Chrome 132 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 January 8, 2025, last updated Feb 4, 2025.

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

Chrome 132 release summary

Current Chrome browser changes	Security / Privacy	User productivity / Apps	Management
Search with Google Lens		✓	
Network Service sandboxed on Windows	✓		
Ad-hoc code signatures for Progressive Web App shims on macOS		✓	
Batch upload		✓	
Connectors Disclaimer workflow updates	✓		
DownloadRestrictions is stricter on file type restrictions	✓		
Updates to desktop identity model		✓	
HTTPS-First Mode for Typically Secure Users	✓		
Passkeys on iOS	✓	✓	
Password Leak Toggle Move	✓		
Removal of old Headless from the Chrome binary		✓	
Remove ThirdPartyBlockingEnabled policy			✓
Remove enterprise policy used for legacy same site behavior			✓
Support non-special scheme URLs	✓		
Translate for Search with Google Lens		✓	
User Link capturing on PWAs		✓	✓
Keyboard-focusable scroll containers		✓	
Remove prefixed HTMLVideoElement fullscreen APIs		✓	

Throw exception for popovers or dialogs in non-active documents		✓	
Current Chrome Enterprise Core changes	**Security/Privacy**	**User productivity/Apps**	**Management**
Customized Chrome Web Store for enterprises		✓	✓
New Chrome user management capabilities in the Admin console)			✓
Copy Source conditions in Chrome DLP Paste rule	✓		
Generating insights for Chrome DevTools Console warnings and errors			✓
Professional Chrome Enterprise Administrator certification			✓
Server Root Certificates for Chrome Enterprise	✓		✓
Legacy Technology Report			✓
Recommended policies (user can override a policy value)		✓	✓
Updated Managed browser list: Most Recent Google Update Activity			✓
Current Chrome Enterprise Premium changes	**Security/Privacy**	**User productivity/Apps**	**Management**
File Download Encryption for DLP Rules	✓		
Upcoming Chrome browser changes	**Security / Privacy**	**User productivity / Apps**	**Management**
Disallow spaces in non-file:// URL hosts	✓		
Read aloud in Reading mode in Chrome 133		✓	
Tab freezing on Energy saver		✓	
Deprecate getters of Intl Locale Info	✓		
Freezing on Energy Saver		✓	

Popover invoker and anchor positioning improvements		✓	
Remove Chrome Welcome page triggering via initial prefs first run tabs	✓		
Remove nonstandard getUserMedia audio constraints	✓		
Remove SwiftShader fallback	✓		
Privacy & security panel in Chrome DevTools	✓	✓	
Chrome Sync will stop supporting Chrome versions that are more than four years old		✓	
V8 security setting	✓		
New option in HttpsOnlyMode policy	✓		✓
SafeBrowsing API v4 → SafeBrowsing API v5 migration	✓		
Blob URL partitioning: Fetching or Navigation	✓		
SharedWorker script inherit controller for blob script URL	✓		
Deprecate mutation events		✓	
UI Automation accessibility framework provider on Windows		✓	
Customizing managed profiles with custom logo and label		✓	✓
Upcoming Chrome Enterprise Core changes	**Security / Privacy**	**User productivity / Apps**	**Management**
New Chrome Enterprise Companion App			✓
Upcoming Chrome Enterprise Premium changes	**Security/Privacy**	**User productivity/Apps**	**Management**
Screenshot prevention V2	✓		
URL filtering on iOS/Android	✓		
Reporting connector for mobile	✓		

Refactor DLP rules UX	✓		
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 version release notes

Current Chrome browser changes

Search with Google Lens

In Chrome 132, we begin to roll out this enhanced feature across all platforms. 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 by right-clicking on an image and selecting **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**. 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, mac, Windows: Rollout of the feature at 1% Stable
- Chrome 127 on ChromeOS, Linux, mac, Windows: Rollout to 100% Stable
- Chrome 131 on iOS: Rollout of the feature at 1% Stable
- **Chrome 132 on ChromeOS, Linux, mac, Windows:** Rollout of the expanded feature at 1% Stable

Network Service sandboxed on Windows

To improve security and reliability, the network service, already running in its own process, is now sandboxed on Windows. As part of this, third-party code that is currently able to tamper with the network service may be prevented from doing so. This might cause interoperability issues with software that injects code into Chrome's process space, such as Data Loss Prevention software. The NetworkServiceSandboxEnabled policy allows you to disable the sandbox if incompatibilities are discovered. You can test the sandbox in your environment using these instructions.
You can report any issues you encounter.

- **Chrome 132 on Windows**
  Network Service sandboxed on Windows

Ad-hoc code signatures for Progressive Web App shims on macOS

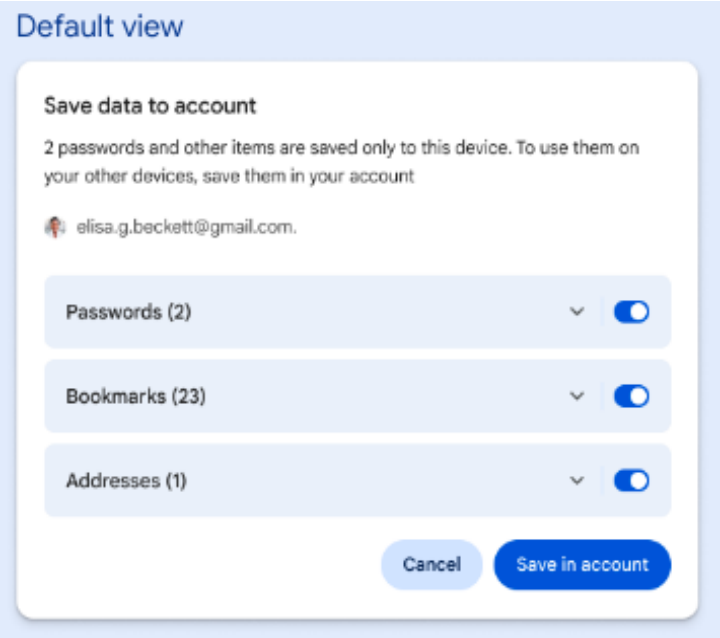
Code signatures for the application shims that are created when installing a Progressive Web App on macOS are changing to use ad-hoc code signatures that are created when the application is installed. The code signature is used by macOS as part of the application's identity. These ad-hoc signatures result in each PWA app shim having a unique identity to macOS, where previously every PWA looked like the same application to macOS.
This update addresses problems when attempting to include multiple Progressive Web Applications in macOS's **Open at Login** preference pane, and permits future improvements to handling of user notifications within PWAs on macOS.
Admins should test for compatibility with any endpoint security or binary authorization tools they use (such as Santa). The feature can be enabled for this testing using `chrome://flags/#use-adhoc-signing-for-web-app-shims`. They can then install a Progressive Web App and ensure that it launches as expected.
If there is an incompatibility between the feature and their current security policies, the AdHocCodeSigningForPWAsEnabled policy can be used to disable the feature while they deploy an updated endpoint security policy. The enterprise policy is intended to be used to disable the feature only until endpoint security policies have been updated, at which point it should be unset.

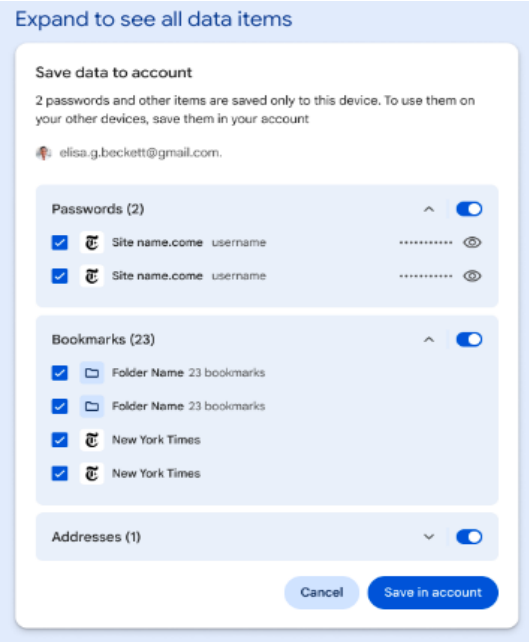
- Chrome 129 on macOS
  Feature disabled behind a flag (`chrome://flags/#use-adhoc-signing-for-web-app-shims`) so that enterprises can test for compatibility with their endpoint security tools, such as Santa. If it is not currently compatible they can disable the feature via the enterprise policy while they update their endpoint security configurations. The enterprise policy is intended to be used to disable the feature only until endpoint security policies have been updated.
- **Chrome 132 on macOS**
  This feature will begin to roll out to stable, starting at 1% rollout.

Batch upload

Since Chrome 128, users have access to their passwords and addresses from their Google Account at the point of sign-in (in addition to their payment methods, which was an existing sign-in feature). These data-types have two distinct storages: local and account. With Chrome 132, we are providing users an opportunity to upload any local data they have to their Google Account. This will first be made available for passwords and addresses and will be expanded to include other data types in the future.
The SyncTypesListDisabled policy applies equally to sync and data upload. Therefore, if either passwords or addresses are disabled, they are not made available for upload in the batch uploader.

- **Chrome 132 on Linux, macOS, Windows**





Connectors Disclaimer workflow updates

We have made updates to our Terms of Service for Chrome Enterprise Core that includes a section on 3rd party data-sharing. These updates improve the sign-up flow for Chrome Browser Enterprise connectors.

- **Chrome 132 on ChromeOS, Linux, macOS, Windowsx**

DownloadRestrictions is stricter on file type restrictions

You can control downloads within your organization using the DownloadRestrictions policy, with options to allow you select an appropriate level of file type restrictions:

0 = No special restrictions. Default.

1 = Block malicious downloads and dangerous file types.

2 = Block malicious downloads, uncommon or unwanted downloads and dangerous file types.

3 = Block all downloads.

4 = Block malicious downloads. Recommended.

Where option value = 1, this means:

1. Chrome browser blocks malicious files flagged by the Safe Browsing server AND blocks all dangerous file types. Only recommended for OUs, browsers, or users that have a high tolerance for false positives.

Where option value = 2, this means:

2. Chrome browser blocks malicious files flagged by the Safe Browsing server AND blocks uncommon or unwanted files flagged by the Safe Browsing server AND blocks all dangerous file types. Only recommended for OUs, browsers, or users that have a high tolerance for false positives.

Previously, the *dangerous file types* blocking was not being correctly applied by Chrome, and this has now been fixed. This means, however, that the policy is now much stricter on certain file types that could be dangerous to the user, like `.exe` or `.msi` files on Windows. If this induces too many false positives, you can leave the policy unset or set the policy value to 4.

- **Chrome 132 on Windows**

Updates to Chrome Identity model on desktop

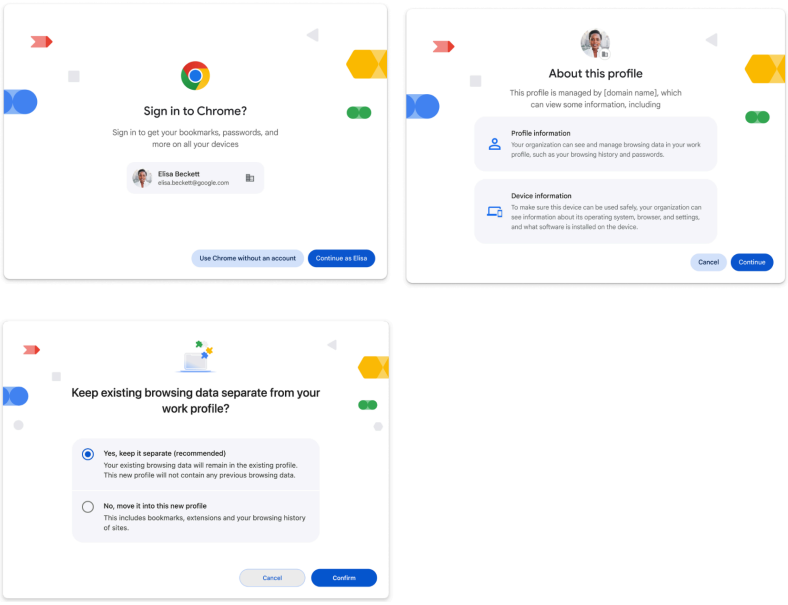
Instead of having to set up Chrome sync on your device, you can now simply sign in to Chrome to access and save items to your Google Account. This new identity model on Desktop also includes an explicit sign-in to Chrome from a web sign-in.
Signing into the web (using Gmail) prompts users to sign-in to Chrome. If they decline, they won't be signed-in to Chrome, only to the web.

- If they accept, profile management (user-based policies), payments (already available today), passwords, addresses, bookmarks*, extensions*, search engine prefs*, themes* and PWAs* will be enabled.
- If they decline, Chrome can still use the sign-in credentials to facilitate a one-click sign-in to Chrome.
- Synchronizing history, Open tabs and tab groups still exist behind a separate opt-in for now.
- Invalidated credentials (e.g. signing out of the web or remote sign-out) will put Chrome in a 'pending' state, previously 'sync paused'. Autofill data will not be

available from the user's Google Account. Users in this state will be prompted to "Verify it's you" in the Chrome toolbar.

*These data types will be enabled behind sign-in (instead of sync opt in) in upcoming Chrome milestones.
Web sign-in intercepts can be controlled using the SigninInterceptionEnabled policy. For more details, see Force users to create a separate profile.

- **Chrome 132 on Linux, macOS, Windows** Roll-out starts



HTTPS-First Mode for Typically Secure Users

HTTPS-First Mode (HFM) enables a default-HTTPS experience in Chrome by automatically upgrading sites to HTTPS. If a site doesn't support HTTPS, HFM shows a warning before loading the HTTP version. HFM significantly improves the security guarantees of HTTPS by preventing loading of HTTP URLs without explicit user approval.
HFM for typically secure users (this feature) is a heuristic that can automatically enable HFM for the user if the user has a typically secure browsing pattern. Typically secure browsing pattern is determined by keeping track of HTTPS-Upgrade fallbacks (i.e. failed HTTPS

Upgrades, which would be HFM interstitials if the user manually enabled HFM) and a few other factors such as profile age and overall site engagement score.
If these signals indicate that the user mostly visits secure sites, the heuristic will automatically enable HFM setting. HFM interstitials caused by this heuristic will display a custom message. The user can disable HFM by simply turning off the UI setting and the heuristic will never kick in again.
This feature can be controlled using the existing enterprise policies HttpsOnlyMode and HttpAllowlist.

- **Chrome 132 on ChromeOS, Linux, macOS, Windows, Fuchsia**

Passkeys on iOS

Passkeys are a more secure alternative to passwords. Unlike passwords, which can be phished or guessed, passkeys let users authenticate to sites and apps using public-key cryptography, as defined in the Webauthn standard.
Google Password Manager passkeys are already available in Chrome on other platforms; this launch brings them to the iOS platform, through enhancements to Chrome's existing Credential Provider Extension ("Passwords in Other Apps"). Using the Extension, Google Password Manager passkeys can be used to sign in to pages in Chrome and other browsers, as well as to native apps.
Passkeys are saved to a user's Google Account and available whenever the user is signed in to Chrome. Relevant enterprise policies such as BrowserSignin, SyncTypesListDisabled and PasswordManagerEnabled will continue to work as before and can be used to configure whether users can use and save passwords in their Google Account.

- **Chrome 132 on iOS**

Password Leak toggle move

The PasswordLeakDetectionEnabled toggle that was originally found on `chrome://settings/security` is moving from under the standard protection heading to further down on the page under the **Advanced** section.

This feature will also remove the PasswordLeakDetectionEnabled dependency on a user's safe browsing status. Previously, a user who had no protection or no safe browsing would not get the PasswordLeakDetectionEnabled functionality. Now, a user has free choice to select the PasswordLeakDetectionEnabled toggle regardless of their safe browsing protection level.

- **Chrome 132 on ChromeOS, Linux, macOS, Windows, Fuchsia**

Removal of old Headless from the Chrome binary

Running Chrome with `--headless=old` no longer launches the old Headless mode, and instead prints the following log message:
`Old Headless mode has been removed from the Chrome binary. Please use the new Headless mode or the chrome-headless-shell which is a standalone implementation of the old Headless mode.`

- **Chrome 132 on Linux, macOS, Windows**

Remove ThirdPartyBlockingEnabled policy

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

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

Remove enterprise policy used for legacy same site behavior

In Chrome 79, we introduced the LegacySameSiteCookieBehaviorEnabledForDomainList policy to revert the SameSite behavior of cookies to legacy behavior on the specified

domains. The LegacySameSiteCookieBehaviorEnabledForDomainList policy's lifetime has been extended and will be removed in Chrome 132.

- **Chrome 132 on Android, ChromeOS, Linux, macOS, Windows**
  Remove LegacySameSiteCookieBehaviorEnabledForDomainList policy

Support non-special scheme URLs

Chrome 130 supports non-special scheme URLs, for example, git://example.com/path. Previously, the Chromium URL parser didn't support non-special URLs. The parser parses non-special URLs as if they had an opaque path, which is not aligned with the URL standard. Now, the Chromium URL parser parses non-special URLs correctly, following the URL standard. For more details, see http://bit.ly/url-non-special.

- Chrome 130 on Windows, macOS, Linux, Android
- **Chrome 132 on Windows, macOS, Linux, Android**
- Chrome 134 on Windows, macOS, Linux, Android: Feature flag being removed

Translate for Search with Google Lens

Augmented Reality-based (AR) Translation capabilities are being implemented to the Search with Google Lens feature. The LensOverlaySettings enterprise policy is in place allowing you to turn the feature on or off.

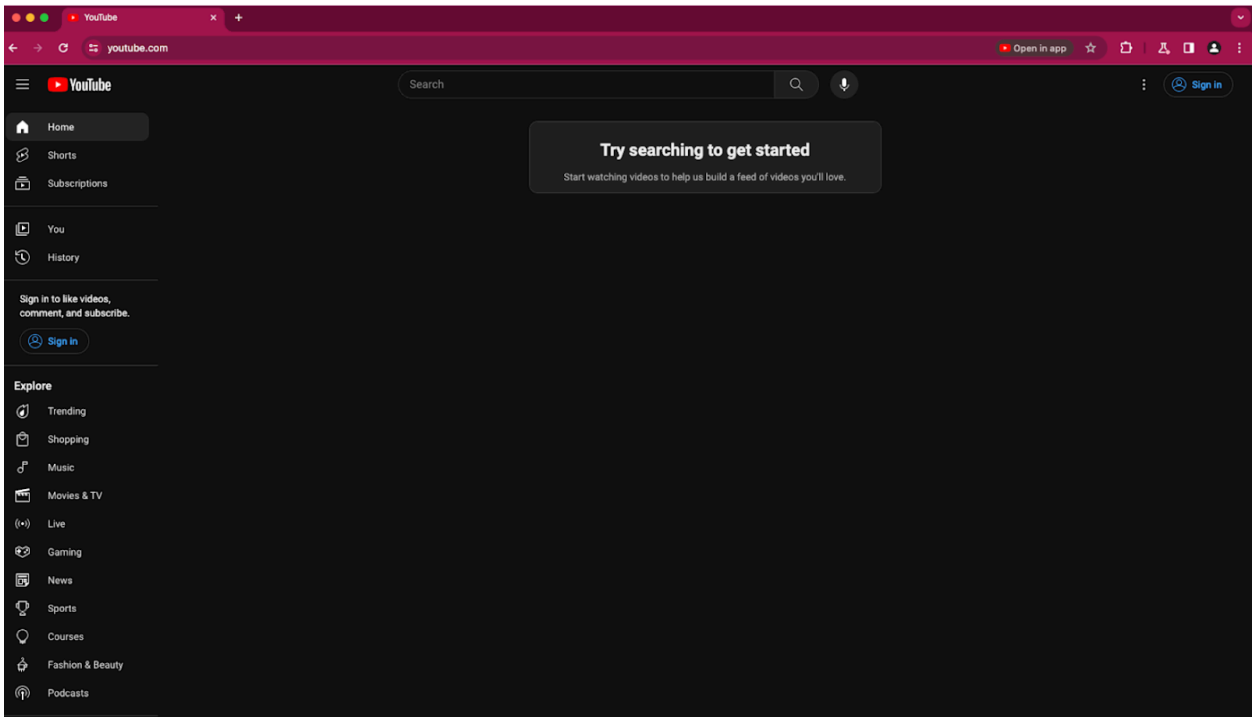
- Chrome 131 on ChromeOS, Linux, macOS, Windows
- **Chrome 132 on ChromeOS, Linux, macOS, Windows**
  In Chrome 131, the translate feature was introduced. In Chrome 132, the translate feature is being expanded with additional language support.

User Link capturing on PWAs

Web links automatically direct users to installed web apps. To better align with users' expectations around installed web apps, Chrome makes it easier to move between the

browser and installed web apps. When the user clicks a link that could be handled by an installed web app, Chrome adds a chip in the address bar to suggest switching over to the app. When the user clicks the chip, this either launches the app directly, or opens a grid of apps that can support that link. For some users, clicking a link always automatically opens the app.
When some users click a link, it always opens in an installed PWA, while some users see the link open in a new tab with a chip in the address bar, clicking on which will launch the app. A flag is available to control this feature:
`chrome://flags/#enable-user-link-capturing-pwa`.

- **Chrome 132 on Linux, macOS, Windows**
  Launch to 100% of Stable with either a default on (always launch apps on link clicks) or a default off (always open in a tab, only launch if the user clicks on chip on address bar).



Keyboard-focusable scroll containers

Improves accessibility by making scroll containers focusable using sequential focus navigation. Today, the tab key doesn't focus scrollers unless tabIndex is explicitly set to 0 or more.
By making scrollers focusable by default, users who can't (or don't want to) use a mouse will be able to focus clipped content using a keyboard's tab and arrow keys. This behavior is enabled only if the scroller does not contain any keyboard focusable children. This logic is necessary so we don't cause regressions for existing focusable elements that might exist within a scroller like a <textarea>.

Note: The previous rollout of this feature (started first in Chrome 127 and again in Chrome 130) was stopped due to an accessibility regression, which should be fixed in the current implementation shipping in Chrome 132.

- **Chrome 132 on Windows, macOS, Linux, Android**

Remove Prefixed HTMLVideoElement Fullscreen APIs

The prefixed HTMLVideoElement-specific fullscreen APIs have been deprecated since Chrome 38. They were replaced by the `Element.requestFullscreen()` API, which first shipped un-prefixed in Chrome 71, in 2018. As of 2024, most browsers have had support for the un-prefixed APIs for a few years now.
This feature tracks removing the following APIs from HTMLVideoElement:

- readonly attribute boolean webkitSupportsFullscreen;
- readonly attribute boolean webkitDisplayingFullscreen;
- void webkitEnterFullscreen();
- void webkitExitFullscreen();

// Note the different capitalization of the "S" in FullScreen.

- void webkitEnterFullScreen();
- void webkitExitFullScreen();

These methods are now only aliases for the modern API. Their use has declined steadily over the years.

- **Chrome 132 on Windows, macOS, Linux, Android**

Throw exception for popovers or dialogs in non-active documents

This is a corner case change that does not impact developers. Previously calling `showPopover()` or `showModal()` on a popover or dialog that resides within an inactive document would silently fail. This means that no exception would be thrown, but since the document is inactive, no popover or dialog would be shown. These situations now throw InvalidStateError. For more information, see the relevant spec pull request on Github.

- **Chrome 132 on Windows, macOS, Linux, Android**

New policies in Chrome browser

Policy	Description
CACertificates	TLS certificates that should be trusted for server authentication
CACertificateManagementAllowed	Allow users to manage all certificates
CADistrustedCertificates	TLS certificates that should be distrusted for server authentication
CAHintCertificates	TLS certificates that are not trusted or distrusted but can be used in path-building for server authentication
CACertificatesWithConstraints	TLS certificates that should be trusted for server authentication with constraints
PasswordManagerPasskeysEnabled	Enable saving passkeys to the password manager
SharedWorkerBlobURLFixEnabled	Make SharedWorker blob URL behavior aligned with the specification
TranslatorAPIAllowed	Allows the use of Translator API

Removed policies in Chrome browser

Policy	Description
LegacySameSiteCookieBehaviorEnabledForDomainList	Revert to legacy behavior for cookies on all sites
NativeClientForceAllowed	Forces Native Client (NaCl) to be allowed to run
PrefixedVideoFullscreenApiAvailability	Manage the deprecated prefixed video fullscreen API's availability

Current Chrome Enterprise Core changes

Customized Chrome Web Store for enterprises

Admins can leverage new settings to customize the Chrome Web Store for their managed users, which includes the ability to:

- Add company logos
- Add hero banners and custom announcements
- Curate extension collections
- Hide extension categories

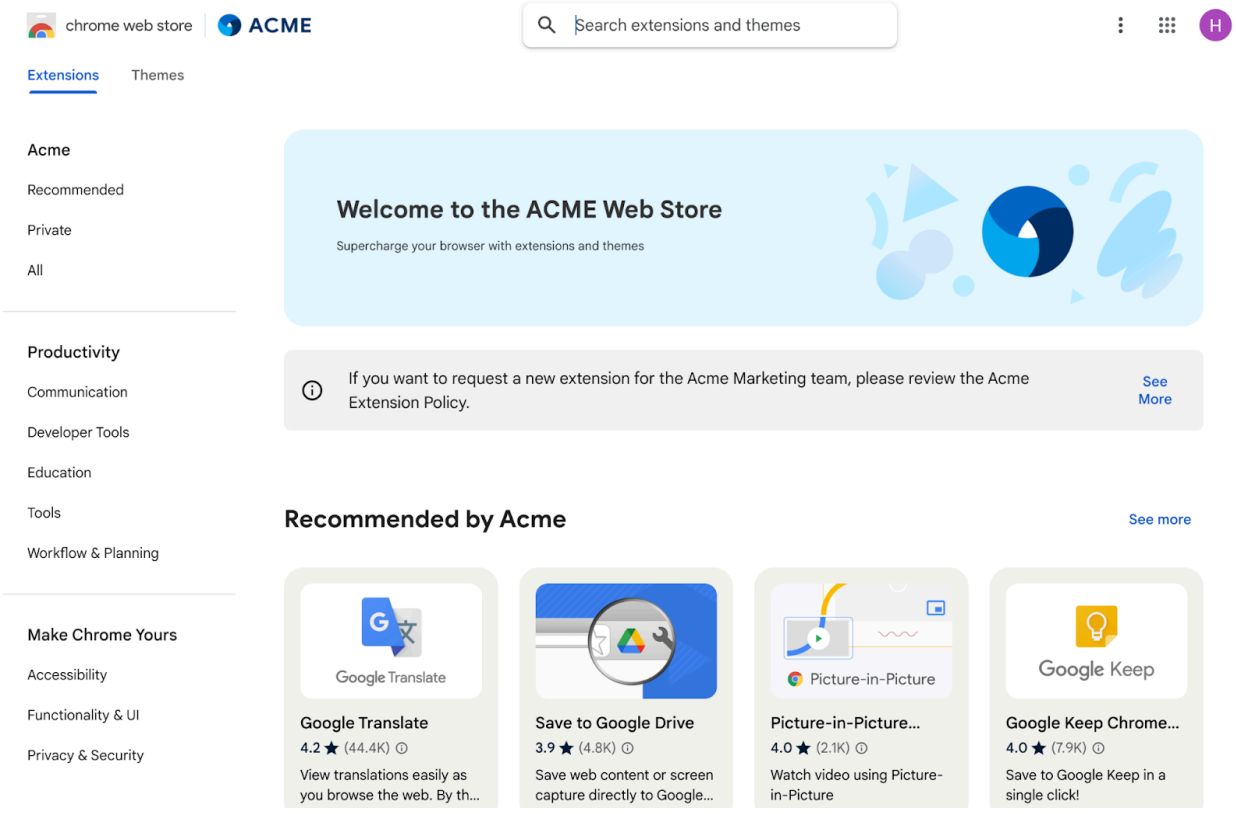
These settings are configurable via the Admin console (learn more) and are available to all signed-in managed users (users signed-in to the Chrome Web Store with a managed Google Account).

Additionally, all managed users who sign in to the Chrome Web Store will see the following changes:

- New tags for items “Blocked by their admin” when searching for an item
- Private domain item search and advanced filtering capabilities
- Private items and recommended items are relocated to the “Extensions” tab

Enrolled browsers (without the need to sign in) will be supported later in 2025.

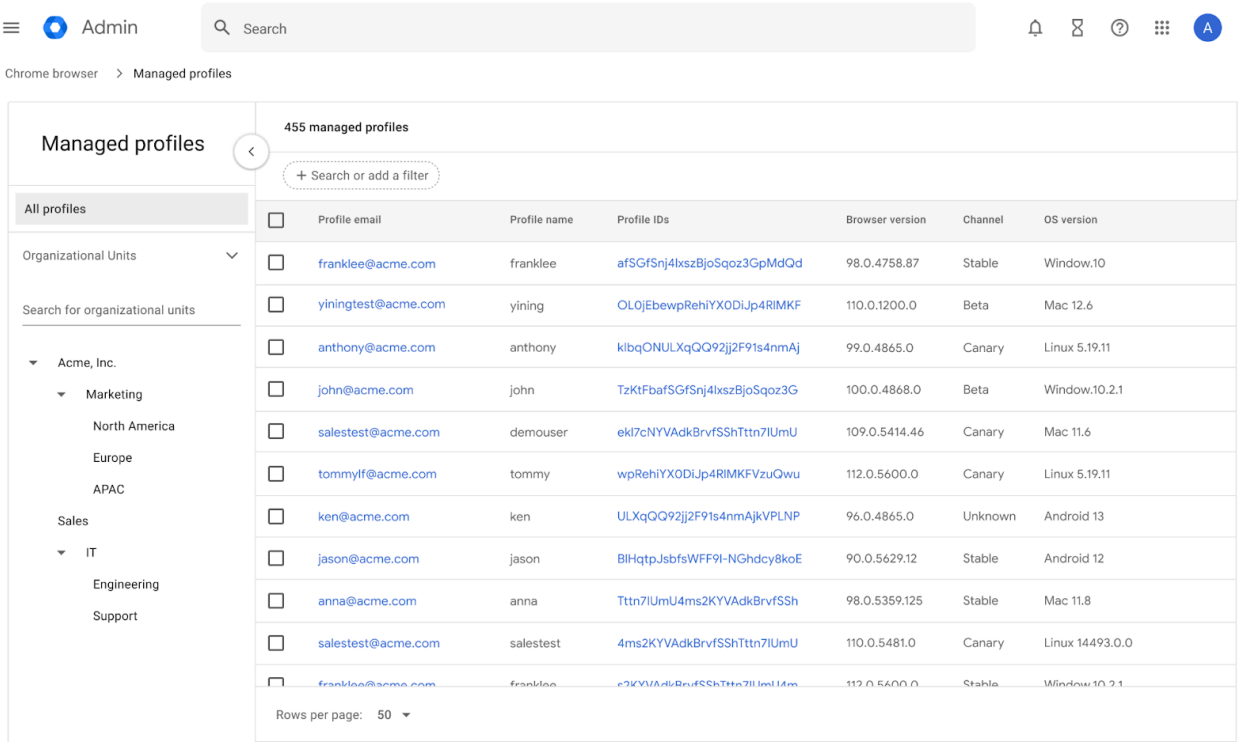
- **Chrome 132 on ChromeOS, Linux, macOS, Windows**



New Chrome user management capabilities in the Admin console

Admins can now get more visibility into Chrome user profiles in their organization with a new profile list and reporting features for signed-in Google Accounts. This centralized view in the Google Admin console provides detailed reports about user profiles in your organization, including profile information, browser version, applied policies and installed extensions. For more details, see View Chrome browser profile details.
To get started, IT administrators can simply turn on the new Chrome Managed profile reporting policy to view the reporting information about managed profiles.

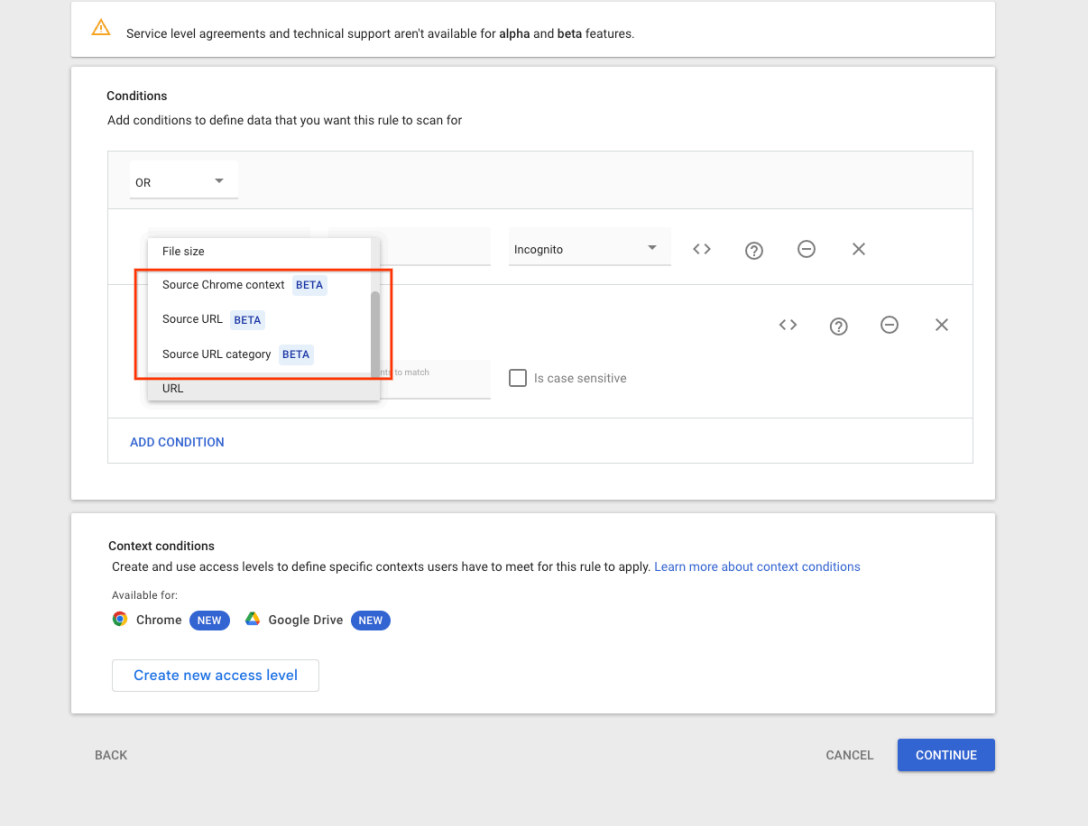
- **Chrome 132 on Android, Linux, macOS, Windows**



Copy Source conditions in Chrome DLP paste rule

In this feature, we are adding copy source conditions, namely Source URL, Source URL category and Source Chrome context in Paste trigger rule for all customers. Admins can now create paste rules using the OnBulkDataEntryEnterpriseConnector policy, with conditions matching where the data or text being pasted is copied from.
For more details, see Use Chrome Enterprise Premium to integrate DLP with Chrome.

- **Chrome 132 on ChromeOS, Linux, macOS, Windows**
  In this rollout, we are adding copy source conditions, namely Source URL category and Source Chrome context in Paste trigger rule for all customers. Admins will be able to create Paste rules (policy) with conditions matching where the data/text being pasted is copied from.



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.

Professional Chrome Enterprise Administrator certification

For organizations using Chrome Enterprise Core, we offer a new certification opportunity – the **Professional Chrome Enterprise Administrator** certification. This certification is designed to validate your expertise in managing Chrome Enterprise browser environments, with a focus on using Chrome Enterprise Core to implement policies, establish controls, and analyze reports.
Designed for Chrome Enterprise Administrators with at least one year of experience with application, policy, and endpoint management, the exam is a two-hour exam consisting of about 70 multiple choice questions. The exam assesses your familiarity with both local and cloud-based solutions to manage, maintain, troubleshoot, secure, and integrate with services related to Chrome.
Google is waiving the exam fee of $125 until March 2025 and admins can now take the Professional Chrome Enterprise Administrator certification exam for free.

- **Chrome 132 on Android, iOS, ChromeOS**

Server Root Certificates for Chrome Enterprise

Chrome 132 adds the capability for enterprise customers or partners to deploy custom Server Root Certificates or Trust Anchors into Chrome's Root Store on fully Managed Browsers via Chrome Browser Cloud Management or into Managed Chrome Profiles on Managed or Unmanaged devices.

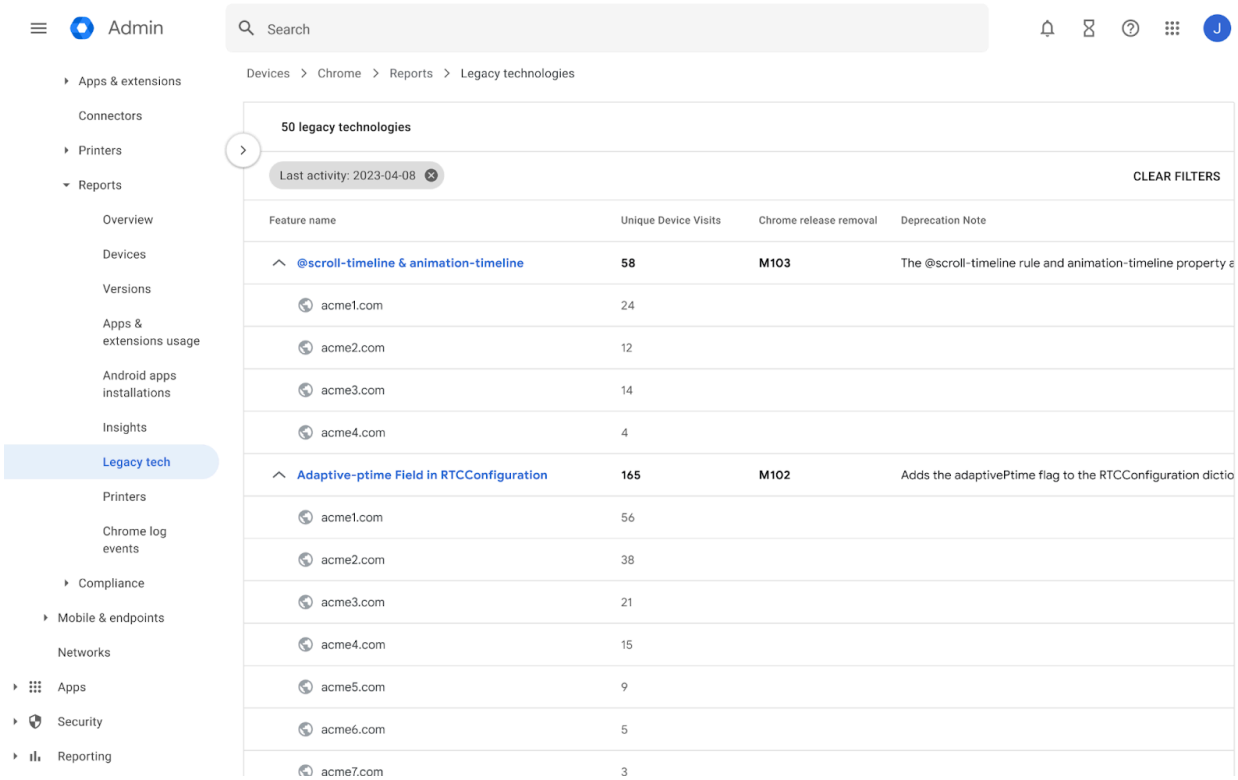
- **Chrome 132 on Linux, macOS, Windows**

Legacy Technology Report

The Legacy Tech Report allows IT administrators to have visibility on websites (both internal and external) that are using deprecated or soon-to-be deprecated technologies (for example, CSS property changes or older security protocols like TLS 1.0 & 1.1). This launch is available in the Google Admin console to all Chrome Enterprise Core. For more details, see [View legacy technology usage details].

This gives an opportunity to IT administrators to have the ability to work with developers to proactively plan technical migrations before a deprecation goes into effect.

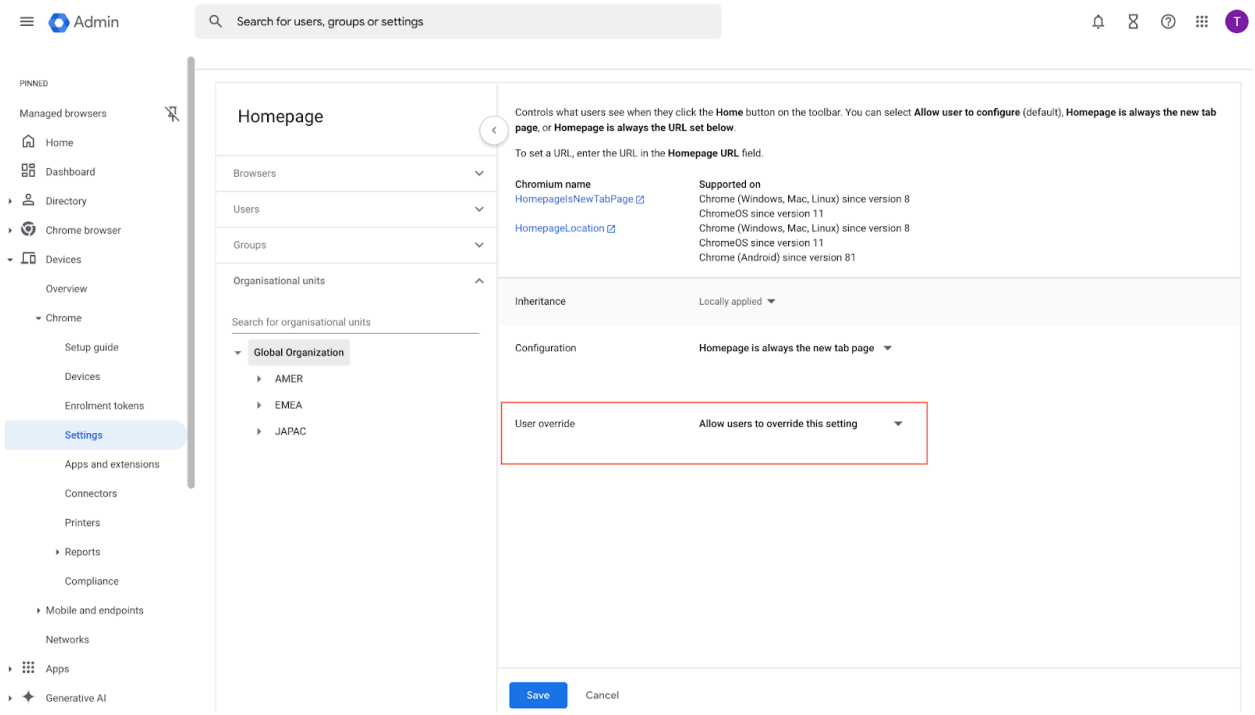
- **Chrome 132 on Linux, macOS, Windows**



Recommended policies (users can override a policy value)

Chrome is introducing 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.

> **On Chrome 132**: the following policies are supported: ShowHomeButton, HomepageIsNewTabPage, HomepageLocation, DownloadRestrictions, SafeBrowsingProtectionLevel, AlwaysOpenPdfExternally, BackgroundModeEnabled, MetricsReportingEnabled, WarnBeforeQuitting, PrintPreviewUseSystemDefaultPrinter, BatterySaverModeAvailability
>
> **As early as Chrome 133**: the following policies will be supported: ImportAutofillFormData, ImportBookmarks, ImportHistory, ImportSavedPasswords, ImportSearchEngine



Updated managed browser list: Most recent Google Update activity

Chrome Enterprise Core is adding the **Most recent Google Update activity** column on the managed browser list. The **Most recent Google Update activity** represents the last recorded time when the GoogleUpdater service interacted with a managed browser.

- **Chrome 132 on Linux, macOS, Windows**

Current Chrome Enterprise Premium changes

File download encryption for DLP Rules

When a file downloaded Data loss Prevention (DLP) rule is triggered, the file is now encrypted on the fly to ensure that end users cannot access that file when a verdict is being returned. This means that users can no longer bypass the rule by moving or renaming the file.
This feature is gated by the existing policy OnFileDownloadedEnterpriseConnector and is only available to Chrome Enterprise Premium users.

- **Chrome 132 on ChromeOS, Linux, macOS, Windows**

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

Disallow spaces in non-file:// URL hosts

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 (see the discussion on Github).
This feature will be part of the ongoing work to bring Chromium closer to spec compliance by forbidding spaces for non-file URLs only.

- **Chrome 133 on Android, ChromeOS, Linux, macOS, Windows, Fuchsia**

Read aloud in Reading mode in Chrome 133

Reading mode is a side-panel feature that provides a simplified view of text-dense web pages. Reading mode will include a Read aloud feature which will allow users to hear the text they are reading spoken out loud. Users will be able to choose different natural voices and speeds, and see visual highlights.

- **Chrome 133 on Linux, macOS, Windows**

Tab freezing on Energy saver

When Energy saver is active, Chrome will freeze a tab that has been hidden and silent for >5 minutes and uses a lot of CPU, unless:

- The tab provides audio- or video- conferencing functionality (detected via microphone, camera or screen/window/tab capture, or an RTCPeerConnection with an open RTCDataChannel or a live MediaStreamTrack).
- The tab controls an external device (detected via usage of Web USB, Web Bluetooth, Web HID or Web Serial).

This will extend battery life and speed up Chrome through reduced CPU usage.
The feature can be tested in Chrome 131 via `chrome://flags/#freezing-on-energy-saver`. Alternatively, it can be tested with `chrome://flags/#freezing-on-energy-saver-testing`, which simulates Energy saver being active and all tabs using a lot of CPU; this allows you to verify whether tabs are eligible for freezing and would be frozen if using a lot of CPU.

- Energy saver availability can be controlled via the BatterySaverModeAvailability policy (this change has no effect when Energy saver is inactive).
- **Chrome 133 on ChromeOS, Linux, macOS, Windows**
  The feature will start rolling out to 1% of stable in Chrome 133.

Deprecate getters of Intl Locale Info

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 133 on Windows, macOS, Linux, Android**

Popover invoker and anchor positioning improvements

This update represents the following related set of changes, which were resolved and landed

1. add an imperative way to set invoker relationships between popovers:

```
popover.showPopover({source})
```

2. invoker relationships create implicit anchor element references.

- **Chrome 133 on Android, ChromeOS, Linux, macOS, Windows, Fuchsia**

Remove Chrome Welcome page triggering via initial prefs first run tabs

Including `chrome://welcome` in the `first_run_tabs` property of the `initial_preferences` file will now have no effect. This is removed because that page is redundant with the First Run Experience that triggers on desktop platforms.
For more details about the context of the `initial_preferences` file, see Configuring Other Preferences.

- **Chrome 133 on Windows, macOS, Linux**

Remove nonstandard getUserMedia audio constraints

Blink supports a number of nonstandard goog-prefixed constraints for `getUserMedia` from some time before 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 133 on Windows, macOS, Linux, Android**

Remove SwiftShader fallback

Allowing automatic fallback to WebGL backed by SwiftShader is deprecated and WebGL context creation will fail 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. 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 133 on Windows, macOS, Linux, Android**

Privacy & security panel in Chrome DevTools

Starting in Chrome 133, developers will be able to use the new **Privacy & security** panel in Chrome DevTools to test how their site will behave when third-party cookies are limited. Developers will be able to temporarily limit third-party cookies, observe how their site behaves, and review the status of third-party cookies on their site.
This feature will not make any permanent changes to existing enterprise policies, but it will let third-party cookie related enterprise policies (that is, BlockThirdPartyCookies and

CookiesAllowedForUrls) be temporarily overridden to be more restrictive. If your enterprise policy already blocks third-party cookies using BlockThirdPartyCookies, this feature will be disabled.

The new **Privacy & security** panel will replace the existing **Security** panel. TLS connection and certificate information will continue to be available on the **Security** tab in the **Privacy & security** panel.

- **Chrome 133 on ChromeOS, Linux, macOS, Windows**

Chrome Sync to end support for Chrome versions more than four years old

Starting in February 2025, Chrome Sync (using and saving data in your Google Account) will no longer support Chrome versions that are more than four years old. You need to upgrade to a more recent version of Chrome if you want to continue using Chrome Sync.

- **Chrome 133 on Android, iOS, ChromeOS, Linux, macOS, Windows**
  This change affects only the old versions of Chrome and will be rolled out server-side. Chrome 133 is specified only to reflect the timeline when the change will make an effect.

V8 Security Setting

Add a setting on `chrome://settings/security` to disable the V8 JIT optimizers, in order to reduce the attack surface of Chrome. This maintains compatibility with Web Assembly. This behavior continues to be controlled by the DefaultJavaScriptJitSetting enterprise policy, and the associated JavaScriptJitAllowedForSites and JavaScriptJitBlockedForSites policies.

- Chrome 122 on ChromeOS,, Linux, macOS, Windows, Fuchsia
  The setting rolls out in Chrome 121. The enterprise policies have been available since Chrome 93.

- **Chrome 133 on Android**
  The setting is available on Android in Chrome 133, under Site Settings. The enterprise policies are no longer marked experimental.

New option in HttpsOnlyMode policy

Ask Before HTTP (ABH, née HTTPS Only/First Modes) is a setting that tells Chrome to ask for user consent before sending insecure HTTP content over the wire. The HttpsOnlyMod policy allows force-enabling, or force-disabling, ABH.
In Chrome 129, we are adding a new middle-ground variant of ABH called "balanced mode". This variant aims to reduce user inconvenience by working like (strict) ABH most of the time, but not asking when Chrome knows that an HTTPS connection isn't possible (such as when connecting to a single-label hostname like internal/).
We are adding a force_balanced_enabled policy option to allow force-enabling this new variant. Setting force_balanced_enabled on browsers before Chrome 129 will result in the default behavior, which places no enterprise restrictions on the ABH setting.
To avoid unexpected impact, if you have previously set force_enabled, we recommend not setting force_balanced_enabled until your entire fleet has upgraded to Chrome 129 or higher. If you are not migrating from force_enabled to force_balanced_enabled, you will be unaffected by this change.

- Chrome 129 on ChromeOS, Linux, macOS, Windows, Fuchsia
- **Chrome 133 on Android**

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 134 on Android, iOS, ChromeOS, Linux, macOS, Windows:** This will be a gradual rollout.

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 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 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 we will pursue spec updates to reflect both of these changes.
This change can be temporarily reverted by setting the **PartitionedBlobURLUsage** policy which will be available in Chrome 134. The policy will be deprecated when the other storage partitioning related enterprise policies are deprecated.

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

SharedWorker script inherit controller for blob script URL

Service Workers should inherit controllers for the blob URL. However, existing code allows only dedicated workers to inherit the controller, and shared workers do not inherit the controller.
This is the fix to make Chromium behavior adjust to the specification.
An enterprise policy SharedWorkerBlobURLFixEnabled is available to control this feature.

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

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. Starting in Chrome 124, a temporary enterprise policy, MutationEventsEnabled, will be available to re-enable deprecated or removed mutation events. If you encounter any issues, file a bug here.

Mutation event support will be disabled by default starting in Chrome 127, around July 30, 2024. Code should be 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 through Chrome 134, ending March 25, 2025.
- A MutationEventsEnabled enterprise policy can also be used for the same purpose, also through Chrome 134.

To read more, see this blog post. Report any issues here.

- **Chrome 135 on Android, Linux, macOS, Windows:** The MutationEventsEnabled enterprise policy will be deprecated.

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.

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 Chrome 133, these policies will be available to customize the logo and label shown on a managed profile.
Starting Chrome 134, 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 133 on macOS, Windows**
  Policies to customize the toolbar label and icon (in profile menu)
- Chrome 134: 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.

Upcoming Chrome Enterprise Core changes

- **New Chrome Enterprise Companion App**

  Chrome Enterprise Companion App (CECA) 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 133 on Windows, macOS**

Upcoming Chrome Enterprise Premium changes

Screenshot prevention

We plan to enhance the existing screenshot prevention feature by extending screen-sharing blocking to meeting apps like Google Meet, Zoom, Teams, and Slack. We will build upon the

successful release of data protection controls by adding key features and addressing gaps and user feedback.

- **Chrome 134 on Windows, Mac**

URL filtering on iOS andAndroid

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 135 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 135 on Android, iOS**

Refactor DLP rules UX

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 134 on Windows, Mac, Linux, CrOS**

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 135 on Windows, Mac, Linux, CrOS**

Previous release notes

Chrome version & targeted Stable channel release date
Chrome 131: November 6, 2024
Chrome 130: October 9, 2024
Chrome 129: September 11, 2024
Chrome 128: August 14, 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