file URLs only.

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

SafeBrowsing API v4 to v5 migration

Chrome calls into the SafeBrowsing v4 API will be migrated to call into the v5 API instead. The method names are also different between v4 and v5.
If admins have any v4-specific URL allowlisting to allow network requests to `https://safebrowsing.googleapis.com/v4*`, these should be modified to allow network requests to the whole domain instead: `safebrowsing.googleapis.com`. Otherwise, rejected network requests to the v5 API will cause security regressions for users.

- **Chrome 145 on Android, iOS, ChromeOS, Linux, macOS, Windows**
  This will be a gradual roll-out.

Upcoming Chrome Enterprise Core updates

Apple Extensible SSO support for Chrome on macOS

Chrome 135 on macOS will enable seamless authentication for identity providers that are enabled via an OS-configured Enterprise Single Sign On (SSO) extension. For this initial release, it will allow end users on managed browsers to sign in to any Microsoft Entra-authenticated resources without the need to enter any credentials. Extensible SSO needs to be pre-configured in your environment and deployed with its respective enterprise device management solution. Additional Identity Providers might be supported in the near future.

- **As early as Chrome 135 on macOS**

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, which 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 Getting started with Isolated Web Apps.
In the initial release, IWAs will only be installable through a 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.

Upcoming Chrome Enterprise Premium updates

Refactor DLP rules user experience

We aim to create a more user-friendly and efficient interface for Chrome-specific DLP rules. This involves redesigning the rule creation workflow in the Admin console to better accommodate existing and upcoming security features for Chrome Enterprise Premium customers.

- **Chrome 135 on Windows, macOS, Linux, ChromeOS**

URL filtering on iOS and Android

We will extend the existing URL filtering capabilities from desktop to mobile platforms, providing organizations with the ability to audit, warn, or block certain URLs or categories of URLs from loading on managed Chrome browsers or managed user profiles on mobile devices. This includes ensuring the functionality works seamlessly with Context-Aware Access (CAA) which allows admins to set access policies based on user context (for example, user role, location) and device state (for example, managed device, security compliance).

- **Chrome 137 on Android, iOS**

Reporting connector for mobile

We are working towards feature parity with the desktop version, enabling organizations to monitor and respond to security events on mobile devices, such as unsafe site visits and potential data exfiltration attempts. This helps ensure consistent security and policy enforcement across different platforms.

- **Chrome 136 on Android**
- **Chrome 137 on iOS**

Connectors API

We plan to simplify the setup process for third-party security connectors and enable providers to manage configurations directly from their own UI. This aims to make it easier for organizations to integrate their preferred security tools and services with Chrome, enhancing security and management across different platforms.

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

Previous release notes

Chrome version & targeted Stable channel release date
Chrome 133: January 9, 2025
Chrome 132: January 8, 2025
Chrome 131: November 6, 2024
Chrome 130: October 9, 2024
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.