chrome enterprise

Chrome 124 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 April 10, 2024.

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

Chrome 124 release summary **2**
Current Chrome version release notes **6**
Chrome browser updates 6
ChromeOS updates 18
Admin console updates 20
Coming soon **23**
Upcoming Chrome browser changes 23
Upcoming ChromeOS changes 33
Upcoming Admin console changes 33
Previous release notes **36**
Additional resources **36**
Still need help? **36**

Chrome 124 release summary

Chrome browser updates	Security/Privacy	User productivity/Apps	Management
Chrome Enterprise Premium product launch	✓		✓
Chrome Browser Cloud Management is now Chrome Enterprise Core	✓		✓
Watermarking (trusted tester)	✓		
Chrome Third-Party Cookie Deprecation (3PCD)	✓		
Permissions prompt for Web MIDI API	✓		
Two Chrome extensions will be upgraded to Manifest V3	✓		✓
Chrome Installer/Updater changes			✓
Bookmarks and reading list improvements on Android		✓	
Default Search Engine choice screen		✓	✓
Deprecate enterprise policy used for throttling			✓
Chrome Desktop support for Windows ARM64			✓
Remove enterprise policy used for GREASE			✓
Deprecate and remove Web SQL	✓		
Chrome bandwidth updates			✓
Form controls support direction value in vertical writing mode		✓	
Remove enterprise policies used for TLS handshake and RSA key usage			✓

Shadow root cloneable attribute	✓		
Local passwords stored in Play services on Android	✓		
X25519Kyber768 key encapsulation for TLS	✓		
Save to Drive and to Photos		✓	
Device bound session credentials google.com prototype	✓		
Windows ClearType Text Tuner integration		✓	
New and updated policies in Chrome browser			✓
Removed policies in Chrome browser			✓
ChromeOS updates	**Security/Privacy**	**User productivity/Apps**	**Management**
WebHID permission delegation	✓		
WiFi QoS on ChromeOS			✓
Scanning DLC	✓		
Increase the max size for the mouse pointer slider		✓	
Fast Pair for HID	✓		
Extension Cache Invalidation for managed guest login screen	✓		
Instant reboot in Managed Guest Session			✓
ChromeOS carrier lock	✓		
Admin console updates	**Security/Privacy**	**User productivity/Apps**	**Management**
Inactive browser deletion in Chrome Enterprise Core			✓
New filter on the App details page			✓

New policies in the Admin console			✓

Upcoming Chrome browser updates	**Security/Privacy**	**User productivity/Apps**	**Management**
UI Automation accessibility framework provider on Windows		✓	
Keyboard-focusable scroll containers	✓		
Network Service on Windows will be sandboxed	✓		
Interoperable mousemove default action			
Telemetry about pages that trigger keyboard and pointer lock APIs	✓		
Remove `window-placement` alias for permission and permission policy descriptors			✓
Extending Storage Access API (SAA) to non-cookie storage	✓		
Cross-site ancestor chain bit for CookiePartitionKey of partitioned cookies	✓		
Extract text from PDFs for screen reader users		✓	
Deprecate Safe Browsing Extended reporting	✓		
Remove enterprise policy used for Base URL inheritance			✓
App-Bound encryption for cookies	✓		
Intent to deprecate: Mutation Events		✓	
User link capturing on PWAs	✓		
All extensions must be updated to leverage Manifest V3 by June 2025	✓	✓	✓
Remove enterprise policy used for legacy same site behavior			✓

Chrome will no longer support MacOS 10.15			✓
Deprecate the includeShadowRoots argument on DOMParser			✓
Upcoming ChromeOS updates	**Security/Privacy**	**User productivity/Apps**	**Management**
ChromeOS Passpoint settings			✓
New policy to control Kiosk wake and sleep times			✓
Upcoming Admin console updates	**Security/Privacy**	**User productivity/Apps**	**Management**
Policy parity: Custom configurations for IT admins			✓
Legacy Technology report			✓

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. Please allow 1 to 2 weeks for translation for some languages.

Current Chrome version release notes

Chrome browser updates

Chrome Enterprise Premium product launch

Chrome Enterprise Premium is now available, providing a centralized solution for robust endpoint security, privacy, and control (setup guide). IT and security teams gain extensive network visibility and can easily deploy advanced protection features. Learn more.

Chrome Browser Cloud Management is now Chrome Enterprise Core

Chrome Enterprise's cloud management offers a centralized tool for configuring and managing browser policies, settings, apps, and extensions across Chrome – no matter the operating system, device, or location. Learn more.

- **Chrome 124 on Linux, MacOS, Windows: Trusted Tester access**
- Chrome 126 on Linux, MacOS, Windows: Feature rolls out

Watermarking (trusted tester)

This Chrome Enterprise Premium feature allows admins to overlay a watermark on top of a webpage if navigating to it triggers a specific Data Loss Prevention (DLP) rule. You can specify a static string to be displayed as the watermark.

This feature is currently released in our Trusted Tester program. If you're interested in helping us test this feature, you can sign up for the Chrome Enterprise Trusted Tester program here.

- **Chrome 124 on Linux, MacOS, Windows: Trusted Tester access**
- Chrome 126 on Linux, MacOS, Windows: Feature rolls out

Chrome Third-Party Cookie Deprecation (3PCD)

As previously announced, Chrome 120 started to restrict third-party cookies by default for 1% of Chrome users to facilitate testing, and subsequent releases will ramp up to 100% of users as early as Q3 2024. The ramp up to 100% of users is subject to addressing any remaining competition concerns of the UK's Competition and Markets Authority (CMA). Browsers that are part of the 1% experiment group also see new Tracking Protection user controls. You can try out these changes in Chrome 120 or higher by enabling `chrome://flags/#test-third-party-cookie-phaseout`.

This testing period allows sites to meaningfully preview what it's like to operate in a world without third-party cookies. As bounce-tracking protections are also a part of 3PCD, the users in this group with third-party cookies blocked have bounce tracking mitigations taking effect, so that their state is cleared for sites that get classified as bounce trackers. Most enterprise users are excluded from this 1% experiment group automatically; however, we recommend that admins proactively use the BlockThirdPartyCookies and CookiesAllowedForUrls policies to re-enable third-party cookies and opt out managed browsers ahead of the experiment. This gives enterprises time to make the changes required to avoid relying on this policy or on third-party cookies.

We are launching the Legacy Technology Report to help identify third-party cookies use cases. Admins can set the BlockThirdPartyCookies policy to F*alse* to re-enable third-party cookies for all sites but this prevents users from changing the corresponding setting in Chrome. Alternatively, to prevent breakage, you can set the CookiesAllowedForUrls policy to allowlist your enterprise applications to continue to receive third-party cookies.

For enterprise end users that are pulled into this experiment group and that are not covered by either enterprise admin policy, they can use the eye icon in the omnibox to temporarily re-enable third-party cookies for 90 days on a given site, when necessary. See this help article for more details on how to toggle these settings for the desired configuration.

Bounce tracking protections are also covered by the same policies as cookies and these protections are enforced when the bouncing site is not permitted to use 3P cookies. So setting the BlockThirdPartyCookies policy to false, or setting the CookiesAllowedForUrls policy for a site, prevents bounce tracking mitigations from deleting state for sites.

Enterprise SaaS integrations used in a cross-site context for non-advertising use cases can register for the third-party deprecation trial or the first-party deprecation trial for continued access to third-party cookies for a limited period of time.

The heuristics feature grants temporary third-party cookie access in limited scenarios based on user behavior. This mitigates site breakage caused by third-party cookie deprecation in established patterns, such as identity provider pop ups and redirects.

For more details on how to prepare, provide feedback and report potential site issues, refer to our updated landing page on preparing for the end of third-party cookies.

- **Starting in Chrome 120 on ChromeOS, Linux, MacOS, Windows**
  1% of global traffic has third-party cookies disabled. Enterprise users are excluded from this automatically where possible, and a policy is available to override the change.

Permissions prompt for Web MIDI API

The Web MIDI API connects to and interacts with Musical Instrument Digital Interface (MIDI) Devices. There have been several reported problems around Web MIDI API's drive-by access to client MIDI devices (see related Chromium bug). To address this problem, the W3C Audio Working Group decided to place an explicit permission on general Web MIDI API access. Originally, the explicit permission was only required for advanced Web MIDI usage in Chrome, including the ability to send and receive system exclusive (SysEx) messages, with gated access behind a permissions prompt. We now intend to expand the scope of the permission to regular Web MIDI API usage.

In Chrome 124, all access to the Web MIDI API requires a user permission. No policies are available to control these changes. If you encounter any issues, file a bug here.

○ **Chrome 124 on Windows, MacOS, Linux, Android**

Two Chrome extensions to be upgraded to Manifest V3

Two extensions will soon be updated to use Manifest V3: User-Agent Switcher, and Chrome Reporting.

This is a major update with a possibility for bugs, so you can try the Beta version of these extensions today. We encourage you to test them in your environment. If you encounter any issues, file a bug here.

- User-Agent Switcher for Chrome - Beta
- Chrome Reporting Extension - Beta

The User-Agent Switcher URL parser changed, so make sure your existing user agent substitutions work with the new version.

- **Chrome 124**: Both extensions receive an update, on their Stable version around April 30, 2024.

Chrome Installer/Updater changes

We are in the process of rolling out a new version of Google Update. As part of this change, the location for **GoogleUpdate.exe** on Windows changes and it is renamed **updater.exe**. Note that the previous path continues to persist until the transition is fully completed. **GoogleUpdate.exe** is also modified to point to **updater.exe**.

* Previous: `C:\Program Files (x86)\Google\Update\GoogleUpdate.exe`

* Current: `C:\Program Files (x86)\Google\GoogleUpdater\<VERSION>\updater.exe`

- **Chrome 124 on Windows**: These changes appear on Windows.

Bookmarks and reading list improvements on Android

On Chrome 124 on Android, some users who sign in to Chrome from the **Bookmark Manager** can use and save bookmarks and reading list items in their Google Account. Relevant enterprise policies, such as BrowserSignin, SyncTypesListDisabled, EditBookmarksEnabled, ManagedBookmarks and ShoppingListEnabled continue to work as before, to configure whether users can use and save items in their Google Account.

- **Chrome 124 on Android:** Feature rolls out.

Default Search Engine choice screen

As part of our Digital Markets Act (DMA) compliance, Google is introducing choice screens for users to choose their default search engine within Chrome. The choice from the prompt controls the default search engine setting, currently available at `chrome://settings/search`.

For enterprises that have chosen to have their administrator set their enterprise users' search settings using the enterprise policies DefaultSearchProviderEnabled and DefaultSearchProviderSearchUrl, those policies continue to control their enterprise's search settings. Where the administrator has not set their enterprise users' search settings by policy, enterprise users might see a prompt to choose their default search engine within Chrome.

Read more about these policies and the related atomic group.

- Chrome 120 on iOS, ChromeOS, LaCrOS, Linux, MacOS, Windows: 1% users might start getting the choice screen with Chrome 120.
- **Starting Chrome 124 on iOS, ChromeOS, LaCrOS, Linux, MacOS, Windows:** full roll-out for applicable users.

Deprecate enterprise policy used for throttling

The underlying code change (throttling same-process, cross-origin display:none iframes) that the ThrottleNonVisibleCrossOriginIframesAllowed enterprise policy overrides has been enabled in stable releases since early 2023. Since known issues have been dealt with, we intend to remove the ThrottleNonVisibleCrossOriginIframesAllowed enterprise policy in Chrome 124. To read the discussions around the throttling issue (and its resolution), see this Chromium issue report.

- **Chrome 124:** Policy is removed.

Chrome Desktop support for Windows ARM64

Chrome is rolling out support for Windows ARM64. We are working on publishing the Enterprise installers. You can continue to test the Canary channel and Beta channel and report bugs there. Note that this is subject to change based on overall stability, as well as feedback from customers. If you encounter any issues, file a bug here.

- **Chrome 124 on Windows (ARM):** New Enterprise installers will be available towards the end of April or early May.

Remove enterprise policy used for GREASE

We plan to deprecate the UserAgentClientHintsGREASEUpdateEnabled policy since the updated GREASE algorithm has been on by default for over a year. The policy will be removed in Chrome 126.

- **Chrome 124 on Android, ChromeOS, Linux, MacOS, Windows:** Policy is deprecated.
- Chrome 126 on Android, ChromeOS, Linux, MacOS, Windows: Policy is removed.

Deprecate and remove Web SQL

With SQLite over WASM as its official replacement, we plan to remove Web SQL entirely. This will help keep our users secure.

The Web SQL database standard was first proposed in April 2009 and abandoned in November 2010. Gecko never implemented this feature and WebKit deprecated this feature in 2019. The W3C encouraged those needing web databases to adopt Web Storage or Indexed Database.

Ever since its release, it has made it incredibly difficult to keep our users secure. SQLite was not initially designed to run malicious SQL statements, and yet with WebSQL we have to do exactly this. Having to react to a flow of stability and security issues is an unpredictable cost to the storage team.

    - Chrome 101: In Chrome 101 the WebSQLAccess policy is added. WebSQL will be available when this policy is enabled, while the policy is available until Chrome 123.
    - Chrome 115: Deprecation message added to console.
    - Chrome 117: In Chrome 117 the WebSQL Deprecation Trial starts. The trial ends in Chrome 123. During the trial period, a deprecation trial token is needed for the feature to be available.
    - Chrome 119: Starting Chrome 119, WebSQL is no longer available. Access to the feature is available until Chrome 123 using the WebSQLAccess policy, or a deprecation trial token.
    - **Chrome 124: on ChromeOS, LaCrOS, Linux, MacOS, Windows, Android:** Starting in Chrome 124, the policy WebSQLAccess and the deprecation trial, which allows for WebSQL to be available, will no longer be available.

Chrome bandwidth updates

Chrome is introducing a new mechanism for updating certain Chrome components that might result in extra bandwidth used within your fleet. You can control this with the **GenAILocalFoundationalModelSettings** policy.

- **Chrome 124 on Windows, MacOS, Linux**

Form controls support direction value in vertical writing mode

The CSS property `writing-mode` allows elements to go vertical, but users cannot set the direction in which the value changes. With this feature, we are allowing the form control elements (meter, progress and range input type) to have vertical writing mode and choose the form control's value direction. If direction is *rtl*, the value is rendered from bottom to top. If direction is *ltr*, the value is rendered from top to bottom. For more information, see this Chrome for Developers blog post.

- **Chrome 124 on Windows, MacOS, Linux, Android**

Remove enterprise policies used for TLS handshake and RSA key usage

In Chrome 114, we introduced InsecureHashesInTLSHandshakesEnabled to control the use of legacy insecure hashes during the TLS handshake process. In Chrome 116, we introduced RSAKeyUsageForLocalAnchorsEnabled to control some server certificate checks. In Chrome 124, both **InsecureHashesInTLSHandshakesEnabled** and **RSAKeyUsageForLocalAnchorsEnabled** policies are removed.

- **Chrome 124 on Android, ChromeOS, Linux, MacOS, Windows:** InsecureHashesInTLSHandshakesEnabled and RSAKeyUsageForLocalAnchorsEnabled policies will be removed.

Shadow root cloneable attribute

The shadow root clonable attribute enables individual control over whether a shadow root is cloneable (via standard platform cloning commands such as `` `cloneNode()` ``). Imperative shadow roots can now be controlled via a parameter to `` `attachShadow({clonable:true})` ``. Declarative shadow roots can be controlled via a new attribute, `` `<template shadowrootmode=open shadowrootclonable>` ``.

Breakage can occur if you are:
a) using declarative shadow DOM
b) cloning templates that contain DSD and
c) expecting those clones to contain cloned shadow roots

- **Chrome 124 on Android, ChromeOS, Linux, MacOS, Windows**

Local passwords stored in Play services on Android

Chrome changes the way local (not syncable) passwords are stored. Previously, they were stored in the Chrome profile. Now they are migrated to the local password storage of the Google Play services similarly to how the Google account passwords are already stored. It also changes the management UI for them to be provided by Google Play services. The

Chrome policy PasswordManagerEnabled is still valid but it doesn't control the behavior outside the Chrome binary. Thus, the new password management UI allows users to import or add passwords there manually.

- Chrome 123 on Android: The feature kicks-in for users without local passwords
- **Chrome 124 on Android:** All local passwords are migrated to the Google Play services.

X25519Kyber768 key encapsulation for TLS

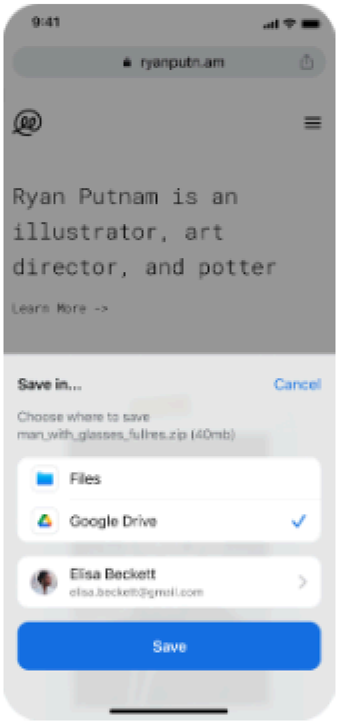
Starting in Chrome 124, Chrome enables by default on all desktop platforms a new post-quantum secure TLS key encapsulation mechanism X25519Kyber768, based on a NIST standard (ML-KEM). This is exposed as a new TLS cipher suite. TLS automatically negotiates supported ciphers, so this change should be transparent to server operators. However, some TLS middleboxes might be unprepared for the size of a Kyber (ML-KEM) key encapsulation, or a new TLS ClientHello cipher code point, leading to dropped or hanging connections. This can be resolved by updating your middlebox, or disabling the key encapsulation mechanism via the temporary PostQuantumKeyAgreementEnabled enterprise policy, which will be available through the end of 2024. However, long term, post-quantum secure ciphers will be required in TLS and the enterprise policy will be removed. This cipher will be used for both TLS 1.3 and QUIC connections.

- **Chrome 124 on Windows, MacOS, Linux**

Save to Drive and to Photos

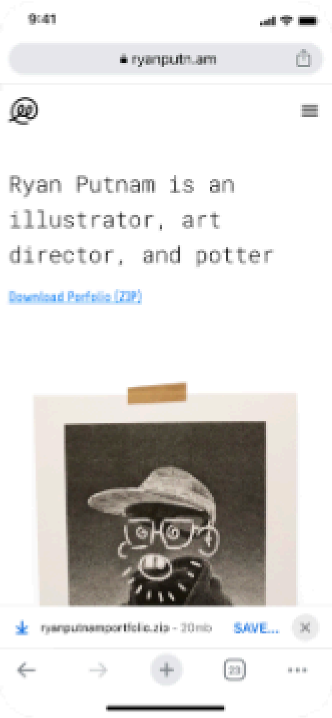
You can directly save a file or document image from the web to your Drive, as well an image to your Google Photos. You can now change the account to which the file is going to be saved. The relevant policies to control these features are ContextMenuPhotoSharingSettings and DownloadManagerSaveToDriveSettings.

- **Chrome 124 on iOS**

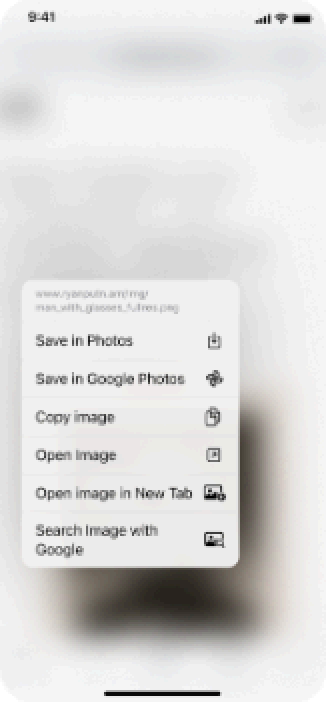


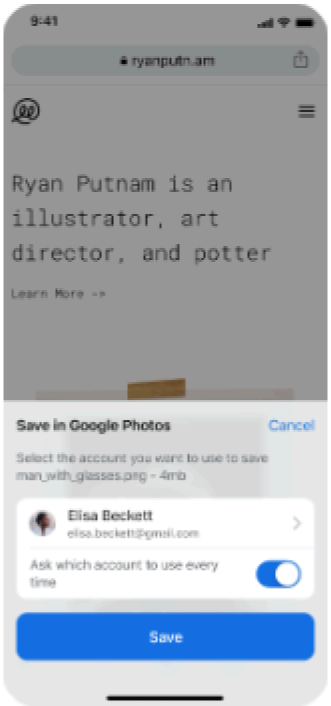
Ryan Putnam is an illustrator, art director, and potter

Choose where to save man_with_glasses_fullres.zip (40mb)



Ryan Putnam is an illustrator, art director, and potter





Ryan Putnam is an illustrator, art director, and potter

Select the account you want to use to save man_with_glasses.png - 4mb

Ask which account to use every time ●

Device Bound Session Credentials google.com prototype

The Device Bound Session Credentials project is intended to move the web away from long-lived bearer credentials like cookies, which can be stolen and reused, to credentials that 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 google.com website. In the future, we plan to standardize this approach for other websites and web browsers (Github).

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

- **Chrome 124 on Windows:** Planned 1% rollout on Chrome stable for google.com cookie binding for the general population. A temporary BoundSessionCredentialsEnabled policy is introduced in this milestone.

Windows ClearType Text Tuner integration

This feature tracks the work to support picking the contrast and gamma values from the Windows ClearType Text Tuner setting and applying them to Skia text rendering. This ensures that users' text rendering preferences are respected on Windows devices.

- **Chrome 124 on Windows, MacOS, Linux**

New and updated policies in Chrome browser

Policy	Description
MutationEventsEnabled	Re-enable deprecated/removed Mutation Events
ProductSpecificationsEnabled	Allow the product specifications feature to be enabled

BoundSessionCredentialsEnabled	Bind Google credentials to a device
AutomaticFullscreenAllowedForUrls	Allow automatic fullscreen on these sites
AutomaticFullscreenBlockedForUrls	Block automatic fullscreen on these sites
CloudProfileReportingEnabled	Enable Google Chrome cloud reporting for managed profile
PrefixedVideoFullscreenApiAvailability	Manage the deprecated prefixed video fullscreen API's availability

Removed policies in Chrome browser

Policy	Description
WebSQLAccess	Force WebSQL to be enabled
InsecureHashesInTLSHandshakesEnabled	Insecure Hashes in TLS Handshakes Enabled
RSAKeyUsageForLocalAnchorsEnabled	Check RSA key usage for server certificates issued by local trust anchors
GetDisplayMediaSetSelectAllScreensAllowedForUrls	Enables auto-select for multi screen captures
ThrottleNonVisibleCrossOriginIframesAllowed	Allows enabling throttling of non-visible, cross-origin iframes

ChromeOS updates

WebHID permission delegation

Chrome Apps now enables WebHID features in Chrome App Webview, for VDI and Zoom HID support.

WiFi QoS on ChromeOS

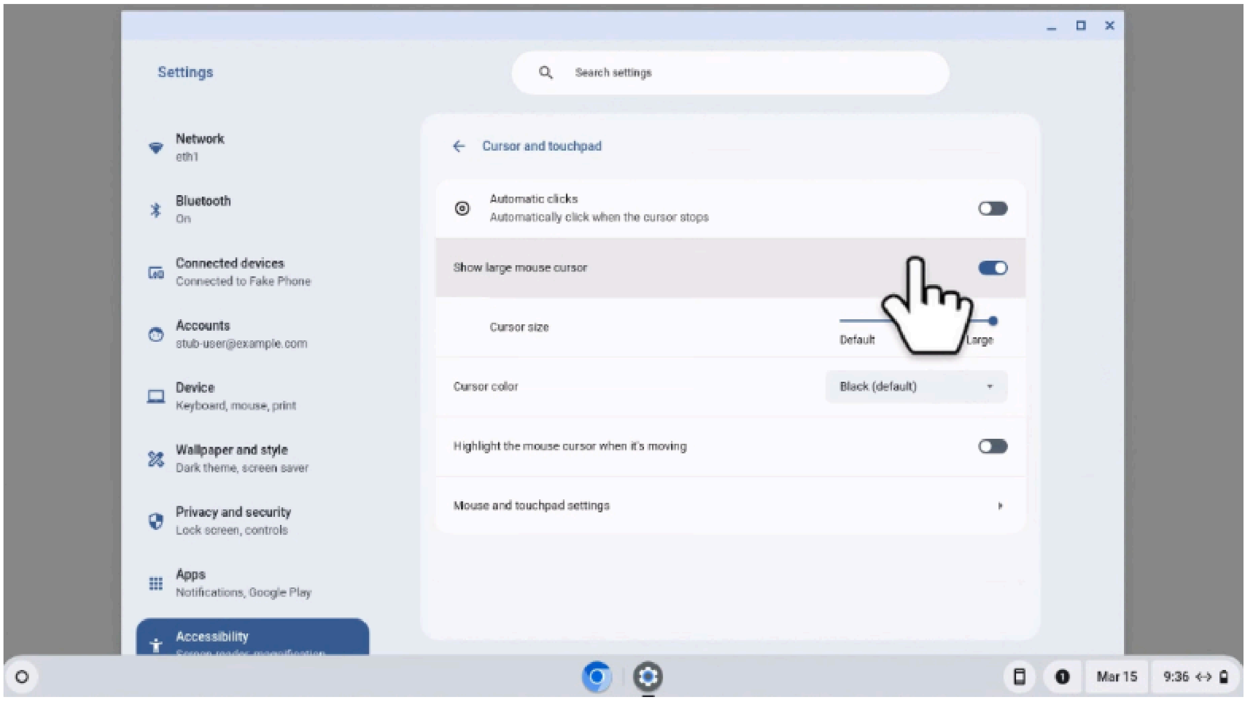
ChromeOS 124 now includes a new Quality of Service (QoS) feature that ensures better traffic prioritization of video conferencing and gaming applications on congested Wi-Fi networks. As a result, users can experience smoother video play with less buffering. In this initial release, this feature is not available for managed users.

Scanning DLC

To optimize the size of ChromeOS updates, we now download the required driver once the user signs in and connects a scanner that requires a driver. The driver downloads automatically without any prompt that the user needs to answer. A notification appears to indicate that external drivers are being installed and when installation is complete.

Increase the max size for the mouse pointer slider

We have expanded the mouse cursor sizes. You can adjust the cursor size by going into settings, accessibility, cursor and touchpad, and sliding the slider to your preferred size. This can be helpful for people who have low vision, for teachers who want students to follow along during a lesson while presenting, for people who are presenting on a video call, or if you just want to have a larger mouse cursor.



Settings

Search settings

Network
eth1

Bluetooth
On

Connected devices
Connected to Fake Phone

Accounts
stub-user@example.com

Device
Keyboard, mouse, print

Wallpaper and style
Dark theme, screen saver

Privacy and security
Lock screen, controls

Apps
Notifications, Google Play

Accessibility
Screen reader, magnification

Cursor and touchpad

Automatic clicks
Automatically click when the cursor stops

Show large mouse cursor

Cursor size — Default … Large

Cursor color — Black (default)

Highlight the mouse cursor when it's moving

Mouse and touchpad settings

Mar 15 9:36

Fast Pair for HID

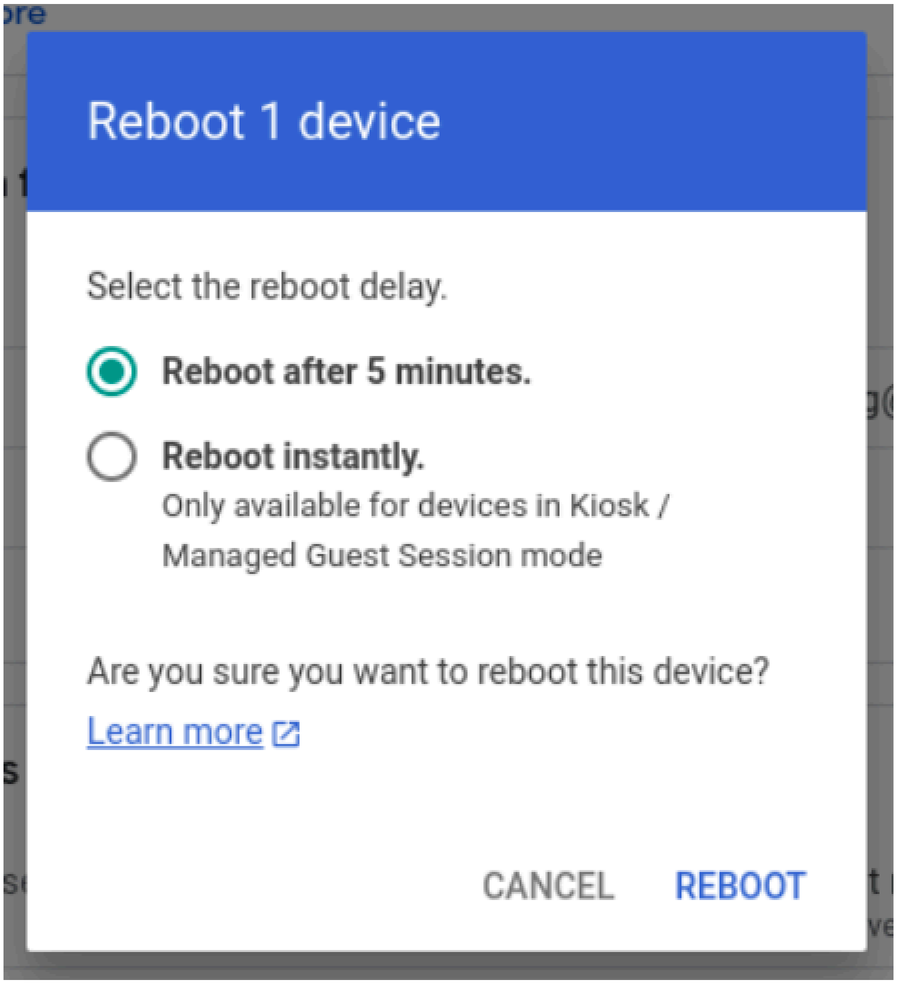
Fast Pair is now available for mice on ChromeOS. You can now bring a Fast Pair-compatible mouse close to your ChromeOS device, and be prompted to pair it with one click. For details, see our Help Center article.

Extension Cache Invalidation for managed guest login screen

From ChromeOS 124, the ExtensionInstallForcelist policy supports the rollback of extensions for managed guest sessions and the login screen. This gives admins the option to rollback extensions in case of an erroneous rollout of a new version.

Instant reboot in Managed Guest Session

ChromeOS 124 introduces a UI for admins to initiate an instant reboot action for Managed Guest Sessions.



Reboot 1 device

Select the reboot delay.

● Reboot after 5 minutes.

○ Reboot instantly.
Only available for devices in Kiosk / Managed Guest Session mode

Are you sure you want to reboot this device?
Learn more

ChromeOS carrier lock

ChromeOS now supports carrier lock for mobile providers that want to provide subsidized devices to users. On all cellular enabled devices, carriers can lock the device to only allow connection to approved SIM profiles (both eSIM and physical SIM). Locked devices get enrolled to a carrier lock server and when the contract ends, the carrier simply releases the lock and the user is notified on their device. Note that in addition to being blocked for using unauthorized SIM profiles, dev mode is blocked on carrier locked devices.

Admin console updates

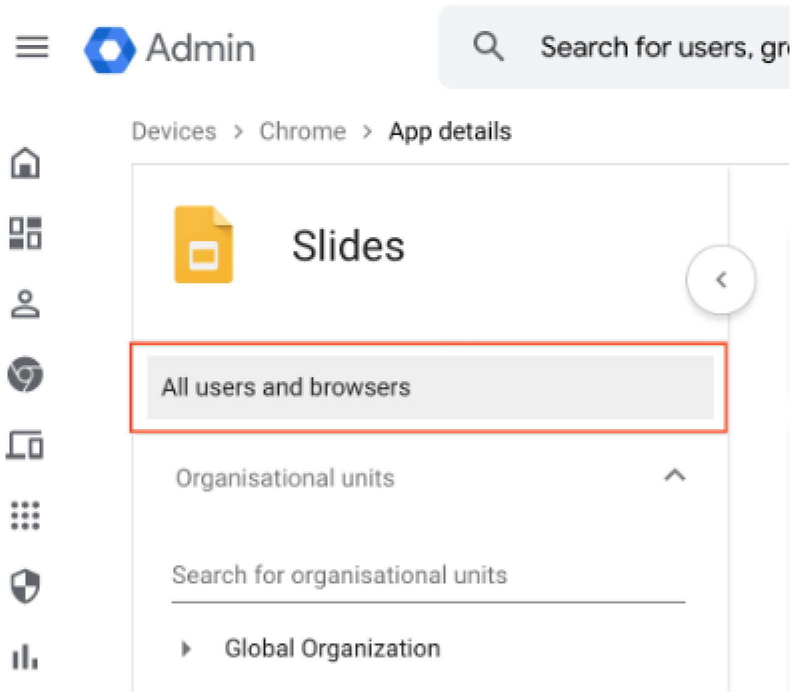
Inactive browser deletion in Chrome Enterprise Core

Starting in April 2024 until May 2024, the **Inactive period for browser deletion policy** will start rolling out and automatically delete enrolled browsers in the Admin console that have been inactive for more than the inactivity period of time determined by the policy. When releasing the policy, the inactivity period of time will have a default value of 540 days. Meaning that by default, all enrolled browsers that have been inactive for more than 540 days will be deleted from your account. Administrators can change the inactive period value using this policy. The maximum value to determine the browser inactivity period will be 730 days and the minimum value is 28 days (learn more).

If you lower the set policy value, it might have a global impact on any currently enrolled browsers. All impacted browsers will be considered inactive and, therefore, be **irreversibly deleted**. To ensure the deleted browsers re-enroll automatically next time they restart, set the Device Token Management policy value to **Delete token** before lowering the value of this policy. The enrollment tokens on these browsers need to still be valid at the time of the restart.

New filter on the App details page

Introducing a new filter for “All users and browsers” on the App Details page. This filter allows IT admins to easily view all the managed browsers and managed users where a specific extension or app is installed.



Admin
Search for users, gr
Devices › Chrome › App details
Slides
All users and browsers
Organisational units
Search for organisational units
Global Organization

New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
AutomaticFullscreenAllowedForUrls	Users & browsers MGS	Android Chrome ChromeOS	User experience
AutomaticFullscreenBlockedForUrls	Users & browsers MGS	Android Chrome ChromeOS	User experience
MutationEventsEnabled	Users & browsers MGS	Android Chrome ChromeOS Android Webview	Legacy site compatibility
PrefixedVideoFullscreenApiAvailability	Users & browsers MGS	Android Chrome ChromeOS Fuschia	Legacy site compatibility

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 changes

UI Automation accessibility framework provider on Windows

Starting in Chrome 126, Chrome will start directly supporting accessibility client software that uses Microsoft Windows's UI Automation accessibility framework. Prior to this change, such software interoperated with Chrome by way of a compatibility shim in Microsoft Windows. This change is being made to improve the accessible user experience for many users. It provides complete support for Narrator, Magnifier, and Voice Access; and will improve third-party apps that use Windows's UI Automation accessibility framework. Users of Chrome will find reduced memory usage and processing overhead when used with accessibility tools. It will also ease development of software using assistive technologies.

Administrators may use the **UiAutomationProviderEnabled** enterprise policy starting in Chrome 125 to either force-enable the new provider (so that all users receive the new functionality), or disable the new provider. This policy will be supported through Chrome 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 Window:** The **UiAutomationProviderEnabled** policy is introduced so that administrators can enable Chrome's UI Automation accessibility framework provider and validate that third-party accessibility tools continue to work.
- Chrome 126 on Windows: The Chrome variations framework will be used to begin enabling Chrome's UI Automation accessibility framework provider for users. It will be progressively enabled to the full stable population, with pauses as needed to

address compatibility issues that can be resolved in Chrome. Enterprise administrators may continue to use the **UiAutomationProviderEnabled** policy to either opt-in early to the new behavior, or to temporarily opt-out through Chrome 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.

Keyboard-focusable scroll containers

Making scroll containers focusable using sequential focus navigation greatly improves accessibility. 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>`.

- **Chrome 125 on Windows, MacOS, Linux, Android**

Network Service on Windows will be sandboxed

To improve security and reliability, the network service, already running in its own process, will be 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 and report any issues you encounter.

- ○ **Chrome 125 on Windows:** Network Service sandboxed on Windows.

Interoperable mousemove default action

Chrome allowed canceling mousemove events to prevent other APIs like text selection (and even drag-and-drop in the past). This does not match other major browsers; nor does it conform to the UI (event spec).

Through this feature, text selection will no longer be the default-action of mousemove. Text selection and drag-and-drop can still be prevented through canceling selectstart and dragstart events respectively, which are spec compliant and fully interoperable.

- **Chrome 125 on Windows, MacOS, Linux, Android**

Telemetry about pages that trigger keyboard and pointer Lock APIs

When an Enhances Safe Browsing user visits a page that triggers keyboard or pointer lock APIs, attributes of that page will be sent to Safe Browsing.

If the telemetry is sent and the page seems to be malicious, users will see a Safe Browsing warning and their keyboard or pointer will be unlocked if they were locked.

- **Chrome 125 on Android, ChromeOS, LaCrOS, Linux, MacOS, Windows, Fuchsia**

Remove window-placement alias for permission and permission policy descriptors

Chrome 124 removes the `window-placement` alias for permission and permission policy descriptors. All instances of `window-placement` are replaced with `window-management`, which better describes the related API functionality. This is a follow-up to Multi-Screen Window Placement API feature enhancements; for more details, see Chrome Platform Status.

- **Chrome 125 on Windows, MacOS, Linux**

Extending Storage Access API (SAA) to non-cookie storage

We propose an extension of the Storage Access API (backwards compatible) to allow access to unpartitioned (cookie and non-cookie) storage in a third-party context, and imagine the API mechanics to be roughly like this (JS running in an embedded iframe):

```
// Request a new storage handle via rSA (this should prompt the user)
let handle = await document.requestStorageAccess({all: true});
// Write some cross-site localstorage
handle.localStorage.setItem("userid", "1234");
// Open or create an indexedDB that is shared with the 1P context
let messageDB = handle.defaultBucket.indexedDB.open("messages");
```

The same flow would be used by iframes to get a storage handle when their top-level ancestor successfully called `rSAFor`, just that in this case the `storage-access` permission was already granted and thus the `rSA` call would not require a user gesture or show a prompt, allowing for hidden iframes accessing storage.

- **Chrome 125 on Windows, MacOS, Linux, Android**
-

Remove enterprise policy used for Base URL inheritance

In Chrome 114 we introduced NewBaseUrlInheritanceBehaviorAllowed to prevent users or Google Chrome variations from enabling NewBaseUrlInheritanceBehavior, in case compatibility issues were discovered. In Chrome 125 the temporary NewBaseUrlInheritanceBehaviorAllowed policy will be removed.

- **Chrome 125 on Android, ChromeOS, Linux, MacOS, Windows:** NewBaseUrlInheritanceBehaviorAllowed policy will be removed.

App-Bound encryption for cookies

To improve the security of cookies on Windows, the encryption key used for cookie encryption will be further secured by binding it to Chrome's application identity. This can help protect against malware that might attempt to steal cookies from the system. This does not protect against an attacker who is able to elevate privilege or inject into Chrome's processes.

An enterprise policy **ApplicationBoundEncryptionEnabled** will be available to disable Application Bound encryption.

- **Chrome 125 on Windows**

Cross-site ancestor chain bit for CookiePartitionKey of partitioned cookies

Chrome 125 adds a cross-site ancestor bit to the keying of the partitioned cookie's `CookiePartitionKey`. This change unifies the partition key with the partition key values used in storage partitioning and adds protection against clickjacking attacks by preventing cross-site embedded frames from having access to the top-level-site's partitioned cookies.

If an enterprise experiences any breakage with embedded iframes, they can use the CookiesAllowedForUrls policy or use `SameSite=None` cookies *without* the Partitioned attribute and then invoke the Storage Access API (SAA) or use the Cross-Origin Resource Sharing (CORS) to ensure that embedded iframes have access to the same cookies as the top level domain.

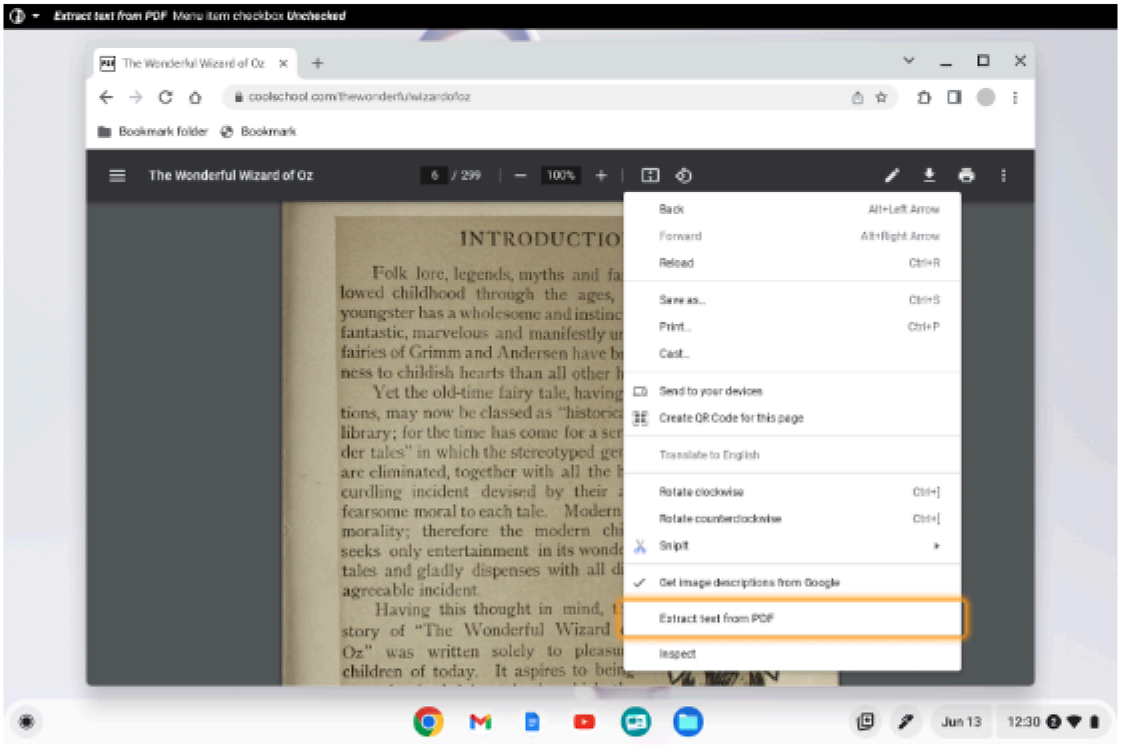
- **Chrome 126 on Windows, MacOS, Linux**

Extract text from PDFs for screen reader users

Chrome browser is launching an Optical character recognition (OCR) AI reader for PDFs, creating the first browser built-in PDF screen reader for inaccessible documents, further filling the gap in accessibility for low vision and blind users across the web.

This feature leverages Google's OCR models to extract, compartmentalize, and section PDF documents to make them more accessible. A local machine intelligence library will be added that uses Screen AI technology to analyze screenshots or the accessibility tree, and extract more information to help assistive technology, such as texts (OCR) and main content of the page.

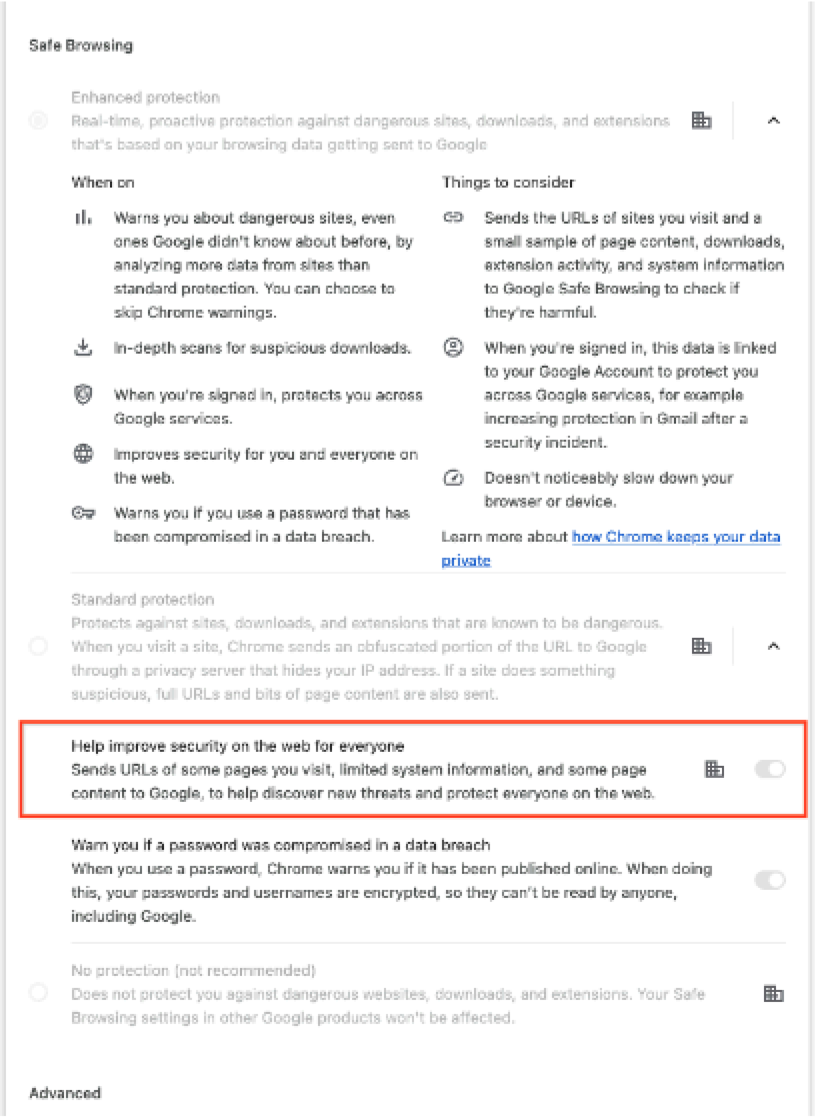
- **Chrome 126 on ChromeOS, Linux, MacOS, Windows**



Deprecate Safe Browsing Extended reporting

Safe Browsing Extended reporting is a feature that enhances the security of all users by collecting telemetry information from participating users that is used for Google Safe Browsing protections. The data collected includes URLs of visited web pages, limited system information, and some page content. However, this feature is now superseded by Enhanced protection mode. We suggest users switch to Enhanced protection to continue providing security for all users in addition to enabling the strongest security available in Chrome. For more information, see [Safe Browsing protection levels](#).

- **Chrome 126 on iOS, ChromeOS, Linux, MacOS, Windows:** Deprecation of Safe Browsing Extended Reporting



Safe Browsing

○ Enhanced protection
Real-time, proactive protection against dangerous sites, downloads, and extensions that's based on your browsing data getting sent to Google

When on

- Warns you about dangerous sites, even ones Google didn't know about before, by analyzing more data from sites than standard protection. You can choose to skip Chrome warnings.
- In-depth scans for suspicious downloads.
- When you're signed in, protects you across Google services.
- Improves security for you and everyone on the web.
- Warns you if you use a password that has been compromised in a data breach.

Things to consider

- Sends the URLs of sites you visit and a small sample of page content, downloads, extension activity, and system information to Google Safe Browsing to check if they're harmful.
- When you're signed in, this data is linked to your Google Account to protect you across Google services, for example increasing protection in Gmail after a security incident.
- Doesn't noticeably slow down your browser or device.

Learn more about how Chrome keeps your data private

○ Standard protection
Protects against sites, downloads, and extensions that are known to be dangerous. When you visit a site, Chrome sends an obfuscated portion of the URL to Google through a privacy server that hides your IP address. If a site does something suspicious, full URLs and bits of page content are also sent.

Help improve security on the web for everyone
Sends URLs of some pages you visit, limited system information, and some page content to Google, to help discover new threats and protect everyone on the web.

Warn you if a password was compromised in a data breach
When you use a password, Chrome warns you if it has been published online. When doing this, your passwords and usernames are encrypted, so they can't be read by anyone, including Google.

○ No protection (not recommended)
Does not protect you against dangerous websites, downloads, and extensions. Your Safe Browsing settings in other Google products won't be affected.

Advanced

Intent to 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.

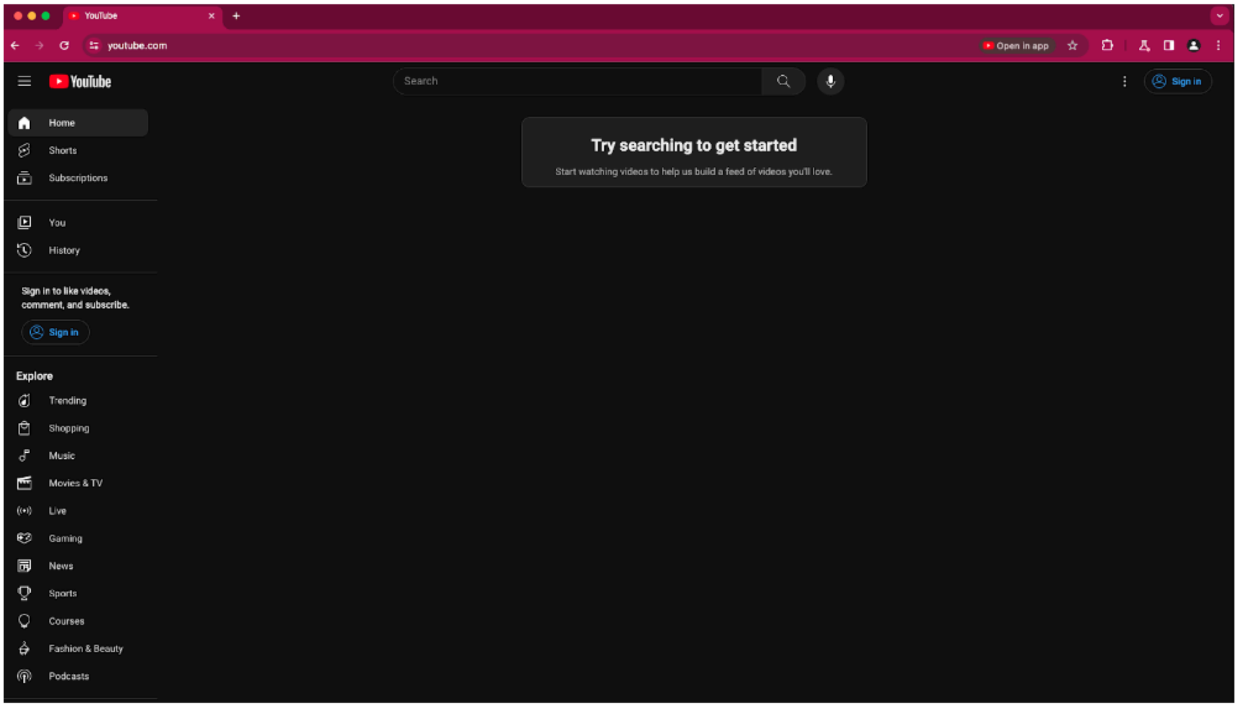
- **Chrome 127 on Android, ChromeOS, Linux, MacOS, Windows:** Mutation events will stop functioning in Chrome 127, around July 30, 2024.

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.

- Chrome 121 on Linux, MacOS, Windows: 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`.

- **Earliest in Chrome 127 on Linux, MacOS, Windows:** We will 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).



Try searching to get started

Start watching videos to help us build a feed of videos you'll love.

Sign in to like videos, comment, and subscribe.

All extensions must be updated to leverage Manifest V3 by June 2025

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

Beginning June 2024, Chrome will gradually disable Manifest V2 extensions running in the browser. An Enterprise policy - ExtensionManifestV2Availability - is available to control whether Manifest v2 extensions are allowed. The policy can be used to test Manifest V3 in your organization ahead of the migration. Additionally, machines on which the policy is enabled will not be subject to the disabling of Manifest V2 extensions until the following year - June 2025 - at which point the policy will be removed.

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

- Chrome 110 on ChromeOS, LaCrOS, Linux, MacOS, Windows: Enterprise policy ExtensionManifestV2Availability is available to control whether Manifest v2 extensions are allowed. The policy can be used to test Manifest V3 in your organization ahead of the migration. After the migration the policy will allow you to extend the usage of Manifest V2 extensions.
- **Chrome 127 on ChromeOS, LaCrOS, Linux, MacOS, Windows:** Chrome will gradually disable Manifest V2 extensions on user devices. Only those with the ExtensionManifestV2Availability enterprise policy enabled would be able to continue using Manifest V2 extensions in their organization.
- Chrome 139 on ChromeOS, LaCrOS, Linux, MacOS, Windows: Remove ExtensionManifestV2Availability 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 on the milestone listed below.

- **Chrome 128 on Android, ChromeOS, Linux, MacOS, Windows:** Remove LegacySameSiteCookieBehaviorEnabledForDomainList policy

Chrome will no longer support MacOS 10.15

Chrome will no longer support MacOS 10.15, which is already outside of its support window with Apple. Users have to update their operating systems to continue to use Chrome browser. Running on a supported operating system is essential to maintaining security. If run on MacOS 10.15, Chrome continues to show an infobar that reminds users that Chrome 129 will no longer support MacOS 10.15.

- **Chrome 129 on MacOS:** Chrome no longer supports MacOS 10.15

Deprecate the includeShadowRoots argument on DOMParser

The includeShadowRoots argument was a never-standardized argument to the `DOMParser.parseFromString()` function, which was there to allow imperative parsing of HTML content that contains declarative shadow DOM. This was shipped in Chrome 90 as part of the initial shipment of declarative shadow DOM. Since the standards discussion rematerialized in 2023, the shape of DSD APIs changed, including this feature for imperative parsing. To read more, see details of the context on the related standards, and information is also available on the related deprecations of shadow DOM serialization and shadow root attribute.

Now that a standardized version of this API, in the form of setHTMLUnsafe() and parseHTMLUnsafe() will ship in Chrome 124, the non-standard includeShadowRoots argument needs to be deprecated and removed. All usage should shift accordingly:

Instead of:

```
  (new
DOMParser()).parseFromString(html,'text/html',{includeShadowRoots:
true});
```

This can be used instead:

```
  document.parseHTMLUnsafe(html);
```

- **Chrome 129 on Windows, Mac, Linux, Android**

Upcoming ChromeOS changes

ChromeOS Passpoint settings

As early as ChromeOS 125, you will be able to view and manage Wi-Fi Passpoint in ChromeOS **Settings**. You will be able to view and remove your installed passpoint subscription under the passpoint detailed page.

New policy to control Kiosk wake and sleep times

As early as ChromeOS 125, we will introduce a new kiosk device policy that will allow Admins to schedule when a device will wake and sleep. For more details, see Kiosk settings.

Upcoming Admin console changes

Policy parity: Custom configurations for IT admins

The **Custom Configurations** page allows IT admins to configure Chrome policies that are not yet in the Admin console, using JSON scripts. As a result, all Chrome policies are now configurable in Chrome Enterprise Core ~~browser Cloud Management in the Admin console~~, either using the **Settings** page or the **Custom Configurations** page. You can also use the page to configure extension installation mode not supported in the Admin console, such as “normal_installed”.

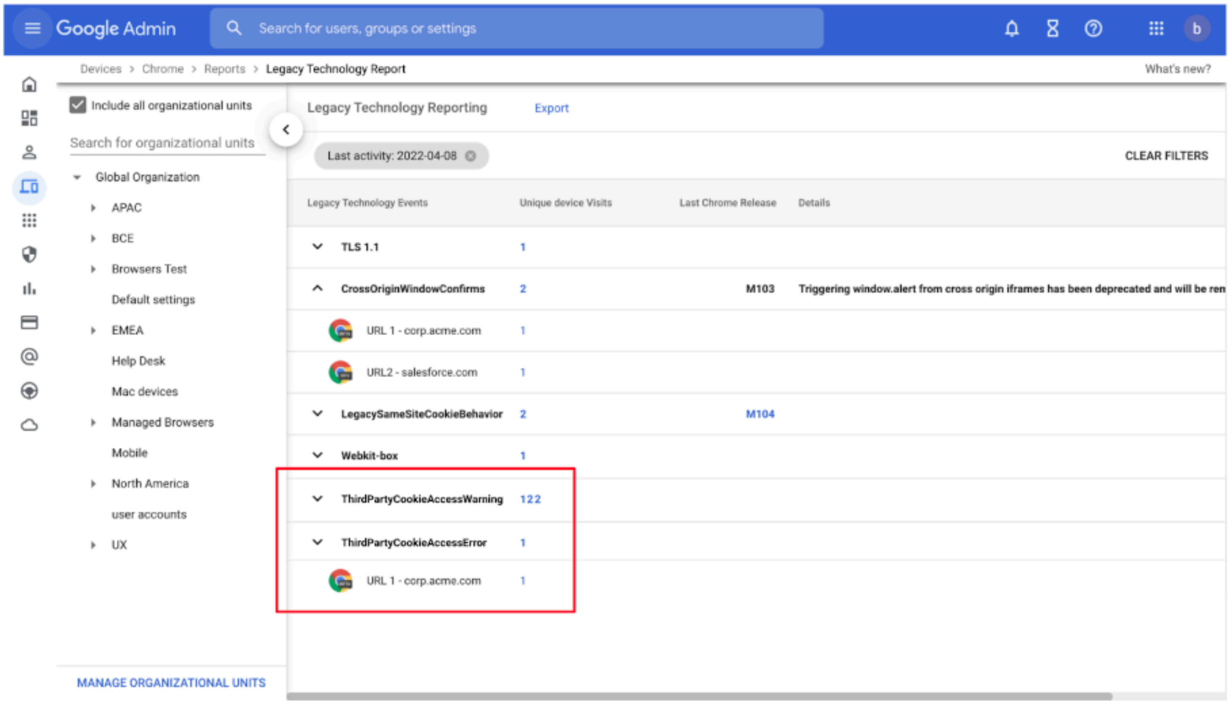
- **As early as Chrome 125 on Android, iOS, Linux, MacOS, Windows:** Trusted Tester access
- As early as Chrome 126 on Android, iOS, Linux, MacOS, Windows: Feature rolls out

Legacy Technology report

As early as Chrome 127, the Legacy Technology report will be available in the Admin console and it will proactively report websites (both internal and external) that are using technology that will be deprecated, for example, third-party cookies, SameSite cookie changes, and older security protocols like TLS 1.0/1.1 and third-party cookies. This information will enable IT administrators to work with developers to plan required tech migrations before the deprecation feature removals goes into effect.

This feature is currently released in our Trusted Tester program. If you’re interested in helping us test this feature, you can sign up for the Chrome Enterprise Trusted Tester program here.

- **As early as Chrome 127 on Linux, MacOS, Windows:** Legacy Technology report will be available in the Admin console.


Google Admin
Search for users, groups or settings
Devices > Chrome > Reports > Legacy Technology Report
What's new?
☑ Include all organizational units
Search for organizational units
Global Organization
APAC
BCE
Browsers Test
Default settings
EMEA
Help Desk
Mac devices
Managed Browsers
Mobile
North America
user accounts
UX
MANAGE ORGANIZATIONAL UNITS
Legacy Technology Reporting
Export
Last activity: 2022-04-08
CLEAR FILTERS

Legacy Technology Events	Unique device Visits	Last Chrome Release	Details
TLS 1.1	1		
CrossOriginWindowConfirms	2	M103	Triggering window.alert from cross origin iframes has been deprecated and will be ren
URL 1 - corp.acme.com	1		
URL2 - salesforce.com	1		
LegacySameSiteCookieBehavior	2	M104	
Webkit-box	1		
ThirdPartyCookieAccessWarning	122		
ThirdPartyCookieAccessError	1		
URL 1 - corp.acme.com	1		

Previous release notes

Chrome version & targeted Stable channel release date	PDF
Chrome 123: March 13, 2023	PDF
Chrome 122: February 14, 2023	PDF
Chrome 121: January 17, 2023	PDF
Chrome 120: November 29, 2023	PDF
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