Chrome 123 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 March 29, 2024.

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

Chrome 123 release summary

Chrome Browser updates	Security/Privacy	User productivity/Apps	Management
Chrome Third-Party Cookie Deprecation (3PCD)	✓		
Generative AI features		✓	
Resume tabs		✓	
Chrome on Android and iOS: cross-device resumption		✓	
Resume the last opened tab on any device		✓	
Change in behavior of the JavaScript JIT policies			✓
Chrome Sync ends support for Chrome 81 and earlier	✓		✓
New idle timeout policies on iOS			✓
Cross-profile password reuse detection	✓		
Telemetry for permission prompts and accepting notification permissions	✓		
ServiceWorker static routing API	✓		
Private network access checks for navigation requests: warning-only mode	✓		
Local passwords stored in Play services		✓	
Zstd content encoding	✓		
Force Sign-in flows revamp		✓	
Google Update changes			✓
New and updated policies in Chrome browser			✓

ChromeOS updates	**Security/Privacy**	**User productivity/Apps**	**Management**
ChromeOS Flex Bluetooth migration			✓
Customizing keyboard shortcuts		✓	
Mouse button customization		✓	
Faster Split Screen setup		✓	
ChromeOS Tether Hotspot		✓	
Per-app language preferences on Android		✓	
New natural-sounding voices for text-to-speech		✓	
Data Processor mode rollout for Norway	✓		
Per-app privacy settings	✓		
Enhanced Android security for new enterprise customers			✓
Admin Console Updates	**Security/Privacy**	**User productivity/Apps**	**Management**
Enhanced Settings page experience		✓	
Remote log collection for ChromeOS devices			✓
Inactive browser deletion in Chrome Browser Cloud Management			✓
Chrome crash report			✓
New policies in the Admin console			✓
Upcoming Chrome Browser updates	**Security/Privacy**	**User productivity/Apps**	**Management**
Default Search Engine choice screen		✓	

User link capturing on PWAs - Windows, MacOS and Linux	✓		
Permissions prompt for Web MIDI API	✓		
Three Chrome extensions will be upgraded to Manifest V3	✓		✓
Bookmarks and reading list improvements on Android		✓	
Deprecate enterprise policy used for throttling			✓
Chrome Desktop support for Windows ARM64			✓
Remove enterprise policy used for GREASE			✓
Network Service on Windows will be sandboxed	✓		
Deprecate and remove WebSQL	✓		
Form controls support direction value in vertical writing mode		✓	
Remove enterprise policies used for TLS handshake and RSA key usage			✓
Remove enterprise policy used for Base URL inheritance			✓
Intent to deprecate: Mutation Events		✓	
Remove enterprise policy used for legacy same site behavior			✓
All extensions must be updated to leverage Manifest V3 by June 2025	✓	✓	✓
Chrome will no longer support macOS 10.15			✓
Upcoming ChromeOS updates	**Security/Privacy**	**User productivity/Apps**	**Management**
Record GIFs with Screen capture		✓	

Upcoming Admin Console Updates	Security/Privacy	User productivity/Apps	Management
Legacy Technology report			✓
Policy parity: Custom Configurations for IT admins			✓

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 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 false to re-enable third-party cookies for all sites but this will prevent 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 receiving 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.

Generative AI features

In Chrome 122, 3 Generative AI (GenAI) features became available for managed users that have signed into Chrome browser: Tab Organizer, Create themes, and Help me write (not available on ChromeOS). Initially, these 3 features are only available to users (18+) in English in the USA. Admins can control these by using the TabOrganizerSettings, CreateThemesSettings and HelpMeWriteSettings policies.

Starting in Chrome 123, we will gradually roll out these features and some users will no longer need to opt in to Experimental AI to use the features if admins set the policies to enabled.

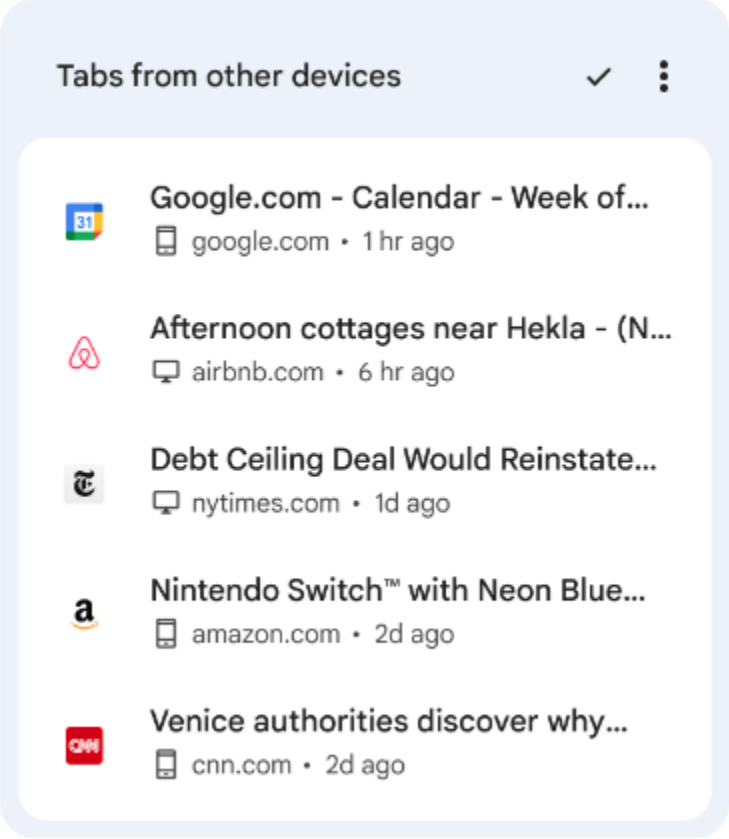
- Chrome 122 on ChromeOS, Linux, Mac, Windows: GenAI features (Tab Organizer, Create themes, and Help me write) become available to managed users in the USA. Users need to turn on Experimental AI.

- **Chrome 123 on ChromeOS, Linux, Mac, Windows:** Features (Tab group suggestions, Create themes, and Help me write) become available to managed users in the USA. Some users will have the feature enabled by default; others will still be able to manually opt-in via the Experimental AI settings page. In both cases, the features will not be available if disabled via policy.

Resume tabs

Chrome 123 introduces a new card on the **New tab** page, which helps users continue with tab suggestions from other devices. Using the NTPCardsVisible policy, admins can control this feature, and other cards on the **New tab** page.

- **Chrome 123 on ChromeOS, Linux, Mac, Windows**



Chrome on Android and iOS: cross-device resumption

To help users resume tasks originating from other devices, Chrome now provides cross-device tab suggestions on the **New tab** page or Home surfaces on Chrome on Android and Chrome on iOS.

- **Chrome 123 on Android, iOS:** Feature launches

Resume the last opened tab on any device

For the last open tab on any device within the last 24 hours with the same signed-in user profile, Chrome now offers users a quick shortcut to resume that tab. Admins can control this feature using an existing enterprise policy called SyncTypesListDisabled.

- **Chrome 123 on iOS:** Feature launches

Change in behavior of the JavaScript JIT policies

As early as Chrome 122, enabling the DefaultJavaScriptJitSetting policy and disabling JavaScript JIT no longer resulted in WebAssembly being fully disabled. The V8 optimizing JIT will continue to be disabled by setting this policy. This allows Chrome to render web content in a more secure configuration.

Chrome Sync ends support for Chrome 81 and earlier

Chrome Sync will no longer support Chrome 81 and earlier. You need to upgrade to a more recent version of Chrome if you want to continue using Chrome Sync.

- **Chrome 123 on Android, iOS, ChromeOS, Linux, MacOS, Windows:** The change will be implemented.

New idle timeout policies on iOS

Enterprises are now able to enforce taking an action after Chrome has been idle for some amount of time on iOS devices. Admins can use the IdleTimeout policy to set a timeout

period and the IdleTimeoutActions policy to specify actions on timeout. The setting will be available as a platform policy and will be available per user profile at a future date.

- **Chrome 123 on iOS:** Policies available on iOS.

Cross-profile password reuse detection

Previously, password reuse detection of corporate credentials was only detectable in the corporate profile. In Chrome 123, password reuse detection will detect corporate credential reuse across all non-Incognito profiles on the managed browser.

- **Chrome 123:** Feature rolls out to enterprises that have MetricsReportingEnabled set to enabled.

Telemetry for permission prompts and accepting notification permissions

When Enhanced Protection is turned on, and a user visits a page that prompts the user to accept a notification permission, attributes of that page might be sent to Safe Browsing. If the telemetry is sent and the page is deemed dangerous, users will see a Safe Browsing warning.

When Enhanced Protection or Safe Browsing Extended Reporting is turned on, and a user accepts a notification permission for a blocklisted page, this event will be sent to Safe Browsing.

These features can be controlled by the SafeBrowsingProtectionLevel and SafeBrowsingExtendedReportingEnabled policies.

- **Chrome 123 Android, ChromeOS, LaCrOS, Linux, Mac, Windows, Fuchsia:** Feature rolls out to enterprises that have MetricsReportingEnabled set to enabled

ServiceWorker static routing API

This API allows developers to configure the routing, and allows them to offload simple things ServiceWorkers do. If the condition matches, the navigation happens without starting

ServiceWorkers or executing JavaScript, which allows web pages to avoid performance penalties due to ServiceWorker interceptions.

- **Chrome 123 on Windows, Mac, Linux, Android**

Private network access checks for navigation requests: warning-only mode

Before a website navigates to a destination site in a user's private network, Chrome will do the following:

1. Checks whether the original navigation request has been initiated from a secure context.
2. Sends a preflight request, and checks whether the destination site responds with a header that allows private network access.

The above checks are made to protect the user's private network. Since this feature operates in *warning-only* mode, we do not fail the requests if any of the checks fail. Instead, a warning will be shown in DevTools Chrome console, to help developers prepare for the coming enforcement. To read about these changes, see Private Network Access (PNA) for Navigation Requests. To learn more, see the PNA specification.

- **Chrome 123 on Android (except for WebView), ChromeOS, Linux, MacOS, Windows:** Warning-only mode.
- Earliest Chrome 130 on Android (except for WebView), ChromeOS, Linux, MacOS, Windows: Requests will fail.

Local passwords stored in Play services

Chrome changes the way local (not syncable) passwords are stored. Previously they were stored in the Chrome profile. Now they are gonna be 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.

Zstd content encoding

Chrome is adding support for Zstandard (zstd) as a data compression mechanism. Supporting zstd content encoding in the browser allows sites to spend less time and CPU or power on compression on their servers, resulting in reduced server costs. A temporary enterprise policy ZstdContentEncodingEnabled is available to turn off the zstd content encoding feature.

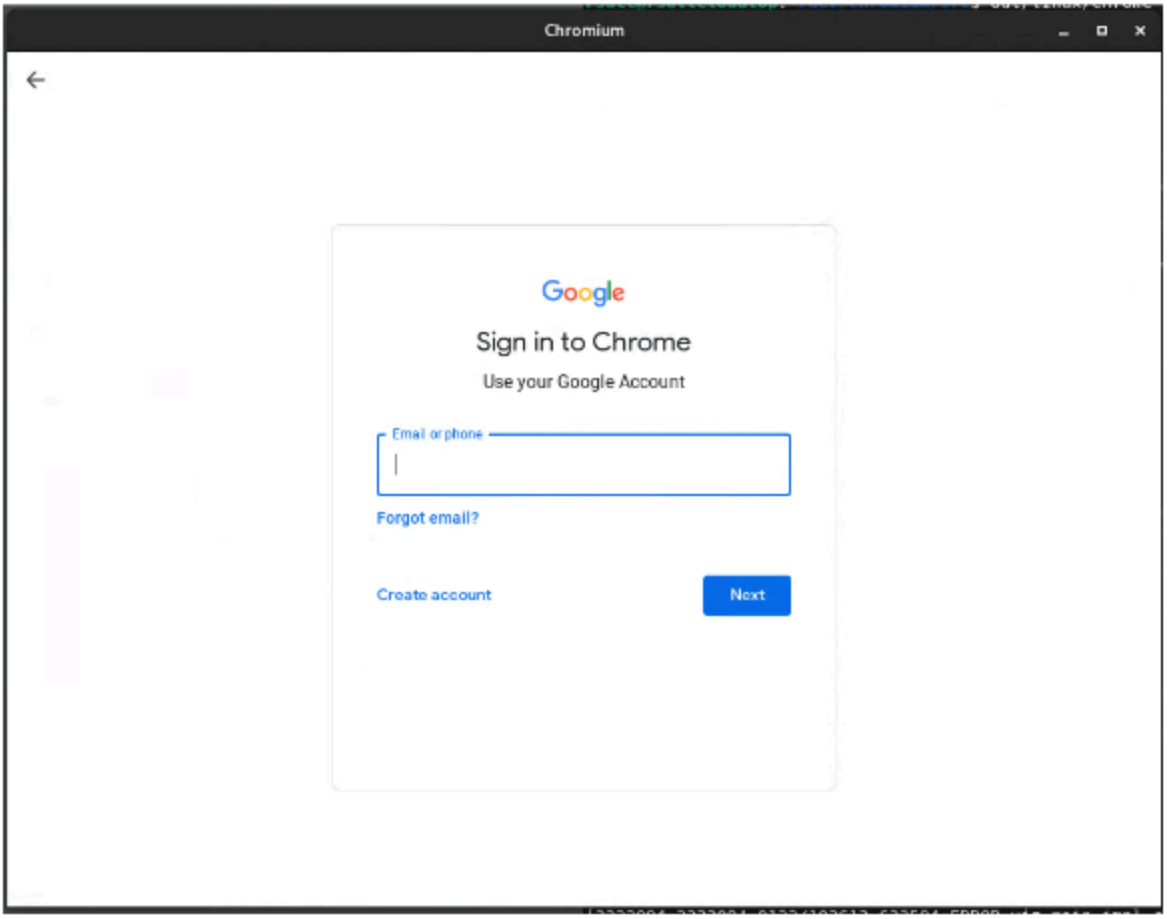
- **Chrome 123 on Android, ChromeOS, LaCrOS, Linux, Mac, Windows, Fuchsia:** Support for zstd is added.

Force sign-in flows revamp

When the BrowserSignin policy is set to **Force users to sign-in to use the browser**, users now sign in to Chrome browser by following the standard sign-in procedure through the Profile Picker.

Previously, the **Force sign-in** flow had a specific UI dialog that did not follow typical Chrome style or standards. Now the flows are aligned with the regular sign-in flows. We've also improved error handling by displaying sign-in errors in a regular dialog with actionable buttons.

- C**hrome 123 on Mac, Windows:** Full launch



Google Update 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 will change and will be named **updater.exe**. Note that the previous path will continue to persist until the transition is fully completed.

- Previous: `C:\Program Files (x86)\Google\Update\GoogleUpdate.exe`
- Current: `C:\Program Files (x86)\Google\GoogleUpdater\VERSION\updater.exe`

New and updated policies in Chrome browser

Policy	Description

WebAnnotations	Allow detecting plain text entities in web pages (on iOS only)
IdleTimeout	Delay before running idle actions (now also available on iOS)
IdleTimeoutActions	Actions to run when the computer is idle (now also available on iOS)
ChromeForTestingAllowed	Allow Chrome for Testing
RemoteAccessHostAllowPinAuthentication	Allow PIN and pairing authentication methods for remote access hosts
RemoteAccessHostAllowUrlForwarding	Allow remote access users to open host-side URLs in their local client browser
DownloadManagerSaveToDriveSettings	Allow saving files directly to Google Drive

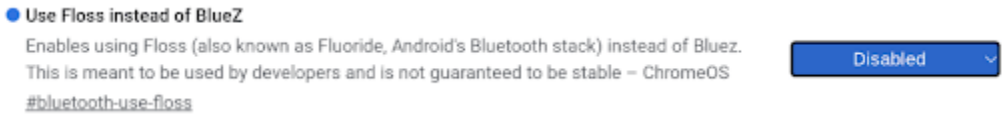
ChromeOS updates

ChromeOS Flex Bluetooth migration

In ChromeOS 123, ChromeOS Flex will upgrade to the Floss Bluetooth stack. As part of this upgrade, the listed devices no longer support Bluetooth functionality. If Bluetooth functionality is critical for these devices, we recommend moving these devices to the LTS channel to extend the Bluetooth functionality through to October 2024.

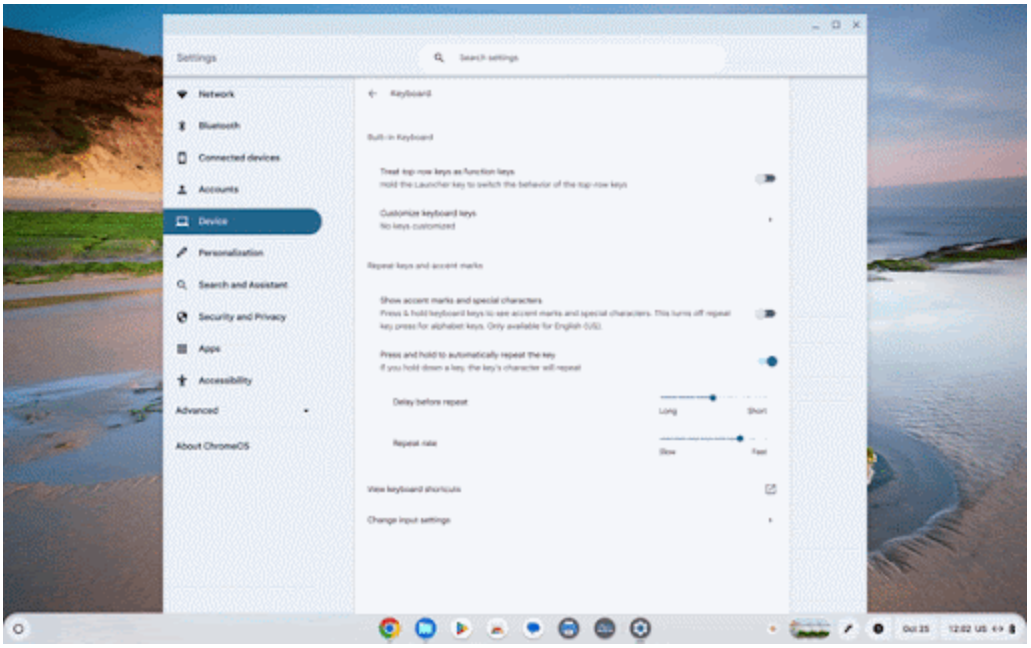
- HP Probook 4530s
- Lenovo ThinkPad T420
- HP Elitebook 8460p
- Apple iMac 11,2
- Lenovo ThinkPad x220
- Dell Vostro 3550
- HP 3115m
- HP Elitebook 2560p
- HP ProBook 6465b
- Lenovo ThinkPad L420

If your devices are unable to connect to Bluetooth after updating to ChromeOS 123, switch the Chrome flag **Use Floss instead of BlueZ** to *Disabled*. □□



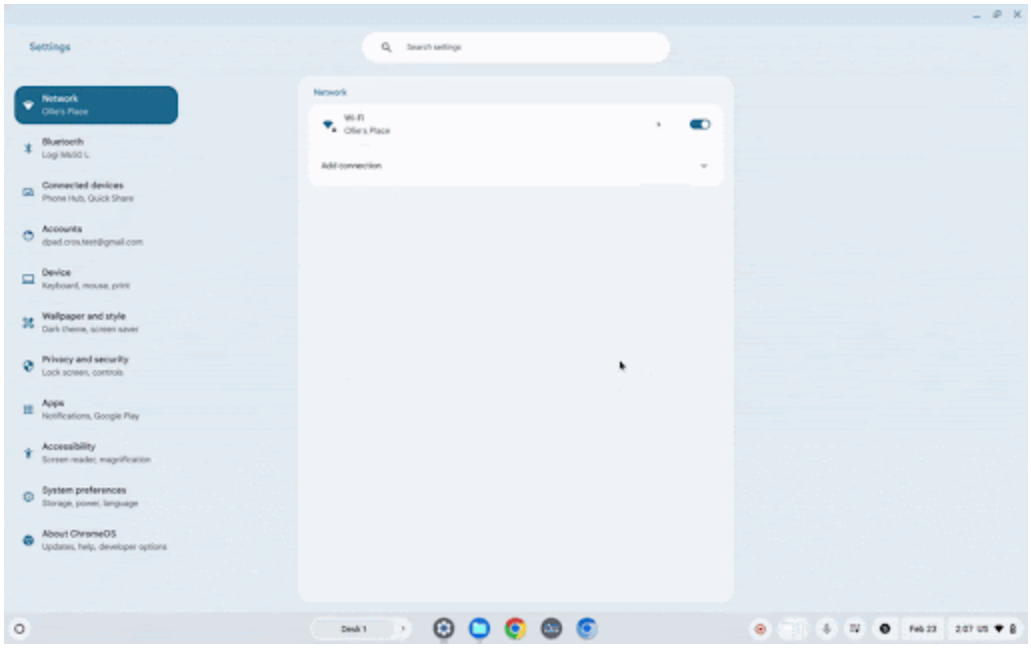
Customizing keyboard shortcuts

Using shortcuts boosts productivity, and we all have our favorites. In ChromeOS 123, with shortcut customization, you will be able to assign your preferred key combination to personalize your shortcuts. Whether you want them to be easier to do with one hand, simpler to remember, or identical to the ones you're familiar with, this feature will simplify your day-to-day workflows.



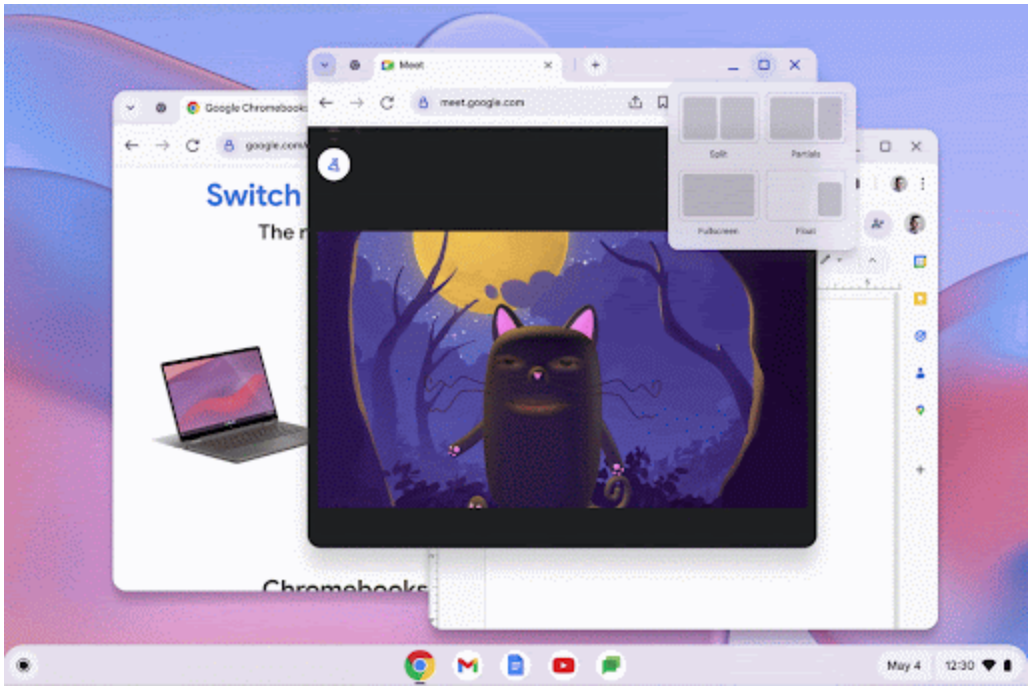
Mouse button customization

Mouse button customization on Chromebook helps users complete quick actions with the click of a button. If your mouse has more than two buttons, you can now assign those to a set list of actions such as taking a screenshot, muting and unmuting, inserting emojis, and so on. You can also select a key combination to assign to your buttons any action performed by a keyboard shortcut.



Faster Split Screen setup

Chromebooks provide a variety of ways to arrange the windows on your screen to help make you more productive — one of which is Split Screen. Just as it sounds, Faster Split Screen setup offers a quicker way to set up your window layout by showing an overview of your open windows on the other side of the screen. With Faster Split Screen, once you snap (or lock) a window in place on one side, you can choose an already-open window from **Overview** to snap into the other side, or select something from the shelf (the row of apps located at the bottom or side of your screen).

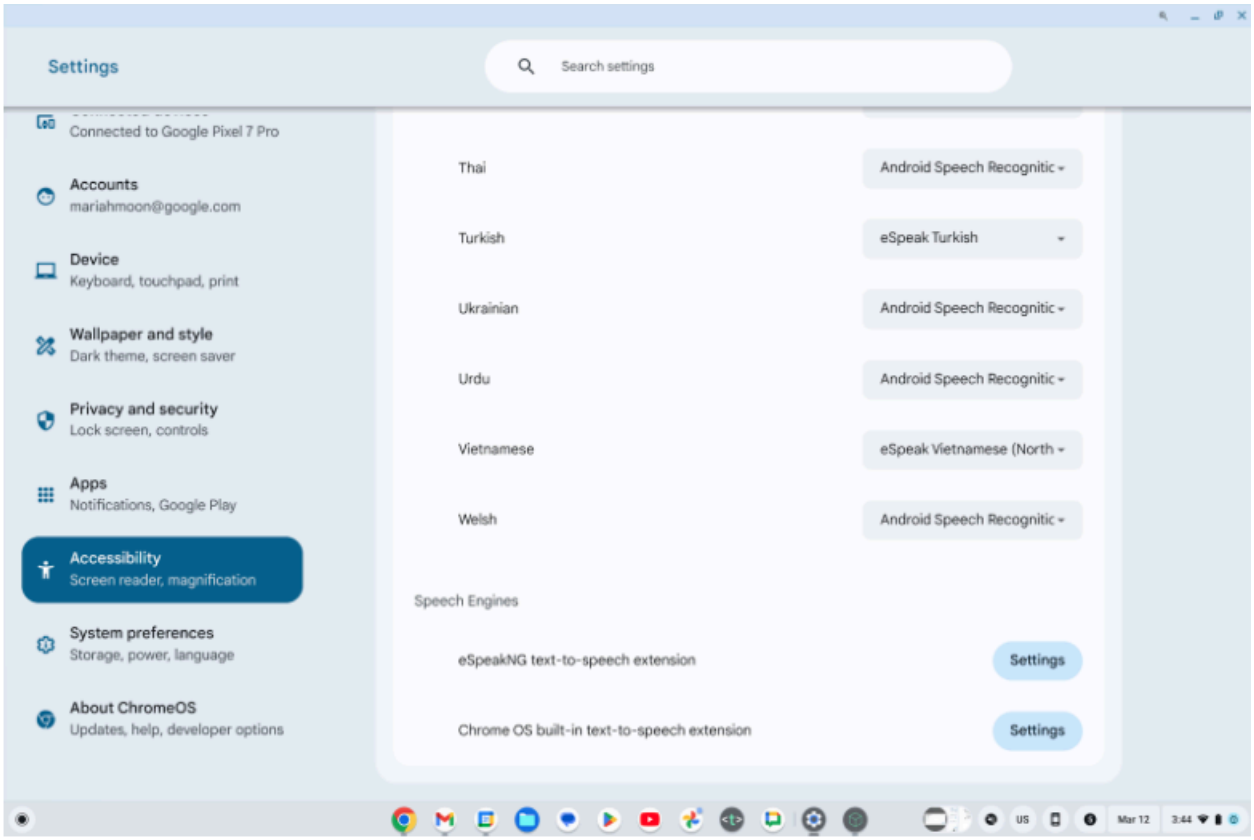


Per-app language preferences on Android

You can now change to your preferred language for your Android apps. These new settings are available in **Settings > Apps > Manage your apps > App language**.

New natural-sounding voices for text-to-speech

In ChromeOS 123, we've added new natural sounding TTS voices that work offline and are available in 31 languages.



ChromeOS Tether Hotspot

Hotspot is now available on ChromeOS! You can now share your cellular network on your Chromebook as a hotspot to other devices without an internet connection! Enable your first hotspot by opening Network Settings and toggling on Hotspot. In ChromeOS 123, we only support T-Mobile in the US but we are working to add other networks in future releases.

Data Processor mode rollout for Norway

In August 2023, data processor mode for ChromeOS was launched in the Netherlands to give organizations more transparency and control over data sent to, and processed by Google. As interest in this space increased recently, we are making data processor mode generally available in additional countries, starting with Norway. This product is available in the Admin console through **Device > Chrome > Compliance**. For more information, see our Help Center article.

Per-app privacy settings

ChromeOS 123 makes privacy controls on Chromebooks easier to manage by consolidating app permissions and privacy controls. This gives users more transparency by showing what apps need access to privacy sensors, and how app permissions are affected by privacy control states. Now with the per-app permissions, for microphone and camera, instead of going to two separate places (privacy controls and app settings), users can directly go to privacy settings to view what apps need access to these sensors and modify app permissions.

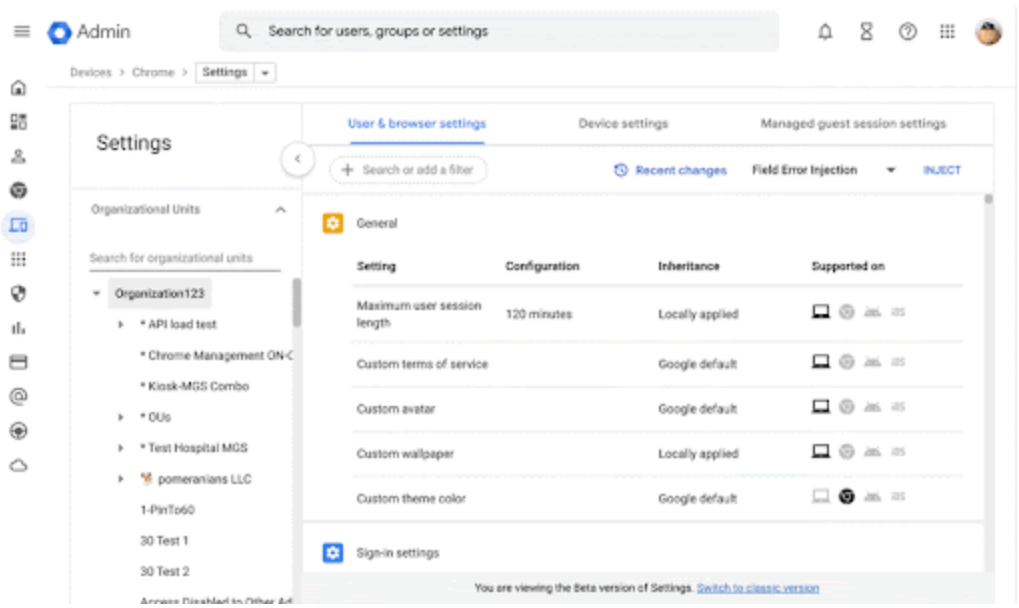
Enhanced Android security for new enterprise customers

ChromeOS 123 enhances the default app security level for enterprise customers. On new enterprise domains, ChromeOS now deactivates Android apps for unaffiliated ChromeOS users by default. Unaffiliated ChromeOS users are users on unmanaged devices or on devices that are managed by a different domain than the user.
Existing enterprise domains will not be affected by this change. Any new or existing education customer will not be affected.
Enterprise customers who want to change the default setting, see our Help Center article.

Admin console updates

Enhanced Settings page experience

Starting in March 2024, all admins will use our updated **Settings** page experience–that means you'll no longer be able to use the legacy **Settings** page experience. Most of you already use the updated experience. This just means that admins will no longer be able to access the legacy view, but you'll still have access to all the same functionality in the updated view.

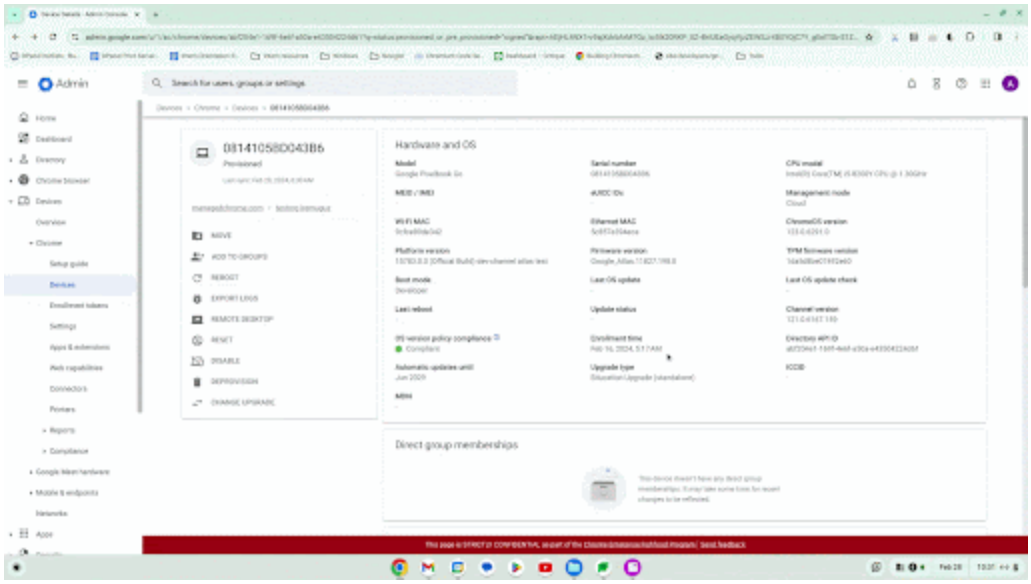


Remote log collection for ChromeOS devices

If you experience problems with a managed ChromeOS device, you can troubleshoot by capturing additional logs from the **Device details** page in the Admin console.You can remotely collect logs for following use cases :

1. Kiosk devices
2. Affiliated and unaffiliated signed-in users
3. Managed guest sessions
4. Login and Locked screen

For more information, see this Help Center article, Remote log collection for ChromeOS devices.



Inactive browser deletion in Chrome Browser Cloud Management

The Inactive period for browser deletion policy is now available for early access in the Admin console. For IT admins who find the 18 month default inadequate, this will allow them to explicitly set a policy value (inactivity period of time) a few weeks before the actual deletion starts.

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.

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.

Chrome crash report

In Chrome 123, you can visualize crash events in the Admin console using the new Chrome crash report page. In this report, you will find a dynamic chart representing Chrome crash events over time, grouped by versions of Chrome. Additional filtering is available for the following fields: OS platforms, Chrome channels and dates. This report helps you proactively identify potential Chrome issues within your organization.

- Chrome 121 on Linux, MacOS, Windows: Trusted Tester program
- **Chrome 123 on Linux, MacOS, Windows:** Feature rolls out

New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
GlanceablesEnabled	User	ChromeOS 123+	User experience
ShortcutCustomizationAllowed	User/MGS	ChromeOS 123+	User accessibility
DeleteKeyModifier	User/MGS	ChromeOS 123+	User accessibility
HomeAndEndKeysModifier	User/MGS	ChromeOS 123+	User accessibility
InsertKeyModifier	User/MGS	ChromeOS 123+	User accessibility
PageUpAndPageDownKeysModifier	User/MGS	ChromeOS 123+	User accessibility
F11KeyModifier	User/MGS	ChromeOS 123+	User accessibility
F12KeyModifier	User/MGS	ChromeOS 123+	User accessibility
ChromeForTestingAllowed	User	ChromeOS 123+	User experience
DownloadManagerSaveToDriveSettings	User	ChromeOS 123+	User experience

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

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.
- **Later this year on iOS, ChromeOS, LaCrOS, Linux, MacOS, Windows:** full roll-out for applicable users.

User link capturing on PWAs - Windows, MacOS and Linux

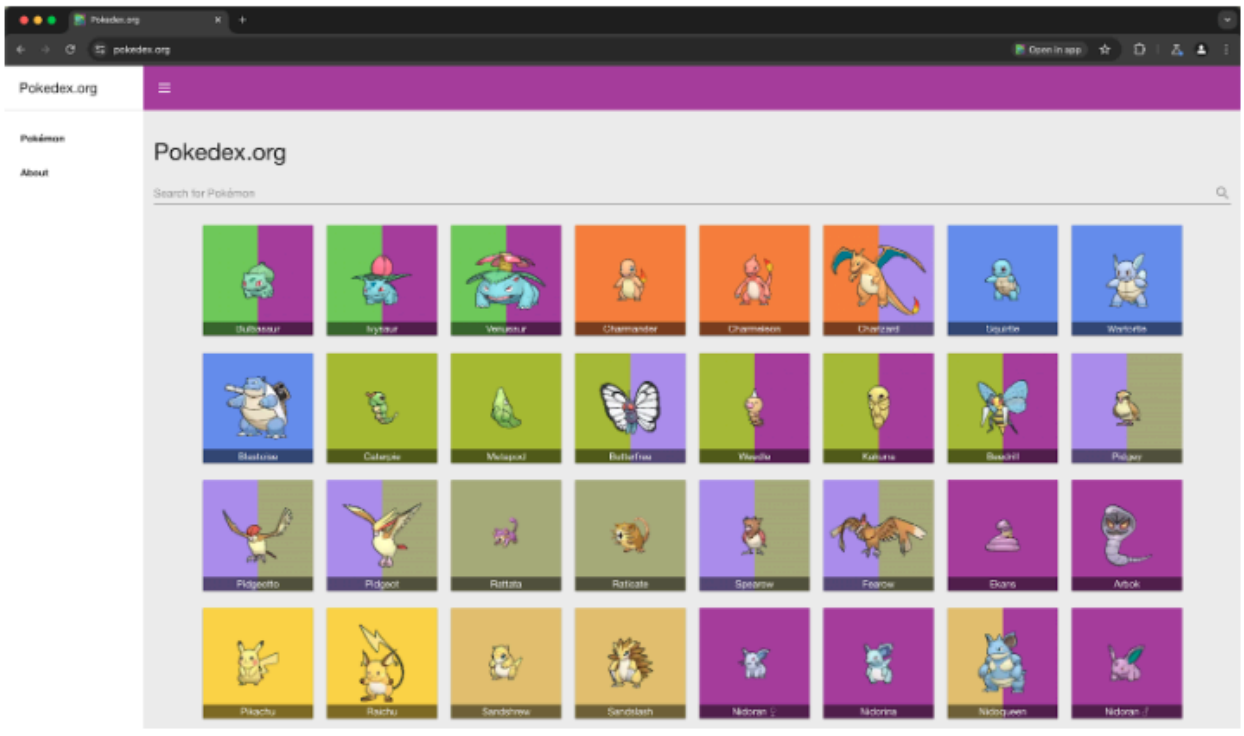
Web links automatically direct users to installed web apps. To better align with users' expectations around installed web apps, Chrome makes it easier to move between the browser and installed web apps. When the user clicks a link that could be handled by an installed web app, Chrome adds a chip in the 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.

Some issues were discovered with the current implementation, so we will not launch this feature in Chrome 123 as initially announced. We definitely plan to launch link capturing this year (bug).

- 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`.

- **Future milestone in 2024 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 user clicks on chip on address bar).



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 will require a user permission. No policies will be available to control these changes. If you encounter any issues, file a bug here.

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

Three Chrome extensions will be upgraded to Manifest V3

Three extensions will soon be updated to use Manifest V3: Legacy Browser Support for Edge, 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.

- Legacy Browser Support for Microsoft Edge - Beta
- 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**: All three extensions receive an update, on their stable version around April 30, 2024.

Bookmarks and reading list improvements on Android

On Chrome 124 on Android, some users who sign in to Chrome from the **Bookmark manager** will be able to use and save bookmarks and reading list items in their Google Account. Relevant enterprise policies, such as BrowserSignin, SyncTypesListDisabled, EditBookmarksEnabled, ManagedBookmarks and ShoppingListEnabled will 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.

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 by Chrome 124. The discussions around the throttling issue (and its resolution) can be found at https://bugs.chromium.org/p/chromium/issues/detail?id=958475.

- **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 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 are available.

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 eventually be removed.

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

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 124 on Windows:** Network Service sandboxed on Windows.

Deprecate and remove WebSQL

With SQLite over WASM as its official replacement, we plan to remove WebSQL 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.

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, Mac, 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 check RSA key usage for server certificates issued by local trust anchors. In Chrome 124, both **InsecureHashesInTLSHandshakesEnabled** and **RSAKeyUsageForLocalAnchorsEnabled** policies will be 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**

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.

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.

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

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 Browser Cloud Management. 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.

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

Upcoming ChromeOS changes

Record GIFs with Screen capture

As early as ChromeOS 124, **Screen capture** will let you record your screen in .GIF format to easily capture, share, and play the recording inline in chat, slides, docs, and more.

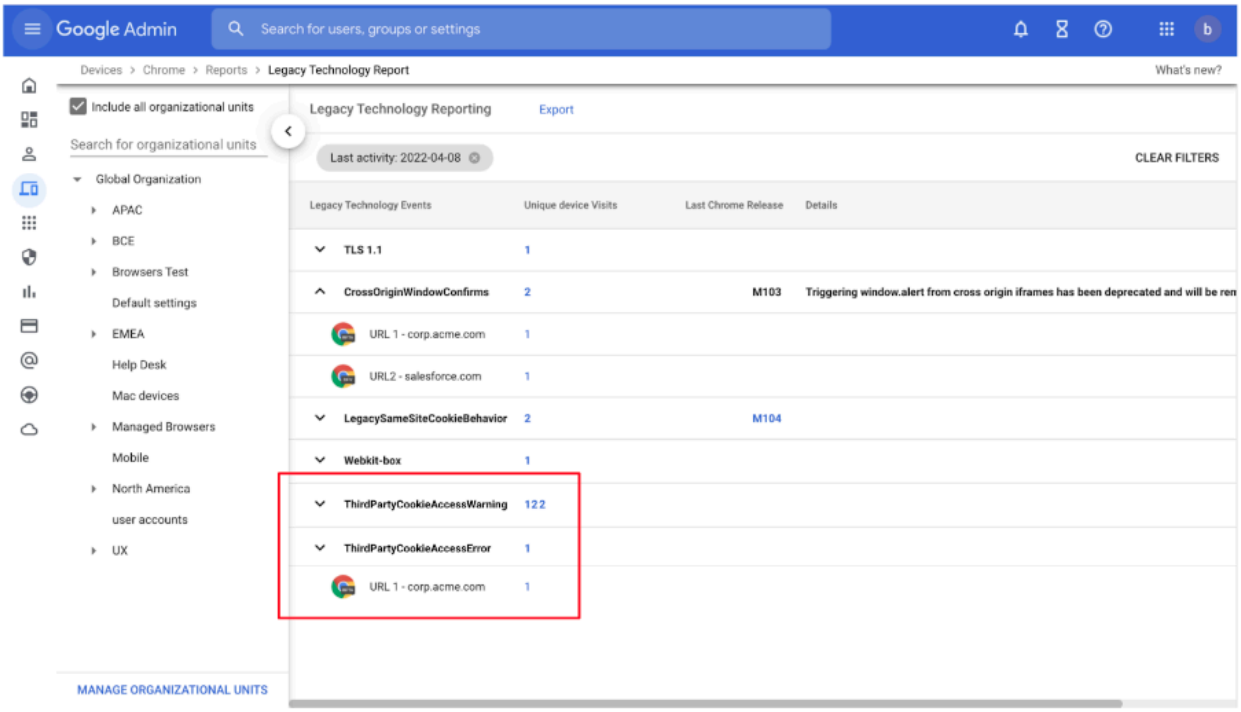
Upcoming Admin Console changes

Legacy Technology report

As early as Chrome 124, 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 124 on Linux, MacOS, Windows:** Legacy Technology report will be available in the Admin console.



Policy parity: Custom Configurations for IT admins

The **Custom Configurations** page allows IT admins to configure Chromium policies that are not yet in the Admin console, using JSON scripts. As a result, all Chrome policies are now configurable in Chrome Browser Cloud Management in the Admin console, either using the **Settings** page or the **Custom Configurations** page.

- **As early as Chrome 124 on Android, iOS, Linux, Mac, Windows:** Trusted Tester access
- As early as Chrome 125 on Android, iOS, Linux, Mac, Windows: Feature rolls out

Previous release notes

Chrome version & targeted Stable channel release date	PDF
Chrome 122: January 17, 2023	PDF
Chrome 121: January 17, 2023	PDF
Chrome 120: November 29, 2023	PDF
Chrome 119: October 25, 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