Chrome 120 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 November 29, 2023.

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

Chrome 120 release summary

Chrome Browser updates	Security/Privacy	User productivity/Apps	Management
Default Search Engine choice screen		✓	
Chrome Third-Party Cookie Deprecation (3PCD)	✓		
Rename FirstPartySets Enterprise Policies to RelatedWebsiteSets	✓		✓
Chrome Web Store: UX Improvements		✓	
Revamped Safety Check on Desktop	✓		
Chrome Desktop responsive toolbar		✓	
Chrome on Android no longer supports Android Nougat			✓
Package tracking (iOS only)		✓	
Unprefix -webkit-background-clip for text and make it an alias	✓		
Chrome user policies for iOS			✓
Chrome profile separation: new policies			✓
Migrate away from data URLs in SVGUseElement	✓	✓	
Password Manager: password sharing		✓	✓
Remove recommended support from multiple policies			✓
Save images to Google Photos on iOS			✓
Remove same-origin blanket enforcement in CSPEE	✓		

Close requests for CloseWatcher, <dialog>, and popover=""	✓		
Deprecate and remove Theora support	✓		
Unmanaged device signals consent			✓
New and updated policies in Chrome browser			✓
Removed policies in Chrome browser			✓
ChromeOS updates	**Security/Privacy**	**User productivity/Apps**	**Management**
New controls for mouse scroll acceleration		✓	
Enhanced *Alt + click* behavior		✓	
XDR Authentication Events			✓
Pinch-to-Resize PiP		✓	
New look for Emoji Picker		✓	
Keyboard Shortcuts - Enabling F11-F12 keys		✓	
Deprecate support for legacy ChromeOS media containers and codecs			✓
ChromeOS Virtual Desk button		✓	
App Details in App Management			✓
Admin Console Updates	**Security/Privacy**	**User productivity/Apps**	**Management**
New policies in the Admin console			✓
Upcoming Chrome Browser updates	**Security/Privacy**	**User productivity/Apps**	**Management**
Generative AI features		✓	

Safer encrypted archives for Standard Safe Browsing users	✓		
Permissions prompt for Web MIDI API	✓		
Network Service on Windows will be sandboxed	✓		
User Link Capturing on PWAs - Windows, Mac and Linux	✓		
Side Panel Navigation: Pinning/Unpinning		✓	
SharedImages for PPAPI Video Decode	✓		
Resume the last opened tab on any device		✓	
Skip unload events	✓		
Remove support for UserAgentClientHintsGREASEUpdateEnabled			✓
Chrome Sync ends support for Chrome 81 and earlier	✓		✓
Deprecate and remove WebSQL	✓		
Remove LegacySameSiteCookieBehaviorEnabledForDomainList policy			✓
Intent to deprecate: Mutation Events		✓	
Extensions must be updated to leverage Manifest V3	✓	✓	✓
Upcoming ChromeOS updates	**Security/Privacy**	**User productivity/Apps**	**Management**
ChromeOS Flex End of Device Support			✓
ChromeOS Flex Bluetooth Migration			✓

Set the screensaver duration		✓	
New look for ChromeOS media player		✓	
Integrate the DLP events into the security investigation tool	✓		
Enterprise DataControls (DLP) files restrictions	✓		
Enhanced notifications for pinned apps		✓	
New ChromeOS sync options	✓	✓	
App disablement by Admin in MGS			✓
Upcoming Admin Console Updates	**Security/Privacy**	**User productivity/Apps**	**Management**
Inactive browser deletion in Chrome Browser Cloud Management			✓
Apps & Extensions usage report: Highlight extensions removed from the Chrome Web Store			✓
Legacy Technology report			✓
Chrome Crash 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

Default Search Engine choice screen

Starting Chrome 120, enterprise end-users might be prompted to choose their default search engine within Chrome.
As part of our building for DMA compliance, some users will be prompted to choose their default search engine for Chrome. This prompt controls the default search engine setting, currently available at `chrome://settings/search`. The enterprise policies, DefaultSearchProviderEnabled and DefaultSearchProviderSearchUrl, will continue to control this setting as it does today, if it is set by the IT admin. Read more on this policy and the related atomic group.

- **Chrome 120 on iOS, Chrome OS, LaCrOS, Linux, Mac, Windows:** 1% users might start getting the choice screen with Chrome 120. 100% by Chrome 122 for applicable users.

Chrome Third-Party Cookie Deprecation (3PCD)

In Chrome 120 and beyond (Jan 2024), Chrome will globally disable third-party cookies for 1% of Chrome traffic as part of our Chrome-facilitated testing in collaboration with the CMA. The facilitated 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 will have bounce tracking mitigations take effect, so that their state is cleared for sites that get classified as a bounce tracker. Most enterprise users should be excluded from this experiment group automatically; however, we recommend that admins proactively use the BlockThirdPartyCookies and CookiesAllowedForUrls policies to re-enable third-party cookies and opt out their managed browsers ahead of the experiment. This will give enterprises time to make the changes required to not rely on this policy or third-party cookies.

We plan to provide more tooling (such as the Legacy Tech 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 User Bypass control (the "eye icon" in the omnibox) to temporarily re-enable third-party cookies for 90 days on a given site when necessary. Enterprise admin policies override User Bypass controls, for example, setting BlockThirdPartyCookies policy to `true` will disable third-party cookies for all sites and prevent users from using this User Bypass control.

Bounce tracking protections are also covered by the same policies as cookies and enforced when the bouncing site is not permitted to have/receive 3P cookies. Thus, setting the **BlockThirdPartyCookies** policy to `false`, or setting the **CookiesAllowedForUrls** policy for a site, will prevent bounce tracking mitigations from deleting state for sites.

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

The heuristics feature will grant 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 the *Mode B: 1% third-party cookie deprecation* blog section and the Preparing for the end of third-party cookies blog.

- **Chrome 120 on ChromeOS, Linux, Mac, 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.

Rename FirstPartySets policies to RelatedWebsiteSets

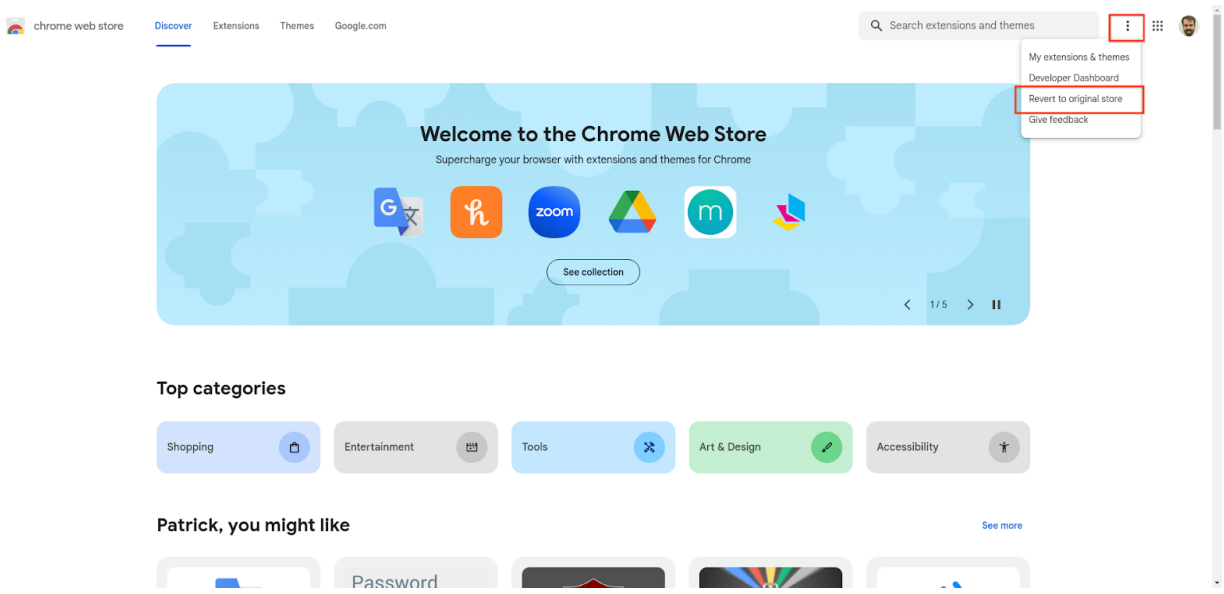
The FirstPartySetsEnabled and FirstPartySetsOverrides enterprise policies are renamed to RelatedWebsiteSetsEnabled and RelatedWebsiteSetsOverrides respectively. There is no change in the policies' behavior. Administrators should use the new policies RelatedWebsiteSetsEnabled and RelatedWebsiteSetsOverrides going forward. To learn more about the rename, follow https://developer.chrome.com/blog/related-website-sets/

- **Chrome 120 on Android, Chrome OS, LaCrOS, Linux, Mac, Windows, Fuchsia**

Chrome Web Store: UX improvements

The Chrome team is unveiling a redesigned Chrome Web Store that simplifies the process of finding and managing extensions. Alongside a refreshing, modern interface, the store introduces new extension categories, including AI-powered extensions and Editors' spotlight. These enhancements will be gradually rolled out over the coming months.

Users can temporarily switch back to the original store layout by clicking the three dots next to their profile avatar and selecting Revert to original store. This temporary option will be disabled in January 2024 and cannot be centrally controlled by administrators.



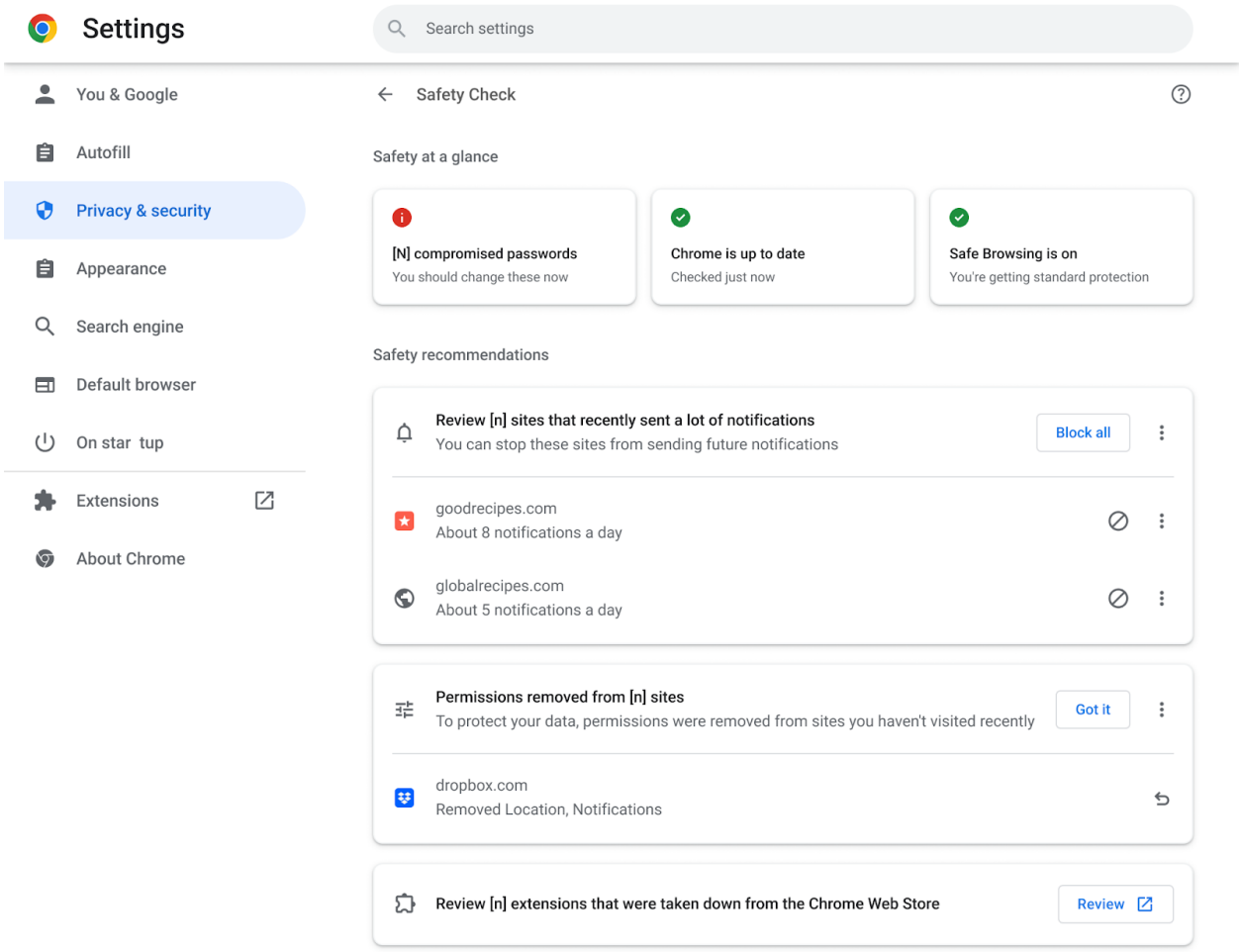
Enterprises will continue to have access to their enterprise policies within the new Chrome Store UX.
The revamped Chrome Web Store will also feature a dedicated section for extensions specific to your domain. For more details on publishing private extensions, see Enterprise Publishing Options.

Note that there is a known issue with ExtensionSettings, where the `blocked_install_message` does not appear correctly in the redesigned Chrome Store UX that we are working on fixing.

Revamped Safety Check on Desktop

In Chrome 120, we begin to roll out a new proactive **Safety Check** that regularly checks the browser for safety-related issues and informs users when there's anything that needs their attention. This launch also introduces a new page with Chrome's proactive safety-related actions and information tailored to each user, designed to make it easier for users to stay safe online.

- **Chrome 120 on ChromeOS, LaCrOS, Linux, Mac, Windows**



Chrome Desktop responsive toolbar

Chrome Desktop customers across devices and input modes (for example, Mouse or Touch) now experience a toolbar that seamlessly responds to changing window sizes. This happens when users manually select and resize a window or use OS-specific window management tools in addition to an overflow menu.

- **Chrome 120 on ChromeOS, LaCrOS, Linux, Mac, Windows**

Chrome on Android no longer supports Android Nougat

The last version of Chrome that supports Android Nougat is Chrome 119, and it includes a message to affected users informing them to upgrade their operating system.

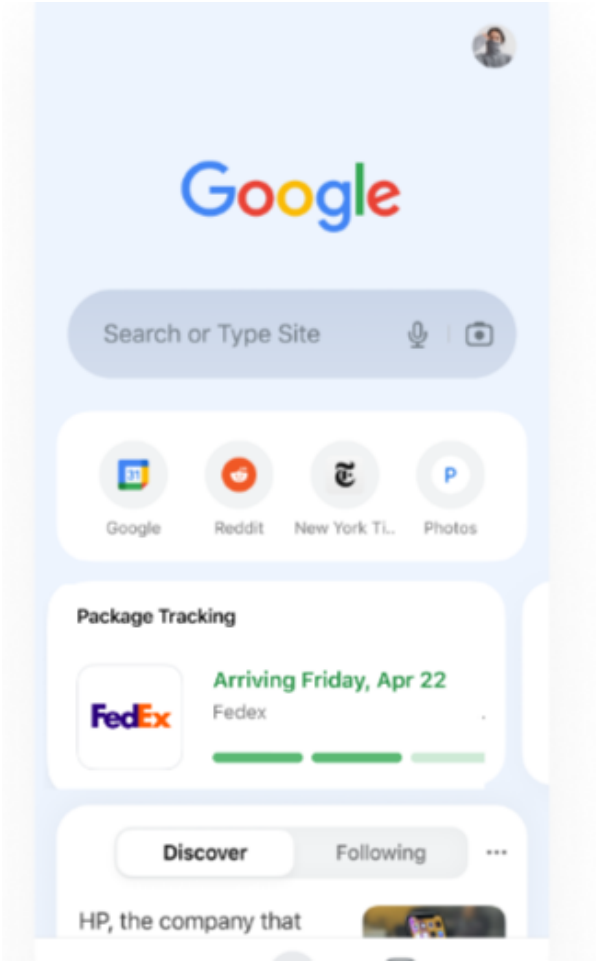
Chrome 120 does not support nor ship to users running Android Nougat.

- **Chrome 120 on Android:** Chrome on Android no longer supports Android Nougat

Package tracking (iOS only)

Users can enable a new package tracking feature that results in estimated delivery dates and package status appearing in a new card on the **New tab** page. This feature is only supported for en-US users and only for packages fulfilled via FedEx and USPS. If needed, you can turn off the feature using a new policy called ParcelTrackingEnabled.

- **Chrome 120 on iOS:** feature launches



Unprefix -webkit-background-clip for text and make it an alias

Chrome allows the use of the unprefixed version for `background-clip: text` and makes `-webkit-background-clip` an alias for `background-clip`. Also, it drops support for non-suffixed keywords (`content`, `padding` and `border`)..

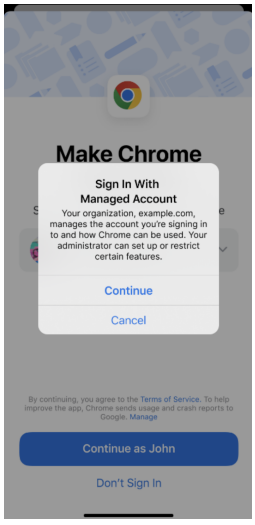
- **Chrome 120 on Windows, Mac, Linux, Android**

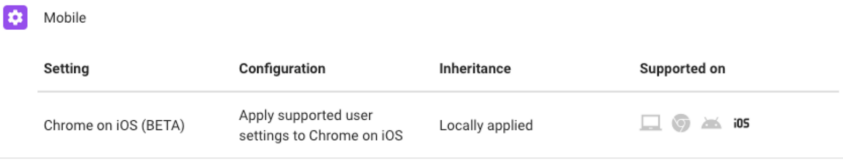
Chrome user policies for iOS

With Chrome user policies for iOS, admins can apply policies and preferences across a user's devices. Settings apply whenever the user signs in to Chrome browser with their managed account on any device, including personal devices.

Starting in Chrome 120, to bring consistency to iOS, managed end-users start to see a management notice stating that their organization manages the account they are signing into. In Chrome 121, admins can turn on this functionality in the Admin console under the **Chrome on iOS** setting. For more information, see Set Chrome policies for users or browsers.

- **Chrome 120 on iOS:** Feature starts gradual roll out.





Chrome profile separation: new policies

Three new policies are now available to help you configure enterprise profiles: **ProfileSeparationSettings**, **ProfileSeparationDataMigrationSettings**, **ProfileSeparationSecondaryDomainAllowlist**. These policies take precedence over ManagedAccountsSigninRestriction and EnterpriseProfileCreationKeepBrowsingData.

- **Chrome 120 on Linux, Mac, Windows**

Migrate away from data URLs in SVGUseElement

The SVG spec was recently updated to remove support for data: URLs in `SVGUseElement`. This improves security of the Web platform as well as compatibility between browsers as Webkit does not support data: URLs in `SVGUseElement`. To read more, see this blog post.

Assigning data: URLs in `SVGUseElement` can lead to Cross-Site Scripting (XSS) and Trusted Types bypass.

For enterprises that need additional time to migrate, the **DataUrlInSvgUseEnabled** policy will be available until Chrome 128 to re-enable Data URL support for `SVGUseElement`.

- **Chrome 120 on Android, ChromeOS, LaCrOS, Linux, Mac, Windows, Fuchsia:** Remove support for data: URLs in `SVGUseElement`

Password Manager: password sharing

Password Manager allows users to share their passwords with members of their Google Family Group (as configured in their Google Account). Users can only share one password at a time. It is not possible to share passwords in bulk. The shared password cannot be updated or revoked by the sender.
As an enterprise admin, you can use the **PasswordSharingEnabled** policy to switch off the share feature for all users.

- **Chrome 120 on iOS, Chrome OS, LaCrOS, Linux, Mac, Windows, Fuchsia**

Remove recommended support from multiple policies

Some policies can be applied as recommended, allowing admins to set an initial value that users can later change. In Chrome 119, recommended support was removed from multiple policies that users had no way of configuring.

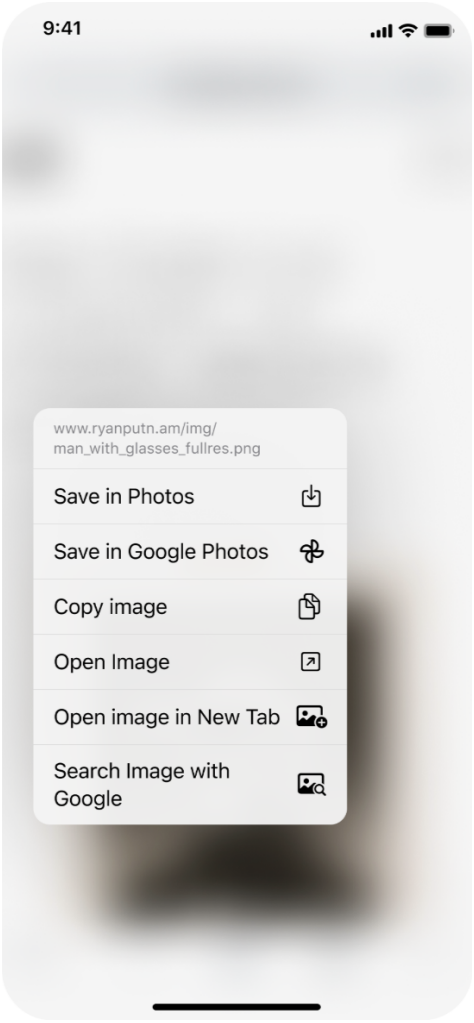
Any affected policies that were previously set as recommended now need to be set as mandatory to ensure they continue to take effect.

- Chrome 119 on Linux, Mac, Windows: Recommended support is being removed from the PrintPdfAsImageDefault enterprise policy.
- **Chrome 120 on Android, Linux, Mac, Windows:** Recommended support is being removed from the following enterprise policies:
    - AlternateErrorPagesEnabled
    - PasswordDismissCompromisedAlertEnabled
    - PasswordLeakDetectionEnabled
    - SafeBrowsingForTrustedSourcesEnabled

Save images to Google Photos on iOS

When a signed-in user long-presses on an image in Chrome, they can save it directly to Google Photos. They have the option to save it to any account logged in on the device. You can use the ContextMenuPhotoSharingSettings policy to turn on this feature.

- Chrome 119 on iOS: Users can directly save images to Google photos
- **Chrome 120 on iOS:** A new policy, ContextMenuPhotoSharingSettings , is introduced to control this functionality



Remove same-origin blanket enforcement in CSPEE

Chrome 120 removes a special treatment for same-origin iframes from CSP Embedded Enforcement.
This aligns the behavior of CSP Embedded Enforcement for cross-origin iframes and same-origin iframes. To read more, see ChromeStatus.

- **Chrome 120 on Windows, Mac, Linux, Android**

Close requests for CloseWatcher, <dialog>, and popover=""

Close requests are a new concept where a user requests to close something currently open, using the *Esc* key on desktop or the back gesture or button on Android. Integrating *Close requests* into Chromium comes with two changes:

- CloseWatcher, a new API for directly listening and responding to close requests.
- Upgrades to `<dialog>` and `popover=""` to use the new close request framework, so that they respond to the Android back button.

- **Chrome 120 on Windows, Mac, Linux, Android**

Deprecate and remove Theora support

Chrome 120 deprecates and removes support for the Theora video codec in Chrome desktop, due to emerging security risks. Theora's low (and now often incorrect) usage no longer justifies support for most users. Ogg containers will remain supported. Our plan is to begin escalating experiments turning down Theora support in Chrome 120. If users encounter problems playing specific videos, they can reactivate support via `chrome://flags/#theora-video-codec` if needed until Chrome 123. You can find more info in Chrome Status.

- **Chrome 120 on ChromeOS, LaCrOS, Windows, Mac, Linux**

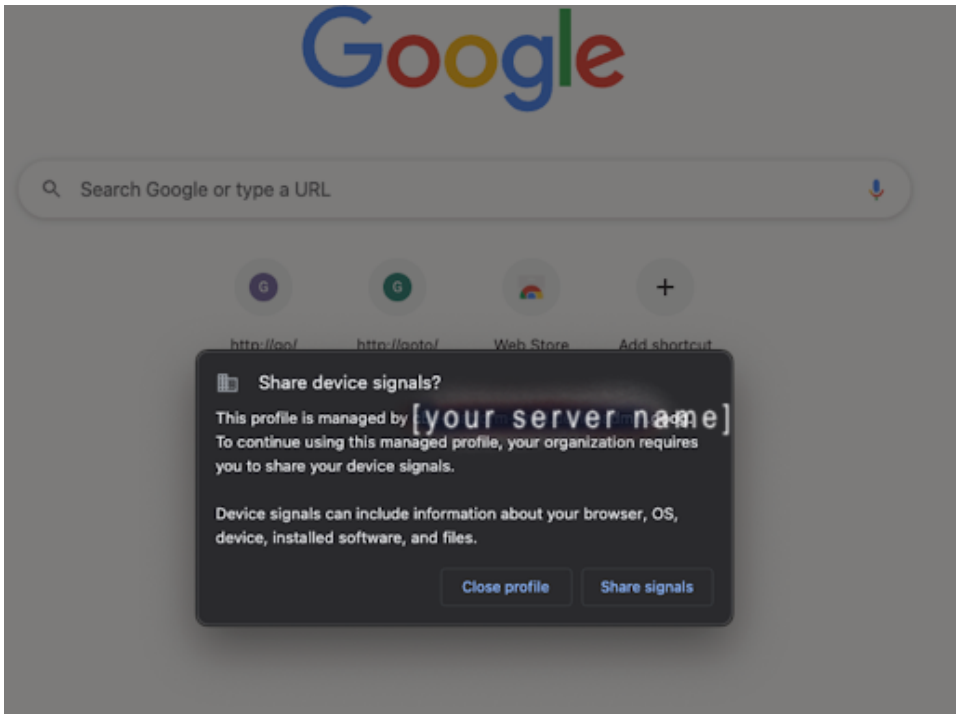
Unmanaged device signals consent

This feature introduces a new consent popup dialog, which collects users' consent on whether they allow Chrome to collect device signals from their device.

The dialog is only displayed for users who satisfy the following conditions:
- user is managed
- user's current device is unmanaged

- user's admin enabled the device trust service
- user's admin did not specifically disable this feature and its corresponding policy

- **Chrome 120 on Linux, Mac, Windows**



New and updated policies in Chrome browser

Policy	Description
ExtensionInstallTypeBlocklist	Blocklist for install types of extensions
ParcelTrackingEnabled	Allows users to track their packages on Chrome (available on iOS)
RelatedWebsiteSetsOverrides	Override Related Website Sets
RelatedWebsiteSetsEnabled	Enable Related Website Sets

DataUrlInSvgUseEnabled	Data URL support for SVGUseElement
ContextMenuPhotoSharingSettings	Allow saving images directly to Google Photos (available on iOS)
FeedbackSurveysEnabled	Specifies whether in-product Google Chrome surveys are shown to users
NativeHostsExecutablesLaunchDirectly	Force Windows executable Native Messaging hosts to launch directly
IPv6ReachabilityOverrideEnabled	Enable IPv6 reachability check override
PasswordSharingEnabled	Enable sharing user credentials with other users
PrivateNetworkAccessRestrictionsEnabled	Specifies whether to apply restrictions to requests to more-private network endpoints

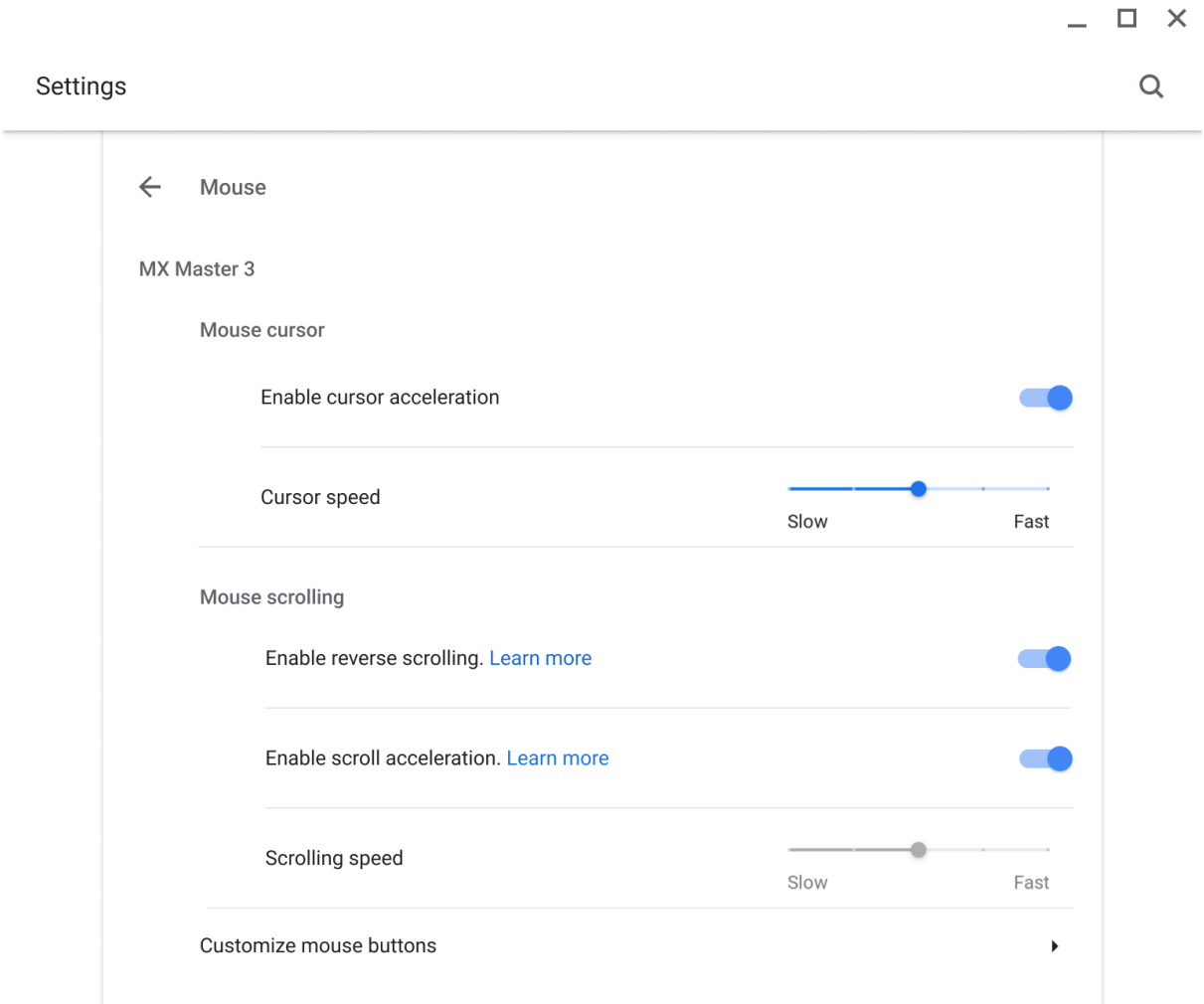
Removed policies in Chrome browser

Policy	Description
NativeClientForceAllowed	Forces Native Client (NaCl) to be allowed to run.
ChromeRootStoreEnabled	Determines whether the Chrome Root Store and built-in certificate verifier will be used to verify server certificates

ChromeOS updates

New controls for mouse scroll acceleration

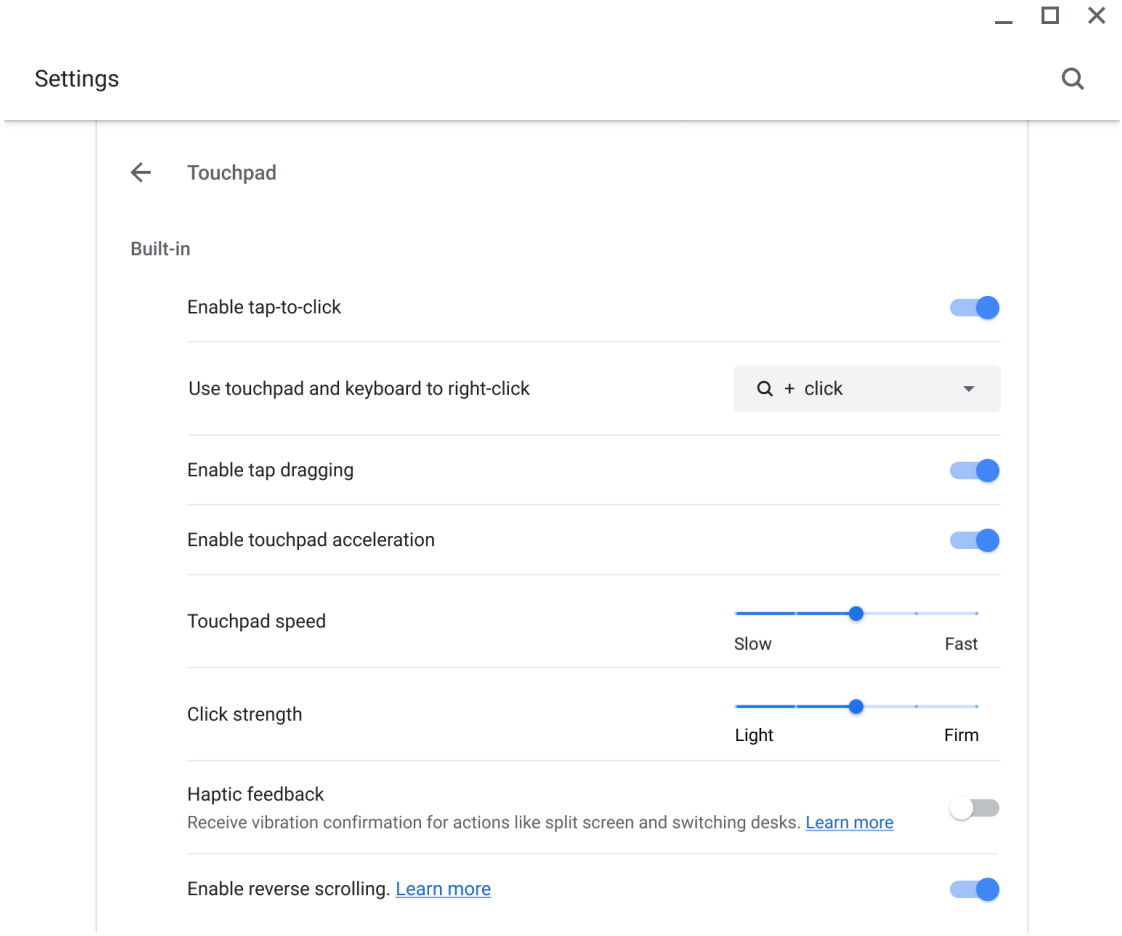
ChromeOS 120 adds new controls to let users disable mouse scroll acceleration and adjust the speed of the scrolling.



Enhanced *Alt + click* behavior

You can configure right-click behavior using the keyboard and touchpad. You can also configure settings for actions such as Home, End, and Page Up, in the **Customize keyboard**

keys subpage.



XDR Authentication Events

Authentication events (login/out lock/unlock) can now be enabled as part of Extended Detection and Response (XDR) on ChromeOS. Once rollout is complete, XDR systems will be able to use these events to provide insights on the device security posture.

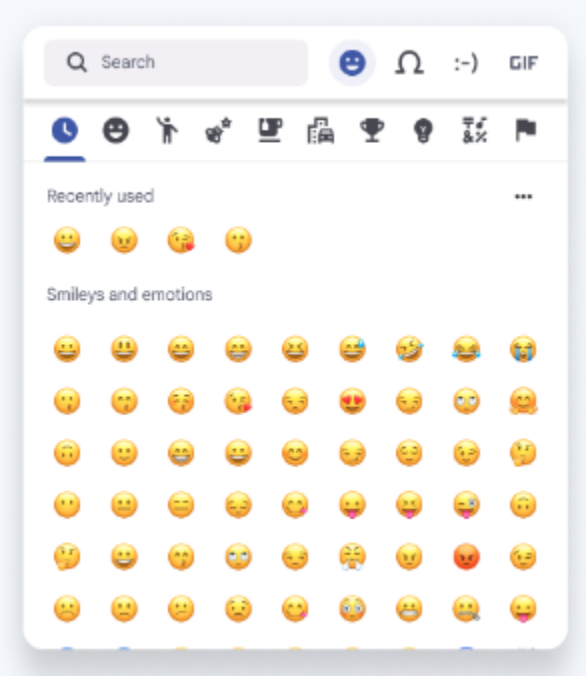
Pinch-to-Resize PiP

Picture-in-Picture (PiP) windows can now be resized with a pinch. Simply place two fingers on the window and pinch them together or spread them apart to find the perfect size for your

screen.

New look for Emoji Picker

ChromeOS 120 brings a new dynamic color palette to the floating Emoji and GIF Picker.



Keyboard Shortcuts - Enabling F11-F12 keys

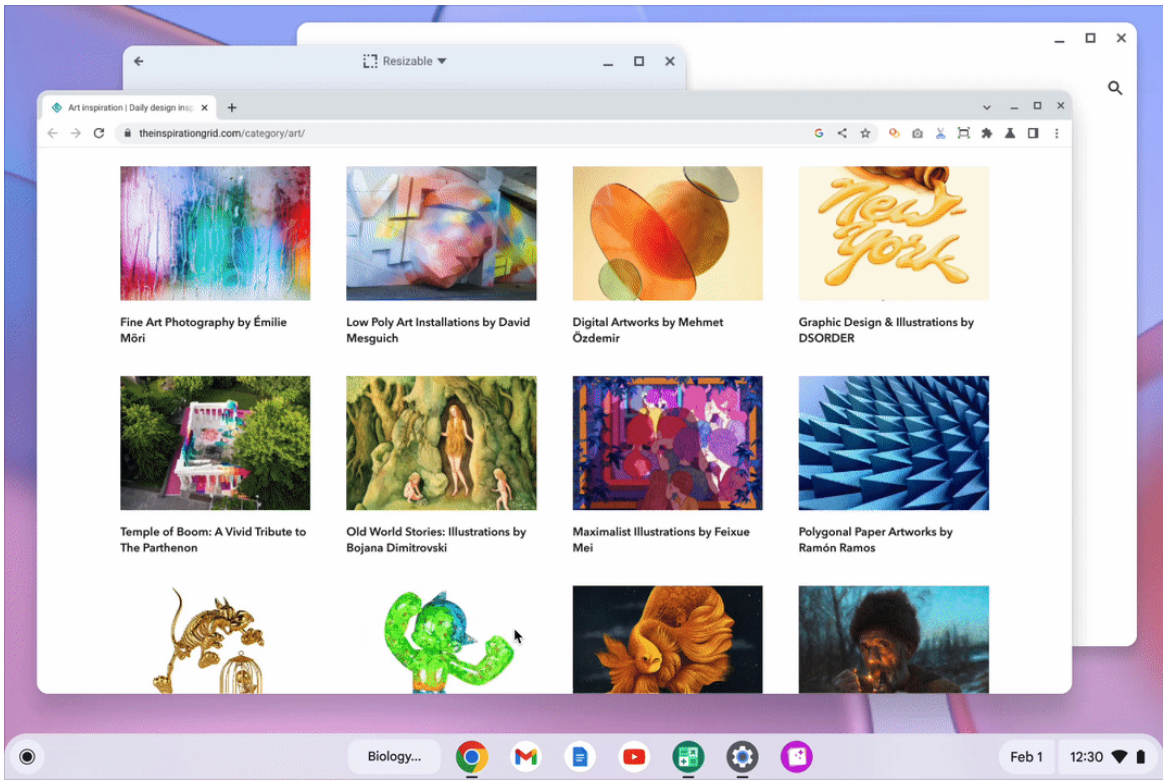
Most ChromeOS keyboards lack F11 and F12 keys, which are expected functionality in many applications. This proposal adds options to remap F11 and F12 keys in the Keyboard key remapping section in Settings.

Deprecate support for legacy ChromeOS media containers and codecs

Deprecated support for MPEG4 Part 2 video codec and AVI container in ChromeOS 120. Users needing this functionality may temporarily re-enable support using `chrome://flags/#cros-legacy-media-formats` until ChromeOS 125, after which support will be removed.

ChromeOS Virtual Desk Button (Bento Button)

Bento Button is a shelf button that's available for all users who utilize virtual desks. The button will allow quick access to desk operations for desk visualizing, desk switching, desk creation and desk ordering. If the user has previously saved desks, they would be able to go to the desk library as well.



App Details in App Management

Settings now include additional details about installed apps. Navigate to **Settings > Apps > Manage** your apps, select an app to view the app's storage usage, version number, and information about how it was installed.

Admin console updates

New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
PowerManagementIdleSettings (screen dim, screen off, idle actions)	User, MGS	ChromeOS	Power and shutdown - Idle settings
ScreenLockDelays	User, MGS	ChromeOS	Power and shutdown - Idle settings
LidCloseAction	User, MGS	ChromeOS	Power and shutdown - Idle settings
ChromeOsLockOnIdleSuspend (lock screen on lid close)	User, MGS	ChromeOS	Power and shutdown - Idle settings
NativeHostsExecutablesLaunchDirectly	User	Chrome Browser	Other settings
ParcelTrackingEnabled	User	Chrome for iOS	Content settings
FeedbackSurveysEnabled	User, MGS	ChromeOS, Chrome Browser, Chrome for Android	Other settings
ExtensionInstallTypeBlocklist	Additional app settings	Chrome Browser	Additional app settings
ContextMenuPhotoSharingSettings	User	Chrome for iOS	Content settings
PrivateNetworkAccessRestrictionsEnabled	User, MGS	ChromeOS, Chrome Browser, Chrome for Android	Network settings

DeviceFlexHwDataForProductImprovementEnabled	Device	ChromeOS	Other settings
IPv6ReachabilityOverrideEnabled	User	ChromeOS, Chrome Browser, Chrome for Android	Network settings
DataUrlInSvgUseEnabled	User, MGS	ChromeOS, Chrome Browser, Chrome for Android	Security

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

Generative AI features

In Chrome 115, Google introduced its first Generative AI (GenAI) integration in the Search Side Panel. As early as Chrome 121, additional GenAI features will be rolled out to Chrome. You'll be able to opt in through a new `chrome://settings` page. Enterprise policies will be available at roll-out to control these features. More details will be shared in upcoming milestones.

- **(Earliest) Chrome 121 on ChromeOS, Linux, Mac, Windows**

Safer encrypted archives for Standard Safe Browsing users

Standard Safe Browsing users will be prompted for a password to some encrypted archive downloads. This will be used to collect more metadata about the download (such as contained file hashes and executable signatures), which will be sent to Google for better quality verdicts. The password will remain local. You can control this feature with the SafeBrowsingDeepScanningEnabled policy.

- **Chrome 121 on Linux, Mac, Windows**

Permissions prompt for Web MIDI API

There have been several reported problems around Web MIDI API's drive-by access to client MIDI devices (bugs). To address this problem, the Audio WG decided to place an explicit

permission on the general MIDI API access. Originally, the explicit permission was only required for advanced MIDI usage (System Exclusive (SysEx) messages) in Chrome, with gated access behind a permissions prompt. We plan to expand the scope of the permission to regular MIDI API usage.

Today the use of SysEx messages with the Web MIDI API requires an explicit user permission. With this implementation, even access to the Web MIDI API without SysEx support will require a user permission. Three new policies—**DefaultMidiSetting, MidiAllowedForUrls and MidiBlockedForUrls**—will be available to allow administrators to pre-configure user access to the API.

- **Chrome 121 on Windows, Mac, 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 121 on Windows:** Network Service sandboxed on Windows

User Link Capturing on PWAs - Windows, Mac and Linux

Web links automatically direct users to installed web apps. To better align with users' expectations around installed web apps, Chrome will make it more seamless to move between the browser and installed web apps. When the user clicks on a link that could be handled by an installed web app, Chrome will add a chip in the address bar to suggest switching over to the app. Clicking on the chip would either launch the app directly, or open a grid of apps that can support that link. For some users, clicking on a link will always automatically open the app.

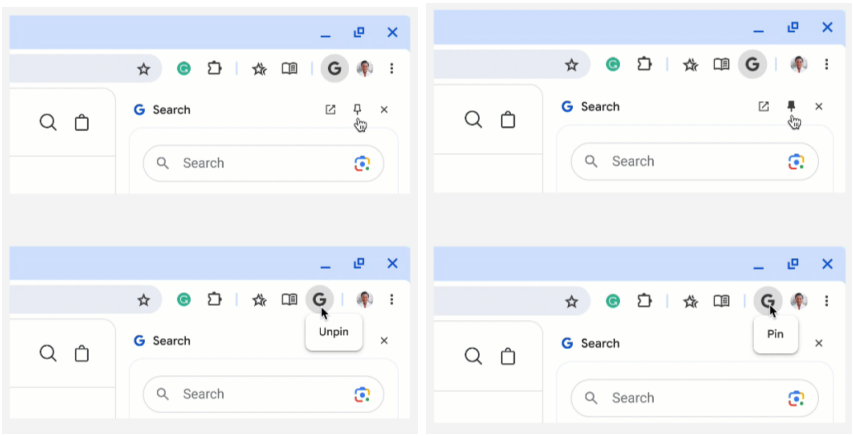
- **Chrome 121 on Linux, Mac, Windows:** When some users click on a link, it will always open in an installed PWA, while some users will see the link open in a new tab with a chip in the address bar clicking on which will launch the app. This is an experiment to determine if users prefer having links launched by default. The experiment will run on Canary/Dev/Beta and 1% of Stable.

- Chrome 123 on Linux, Mac, Windows: Based on the outcome of the experiment in Chrome 121, 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).

Side Panel Navigation: Pinning/Unpinning

As early as Chrome 121, the side panel icon is being removed in favor of evolving the side panel navigation to offer customization through toolbar pinning. This will allow for efficient direct access to a suite of panels.

- **Chrome 121 on Chrome OS, LaCrOS, Linux, Mac, Windows, Fuchsia**



SharedImages for PPAPI Video Decode

Chrome 119 introduces a new PPAPISharedImagesForVideoDecoderAllowed policy to control the recent refactor for VideoDecoder APIs in PPAPI plugin.

- Chrome 119 on ChromeOS, LaCrOS: Introduces escape hatch policy.
- **Chrome 122 on ChromeOS, LaCrOS:** Escape hatch policy and corresponding old code paths are removed.

Skip unload events

The presence of unload event listeners is a primary blocker for back/forward cache on Chromium based browsers and for Firefox on desktop platforms. On the other hand, for mobile platforms, almost all browsers prioritize the bfcache by not firing unload events in most cases. To improve the situation, we've been working with lots of partners and successfully reduced the use of unload event listeners over the last few years. To further accelerate this migration, we propose to have Chrome for desktop gradually skip unload events.

In case you need more time to migrate away from unload events, we'll offer temporary opt-outs in the form of a Permissions-Policy API and an enterprise policy ForcePermissionPolicyUnloadDefaultEnabled, which will allow you to selectively keep the behavior unchanged.

- Chrome 117 on Chrome OS, Linux, Mac, Windows: Dev Trial
- Chrome 119 on Chrome OS, Linux, Mac, Windows: Introduces ForcePermissionPolicyUnloadDefaultEnabled policy
- **Chrome 121 -131 on Chrome OS, Linux, Mac, Windows:** Deprecation trial (general rollout of deprecation will be limited scope until deprecation trial is ready)

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 will offer users with a quick shortcut to resume that tab. Admins will be able to control this feature using an existing enterprise policy called SyncTypesListDisabled.

- **Chrome 122 on iOS:** Feature launches

Remove support for UserAgentClientHintsGREASEUpdateEnabled

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 122 on Android, ChromeOS, Linux, Mac, Windows:** Policy is deprecated
- Chrome 125 on Android, ChromeOS, Linux, Mac, Windows: Policy is removed

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, Chrome OS, Linux, Mac, Windows:** The change will be implemented.

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 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 policy, WebSQLAccess, 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.
- **Chrome 123: on Chrome OS, LaCrOS, Linux, Mac, Windows:** Starting in Chrome 123, the policy WebSQLAccess, which allows for WebSQL to be available, will no longer be available.

Remove LegacySameSiteCookieBehaviorEnabledForDomainList policy

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, Mac, Windows:** Remove LegacySameSiteCookieBehaviorEnabledForDomainList policy

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.

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

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, Mac, 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, Mac, Windows: Chrome will gradually disabled 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, Mac, Windows:** Remove ExtensionManifestV2Availability policy.

Upcoming ChromeOS changes

ChromeOS Flex End of Device Support

As of the 1st Jan 2024, devices scheduled to end support in 2023 will no longer be supported. Devices include those detailed below, for the full list of devices ending support please review our certified devices list.

- HP Compaq 6005 Pro
- HP Compaq Elite 8100
- Lenovo ThinkCentre M77
- HP ProBook 6550b
- HP 630
- Dell Optiplex 980

The devices will continue to receive ChromeOS Flex updates but these updates will no longer be tested or maintained by the Flex team.

We recommend customers look to upgrade to newer ChromeOS devices to benefit from new features and security improvements.

ChromeOS Flex Bluetooth Migration

ChromeOS Flex will be upgrading to the Floss bluetooth stack in ChromeOS 121. As part of this upgrade the following devices will no longer support bluetooth functionality.

- 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

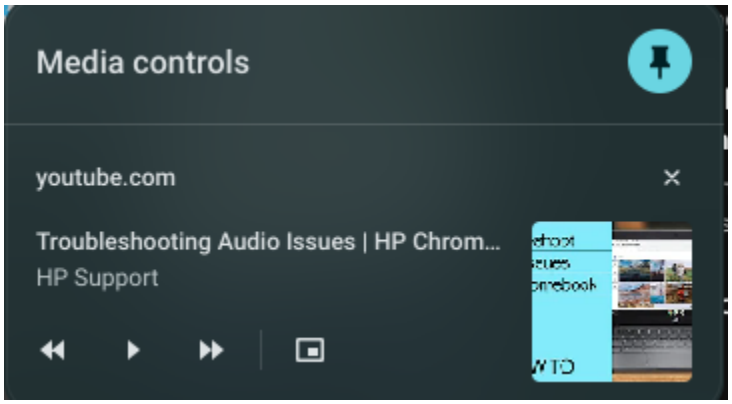
- Lenovo ThinkPad L420

Set the screensaver duration

In ChromeOS 121, you will be able to set the duration for ChromeOS screensaver while charging. Users can choose how long their screensaver runs while their device is charging (not on battery). You will be able to control this using a new enterprise policy. The default setting is *Forever*, and can be reduced using drop-down options.

New look for ChromeOS media player

As early as ChromeOS 121, the media player will have bigger buttons and colors to match your wallpaper. The media player will appear when you are playing any video or audio (like Spotify or YouTube) in Quick Settings. You will be able to click the pin icon to move the media player to the shelf. In addition to controlling media that is being cast, you will be able to start casting web media to any speakers or screens on your local network.



Integrate the DLP events rule Id and name into the security investigation tool

ChromeOS Data Control events will have additional fields to enrich admin insights in the security investigation tool.

Enterprise DataControls (DLP) file restrictions

In ChromeOS 121, ChromeOS Data Controls will enable IT and Security teams to protect important business and customer data. It will be available for events like copy and paste, screen capture, screen sharing, and printing. IT administrators will be able to create an information protection strategy with rules based on the data source, destination and user. We will have new functionality to control what users can do with files on ChromeOS devices through source and destination based rules.

Enhanced notifications for pinned apps

As early as ChromeOS 121, you will be able to visually separate pinned notifications from other notifications. We will change the visual specs, buttons, and notification text to fit within fixed size bubbles. This significantly differentiates the visual look of pinned notifications from typical notifications to reflect their significant difference in purpose (notifying the user of an ongoing process rather than an instantaneous event).

New ChromeOS sync options

ChromeOS will soon deliver an updated device setup experience that lets users customize sync settings for apps, settings, wi-fi networks, and wallpaper.

App disablement by Admin in MGS

Up until now, Managed Guest Sessions (MGS) include a set of applications (Explore, Gallery, and Terminal apps) that are available to the user. With the SystemFeaturesDisableList policy, Admins will soon be able to disable these apps, blocking and hiding them from users across your enterprise.

Upcoming Admin Console changes

Inactive browser deletion in Chrome Browser Cloud Management

As early as Chrome 123, the **Inactive period for browser data deletion policy** will be added to the Admin Console and it will automatically delete browsers that have not contacted the server 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 18 months. All enrolled browsers that have been inactive for more than 18 months will be deleted from your account shortly after the release of this policy. The maximum value to determine the browser inactivity period will be 730 days and the minimum value is 28 days.
Note. Shortening the period significantly will cause more enrolled browsers to be considered inactive and deleted, and should be done with caution. To mitigate this, you can set the Device Token Management policy value to "Delete token" ahead of time, which allows deleted browsers to automatically re-enroll in Chrome Browser Cloud Management the next time the browser restarts (if the enrollment token is still valid). You can find the Device Token Management policy here.

- **As early as Chrome 121:** The Inactive period for browser data deletion policy UI will be 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.

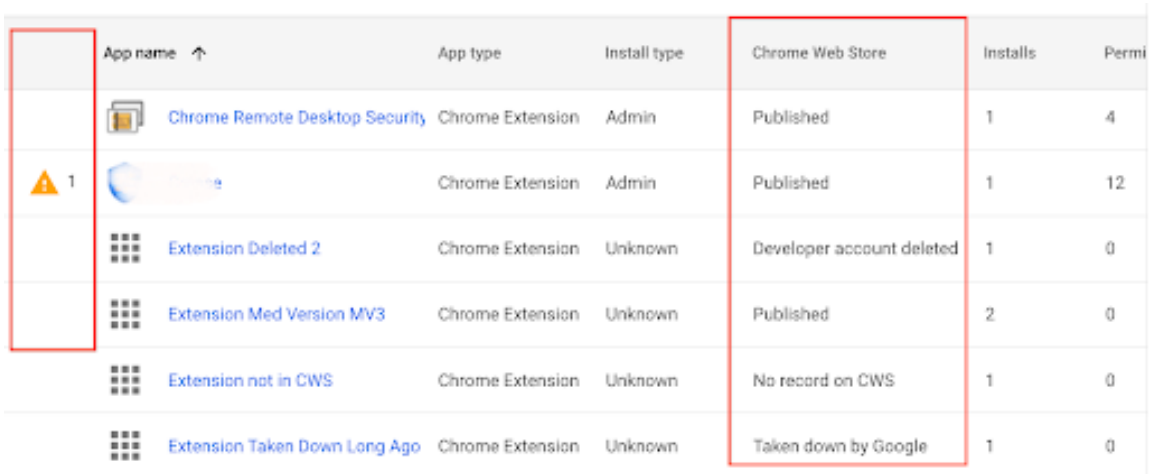
Apps & Extensions usage report: Highlight extensions removed from the Chrome Web Store

As early as 121, Chrome is adding new information on the Apps & Extensions usage report to help you identify if an extension was recently removed from the Chrome Web Store via a new notifications column and a new **Chrome Web Store** column that represents the listing status of an extension. On the **App Details** page, you can find the reason why an extension was removed from the Chrome Web Store. This feature will help IT administrators identify the impact of using the policy to disable unpublished extensions.

This feature is available to test for the members of the Chrome Enterprise Trusted Tester program. You can sign up for our Trusted Tester program here.

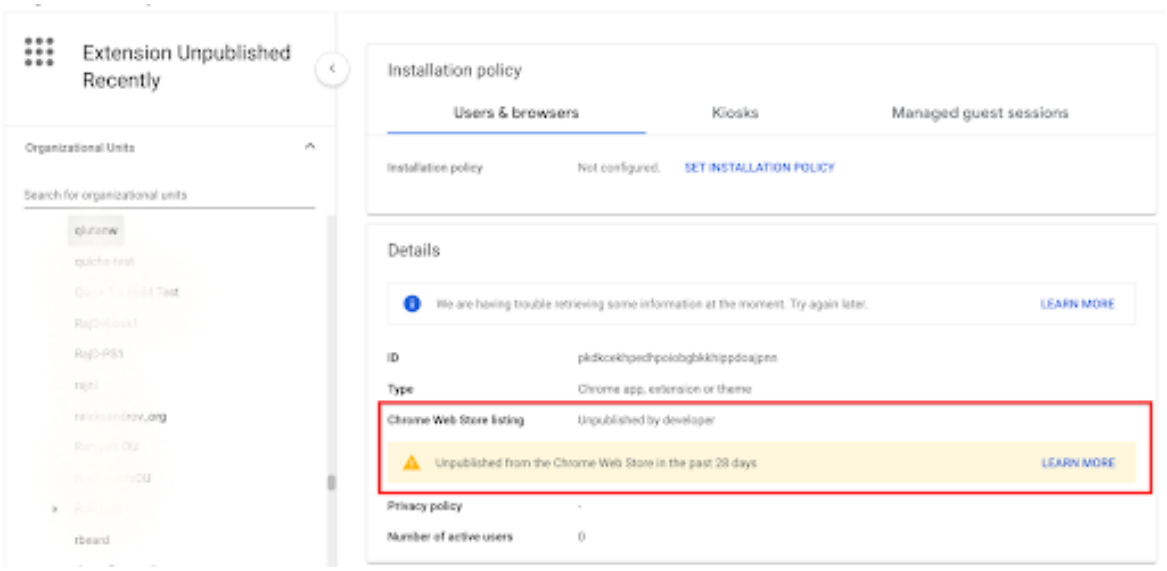
- **Chrome 120 on Linux, Mac, Windows:** Trusted Tester program
- Chrome 121 on Linux, Mac, Windows: Feature rolls out

Apps & Extensions usage report:



	App name	App type	Install type	Chrome Web Store	Installs	Permi
	Chrome Remote Desktop Security	Chrome Extension	Admin	Published	1	4
1	[redacted]	Chrome Extension	Admin	Published	1	12
	Extension Deleted 2	Chrome Extension	Unknown	Developer account deleted	1	0
	Extension Med Version MV3	Chrome Extension	Unknown	Published	2	0
	Extension not in CWS	Chrome Extension	Unknown	No record on CWS	1	0
	Extension Taken Down Long Ago	Chrome Extension	Unknown	Taken down by Google	1	0

App Details page:

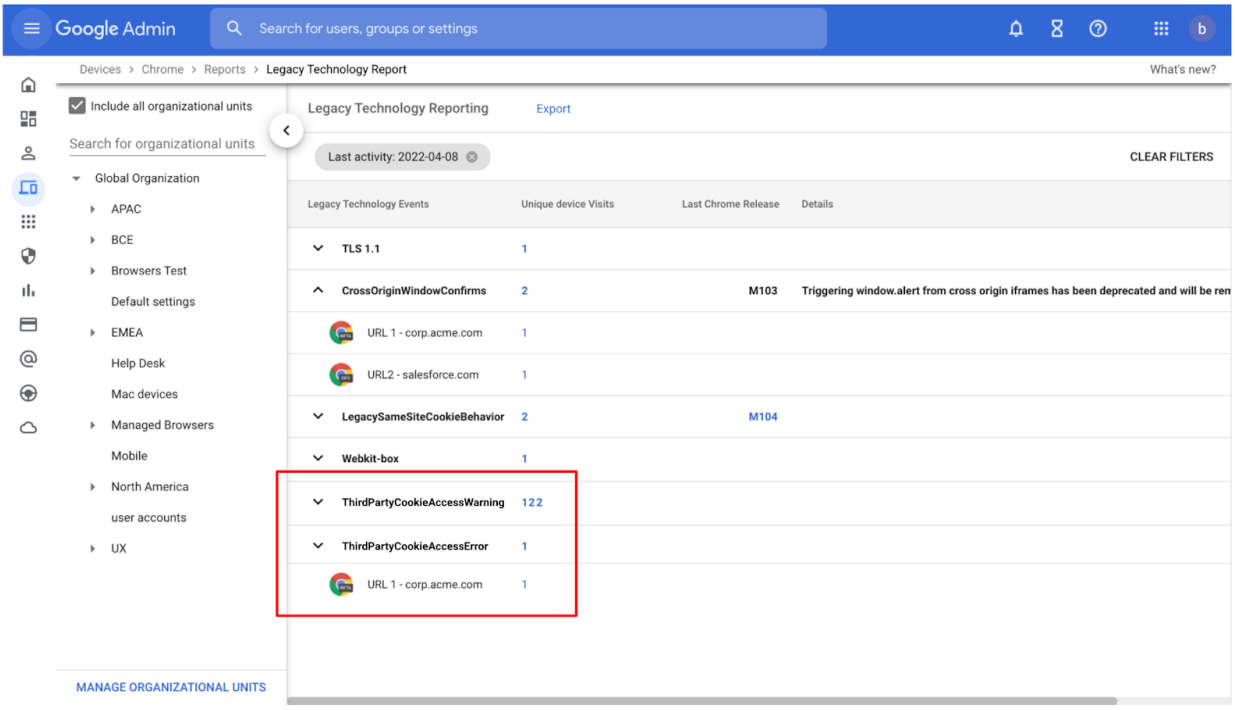


Legacy Technology report

As early as Chrome 121, 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, SameSite cookie changes, 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 goes into effect.

This feature will be released in our Trusted Tester program as early as Chrome 120. 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 121 on Linux, Mac, Windows**

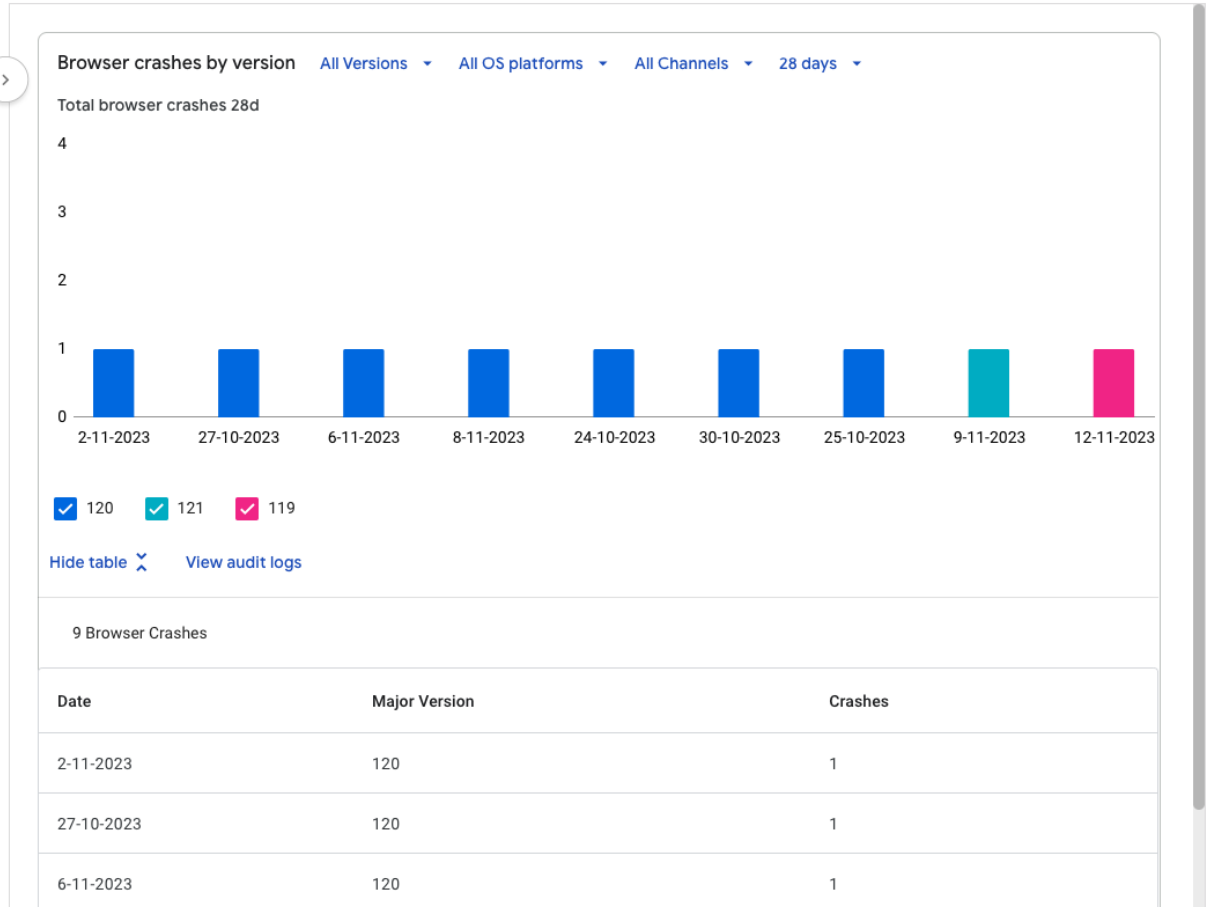


Chrome crash report

As early as Chrome 122, you will be able to 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 will help you proactively identify potential Chrome issues within your organization.

This feature will be released in our Trusted Tester program as early as Chrome 121. If you're interested in helping us test this feature, you can sign up for the Chrome Enterprise Trusted Tester program here.

- **Chrome 121 on Linux, Mac, Windows:** Trusted Tester program
- Chrome 122 on Linux, Mac, Windows: Feature rolls out



Previous release notes

Chrome version & targeted Stable channel release date	PDF
Chrome 119: October 25, 2023	PDF
Chrome 118: October 04, 2023	PDF
Chrome 117: September 08, 2023	PDF
Chrome 116: August 09, 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

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