chrome enterprise

Chrome 119 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 October 25, 2023.

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

Chrome 119 release summary

Chrome Browser updates	Security/Privacy	User productivity/Apps	Management
Chrome release schedule changes			✓
Deprecate and remove WebSQL		✓	
Native Client support updates	✓		
Remove Sanitizer API	✓		
Tab groups can be saved, recalled, and synced		✓	
Deprecate non-standard *shadowroot* attribute for declarative shadow DOM	✓		
Shifting UI strings in Chrome from Clear to Delete when getting rid of data			✓
DevTools internal errors reported to Chrome internal crash reporting			✓
Skip unload events		✓	
SharedImages for PPAPI Video Decode	✓		
Remove Authorization header upon cross-origin redirect	✓		
Dedicated setting for Permission Suggestions Service			✓
Hash-prefix real-time lookups	✓		
Remove recommended support from multiple policies			✓
Standard compliant URL host punctuation characters		✓	
Save images to Google Photos on iOS		✓	

New and updated policies in Chrome browser			✓
Removed policies in Chrome browser			✓
ChromeOS updates	**Security/Privacy**	**User productivity/Apps**	**Management**
Privacy Hub	✓		
ChromeOS Admin templates			✓
Using Drive offline on Chromebook Plus		✓	✓
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**
Default Search Engine choice screen		✓	
Rename FirstPartySets Enterprise Policies to RelatedWebsiteSets	✓		✓
Revamped Safety Check on Desktop	✓		
Chrome Desktop responsive toolbar		✓	
Chrome on Android will no longer support Android Nougat			✓
Chrome Third-Party Cookie Deprecation	✓		
Package tracking (iOS only)		✓	
Network Service on Windows will be sandboxed	✓		
Display banner allowing to resume last tab from other devices		✓	

Resume the last opened tab on any device		✓	
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		✓	✓
Permissions prompt for Web MIDI API	✓		
IP Protection Phase 0 for Chrome	✓		
Apps & Extensions Usage Report: Highlight extensions removed from the Chrome Web Store			✓
Legacy Technology Report			✓
Remove support for UserAgentClientHintsGREASEUpdateEnabled			✓
Chrome Sync ends support for Chrome 81 and earlier			
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**
Set the screensaver duration		✓	

New controls for mouse scroll acceleration		✓	
Enhanced *Alt + click* behavior		✓	
New look for ChromeOS media player		✓	
Enhanced notifications for pinned apps		✓	
New ChromeOS sync options	✓	✓	
App disablement by Admin in MGS			✓

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 release schedule changes

Chrome 119 and all subsequent releases will be moved forward by one week. For example, Chrome 119 has its early stable release on October 25 instead of Nov 1. Beta releases will also be moved forward by one week starting in Chrome 119.

For more details, see the Chrome Release Schedule.

- **Chrome 119 on Android, iOS, ChromeOS, Linux, Mac, 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 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.

Native Client support updates

Chrome 119 removes a temporary enterprise policy, NativeClientForceAllowed, which allowed Native Client to continue to be used.

- Chrome 117 on Linux, Mac, Windows: Removes Native Client NaCl support from extensions on Windows, macOS, Linux.
- **Chrome 119 on Linux, Mac, Windows:** Removes NativeClientForceAllowed policy.

Remove Sanitizer API

To prevent the current Sanitizer API from becoming entrenched, we plan to remove the current implementation. We expect to re-implement the Sanitizer API when the proposed specification stabilizes again.

The Sanitizer API aims to build an easy-to-use, always secure, browser-maintained HTML sanitizer into the platform. We shipped an initial version of the Sanitizer API in Chrome 105, based on the then-current specification draft. However, the standards discussion has meanwhile moved on and the proposed API shape has changed substantially.

- **Chrome 119 on Windows, Mac, Linux, Android**

Tab Groups can be saved, recalled, and synced

Users can now save tab groups, which allows them to close and re-open the tabs in the group, as well as sync them across devices. You can disable syncing Tab Groups using the SyncTypesListDisabled policy.

- **Chrome 119 on ChromeOS, Linux, Mac, Windows**

Deprecate non-standard *shadowroot* attribute for declarative Shadow DOM

The standards-track `shadowrootmode` attribute, which enables declarative Shadow DOM, was shipped in Chrome 111 (ChromeStatus). The older, non-standard `shadowroot` attribute is now deprecated. During the deprecation period, both attributes are functional, however the shadowroot attribute does not enable the new streaming behavior, whereas `shadowrootmode` allows streaming of content. There is a straightforward migration path: replace `shadowroot` with `shadowrootmode`.

The old `shadowroot` attribute is deprecated as of Chrome 112, and it will be removed (no longer supported) in Chrome 119. Chrome 119 goes to Stable on October 31, 2023.

- **Chrome 119 on Windows, Mac, Linux, Android**

Shifting UI strings in Chrome from *Clear* to *Delete* when getting rid of data

Chrome is updating settings text to reflect *delete* instead of *clear* when referring to the destruction of data. We expect this change to improve users' understanding of the associated effect on data. Users who intend to get rid of data should feel reassured that the data is actually *deleted,* not just *cleared* from one view but possibly accessible elsewhere.

- **Chrome 119 on Android, iOS, ChromeOS, Mac, Windows:** The earliest milestone that users may see these changes is 119.

DevTools internal errors reported to Chrome internal crash reporting

To improve Chrome's stability, DevTools internal errors are now reported through Chrome's existing crash reporting pipeline. This provides visibility of the stability of Chrome DevTools. Admins can control all crash reporting, including these errors, using the MetricsReportingEnabled enterprise policy.

- **Chrome 119 on ChromeOS, Linux**

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 120-131 on Chrome OS, Linux, Mac, Windows: Deprecation trial (general rollout of deprecation will be limited scope until deprecation trial is ready)

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.

Remove Authorization header upon cross-origin redirect

The Fetch standard has been updated to remove Authorization header on cross origin redirects. Chrome 119 implements this change to the specification. Prior to Chrome 119, when a cross origin redirect, such as from `foo.test` to `bar.test,` happened with an Authorization header, Chrome preserved the Authorization header and `bar.test` could receive the header. Starting Chrome 119, Chrome removes Authorization headers when cross origin redirects happen, meaning that `bar.test` no longer receives the Authorization header.

- **Chrome 119 on ChromeOS, Windows, Mac, Linux, Android**

Dedicated setting for Permission Suggestions Service

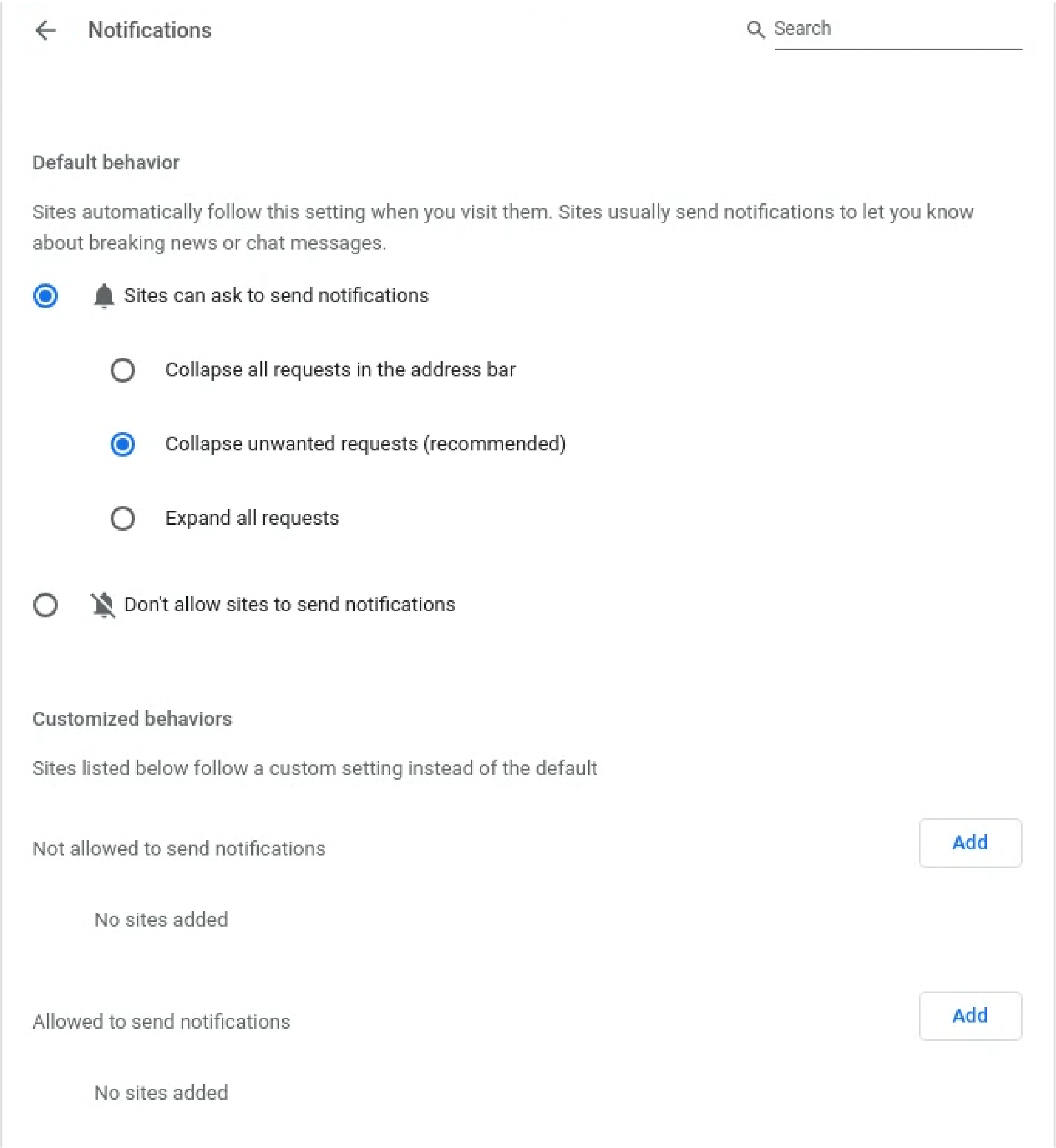
The settings page for notification and geolocation permissions now has an additional option to explicitly enable the Permission Suggestions Service. Permission Suggestions Service is an already existing feature, but it didn't have its dedicated setting. It was tied to Standard Safe Browsing being enabled. Now the users can choose between four different states:

1. Always show the notification/geolocation permission prompt
2. Let Permission Suggestion Service quieten unwanted notification/geolocation requests (new)
3. Always quieten notification permission requests
4. Always block notifications/geolocation permission requests

Admins can use the existing policies to either always allow or always block notifications or geolocation requests globally or for particular sites.

- DefaultNotificationsSetting
- NotificationsAllowedForUrls and NotificationsBlockedForUrls
- DefaultGeolocationSetting

- **Chrome 119 on Linux, Mac, Windows**



← Notifications

Search

Default behavior

Sites automatically follow this setting when you visit them. Sites usually send notifications to let you know about breaking news or chat messages.

● Sites can ask to send notifications

○ Collapse all requests in the address bar

● Collapse unwanted requests (recommended)

○ Expand all requests

○ Don't allow sites to send notifications

Customized behaviors

Sites listed below follow a custom setting instead of the default

Not allowed to send notifications

No sites added

Allowed to send notifications

No sites added

Notification Allowed state (Permission Suggestion Service enabled)

Hash-prefix real-time lookups

For standard Safe Browsing protection users, visited URLs now have their safety checked in real time instead of against a less frequently updated local list of unsafe URLs. This is done by sending partial hashes of the URLs to Google Safe Browsing through a proxy via Oblivious HTTP, so that the user's IP address is not linked to the partial hashes. This change improves security while maintaining privacy for users. If needed, the feature can be disabled through the policy SafeBrowsingProxiedRealTimeChecksAllowed.

- **Chrome 119 on Android, iOS, Chrome OS, LaCrOS, Linux, Mac, Windows**

Remove recommended support from multiple policies

Some policies can be applied as recommended, allowing administrators to set an initial value which end-users can later change. Beginning in Chrome 119, recommended support will be removed from multiple policies which end-users currently have no way of configuring.

Any affected policies that were previously set as recommended will 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

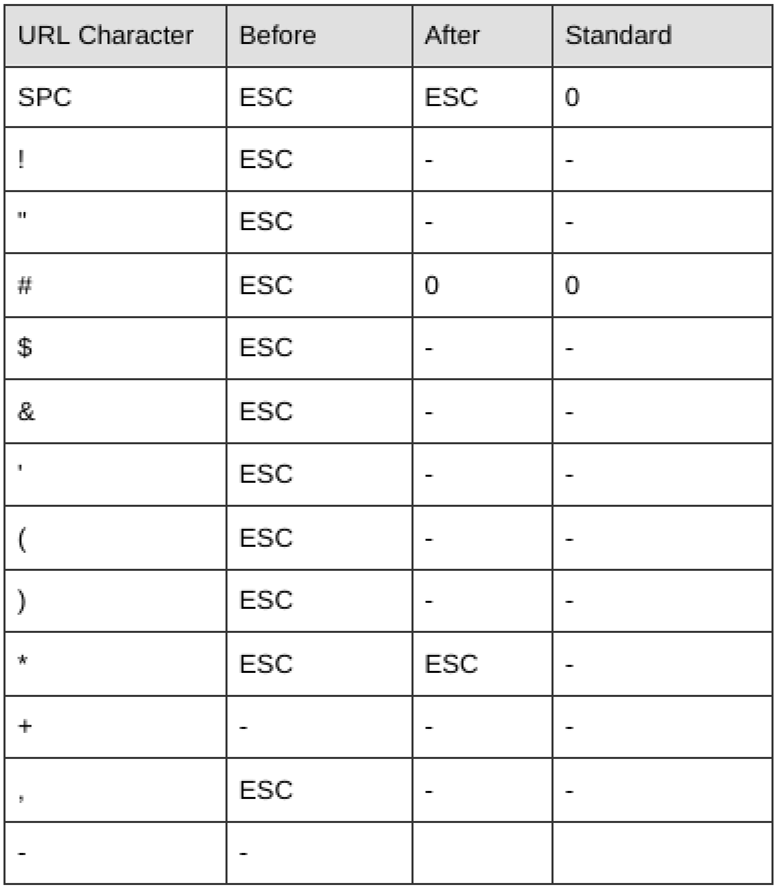
Standard-compliant URL host punctuation characters

Chrome 119 continues our efforts to make Chrome's handling of URL host punctuation characters standard-compliant. Here is a summary of changes in Chrome 119:

Notation:

- 'ESC': Allowed, but Chrome escapes it, which is non-compliant.
- '-': Allowed.
- '0': Forbidden. URL will be invalid if the host contains a forbidden character.

Warning: SPACE and ASTERISK are still non-compliant.



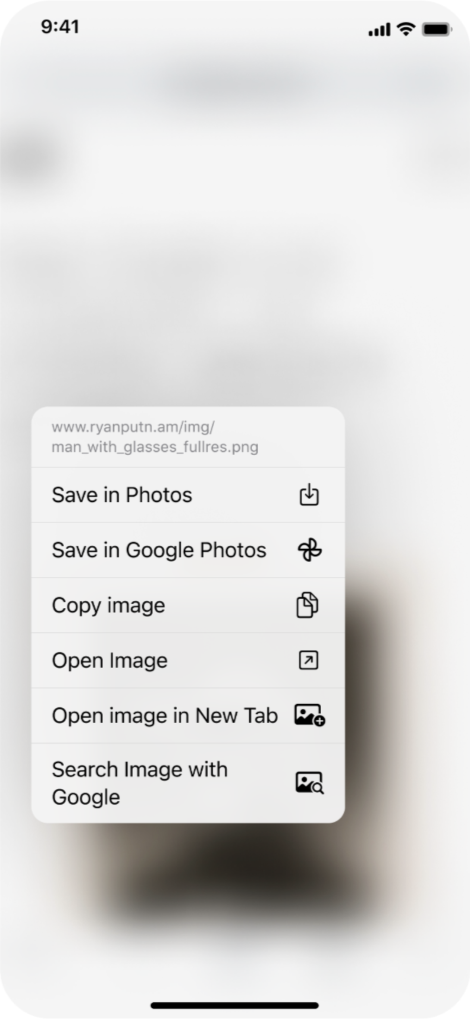
URL Character	Before	After	Standard
SPC	ESC	ESC	0
!	ESC	-	-
"	ESC	-	-
#	ESC	0	0
$	ESC	-	-
&	ESC	-	-
'	ESC	-	-
(	ESC	-	-
)	ESC	-	-
*	ESC	ESC	-
+	-	-	-
,	ESC	-	-
-	-		

- **Chrome 119 on Windows, Mac, Linux, Android**

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.

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



New and updated policies in Chrome browser

Policy	Description
SafeBrowsingDeepScanningEnabled	Allow download deep scanning for Safe Browsing-enabled users
SafeBrowsingProxiedRealTimeChecksAllowed	Allow Safe Browsing Proxied Real Time Checks (now also available on Android)

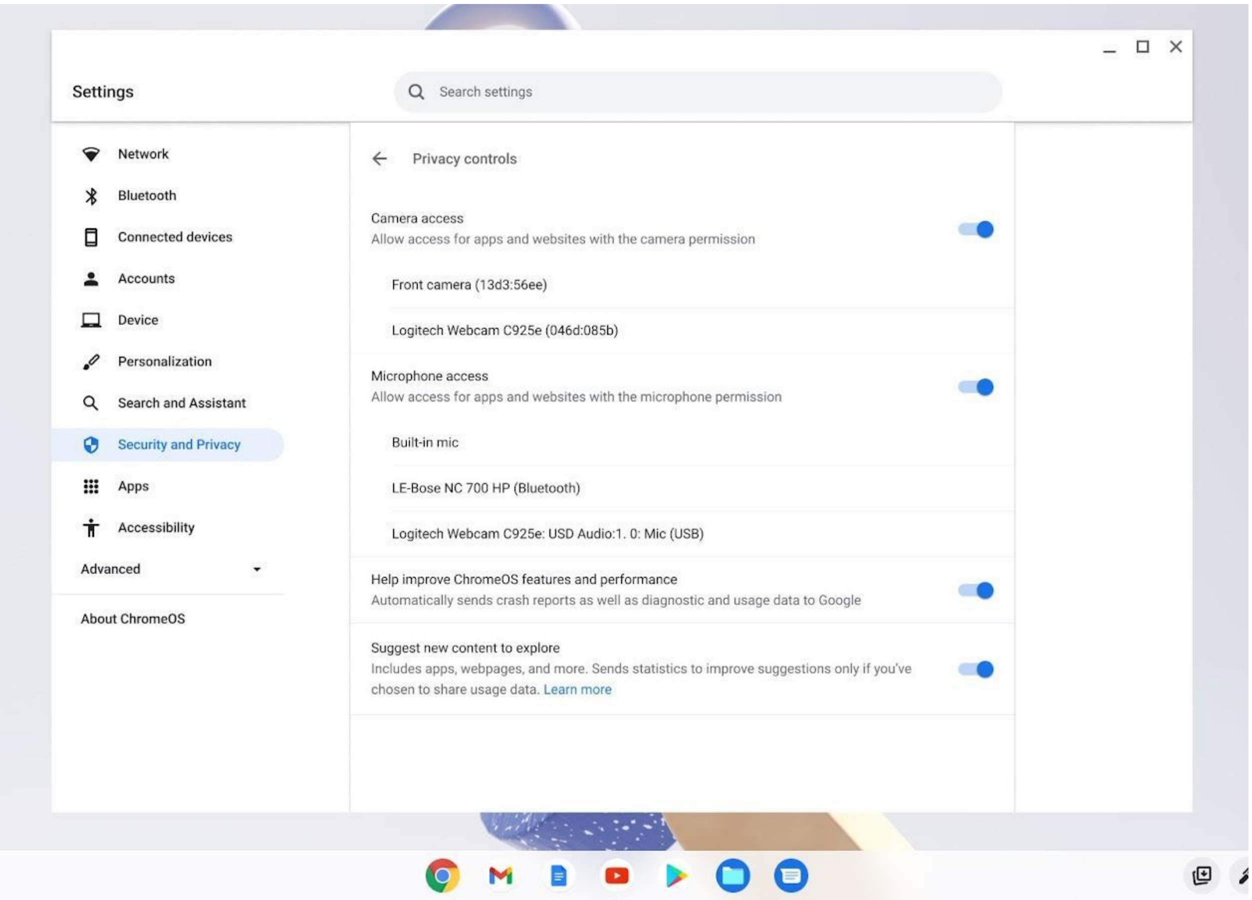
Removed policies in Chrome browser

Policy	Description
ChromeCleanupEnabled	Enable Chrome Cleanup on Windows
DownloadBubbleEnabled	Enable download bubble UI
ChromeCleanupReportingEnabled	Control how Chrome Cleanup reports data to Google

ChromeOS updates

Privacy Hub

Users can now manage their camera and microphone settings across the operating system from one place in **Settings>Security and Privacy>Privacy controls**. Now it only takes one click for users to completely turn off their camera or microphone all from one place when they need extra confidence in staying on mute.



Settings

Search settings

- Network
- Bluetooth
- Connected devices
- Accounts
- Device
- Personalization
- Search and Assistant
- Security and Privacy
- Apps
- Accessibility
- Advanced
- About ChromeOS

← Privacy controls

Camera access
Allow access for apps and websites with the camera permission

Front camera (13d3:56ee)

Logitech Webcam C925e (046d:085b)

Microphone access
Allow access for apps and websites with the microphone permission

Built-in mic

LE-Bose NC 700 HP (Bluetooth)

Logitech Webcam C925e: USD Audio:1. 0: Mic (USB)

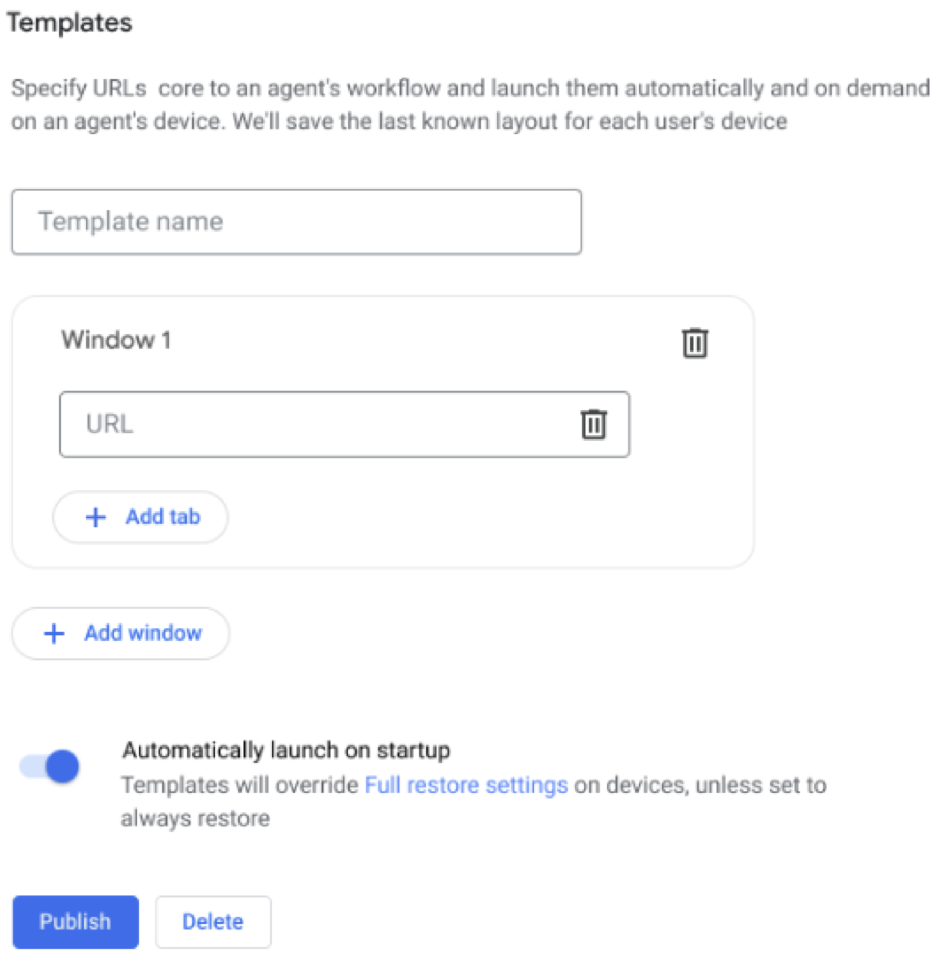
Help improve ChromeOS features and performance
Automatically sends crash reports as well as diagnostic and usage data to Google

Suggest new content to explore
Includes apps, webpages, and more. Sends statistics to improve suggestions only if you've chosen to share usage data. Learn more

ChromeOS Admin templates

With App Launch Automation, admins can now configure groups of applications, windows and tools that can be launched automatically on startup or on-demand by users throughout their day. With App Launch Automation, you can get users up and running quickly at the start of their day, provide users with a way to easily get to an optimal starting point for new tasks, and remember the window layout each user sets up for their individual workflows for future use.

You can turn on this feature using the `#app-launch-automation` flag, and then create templates in the Admin console.



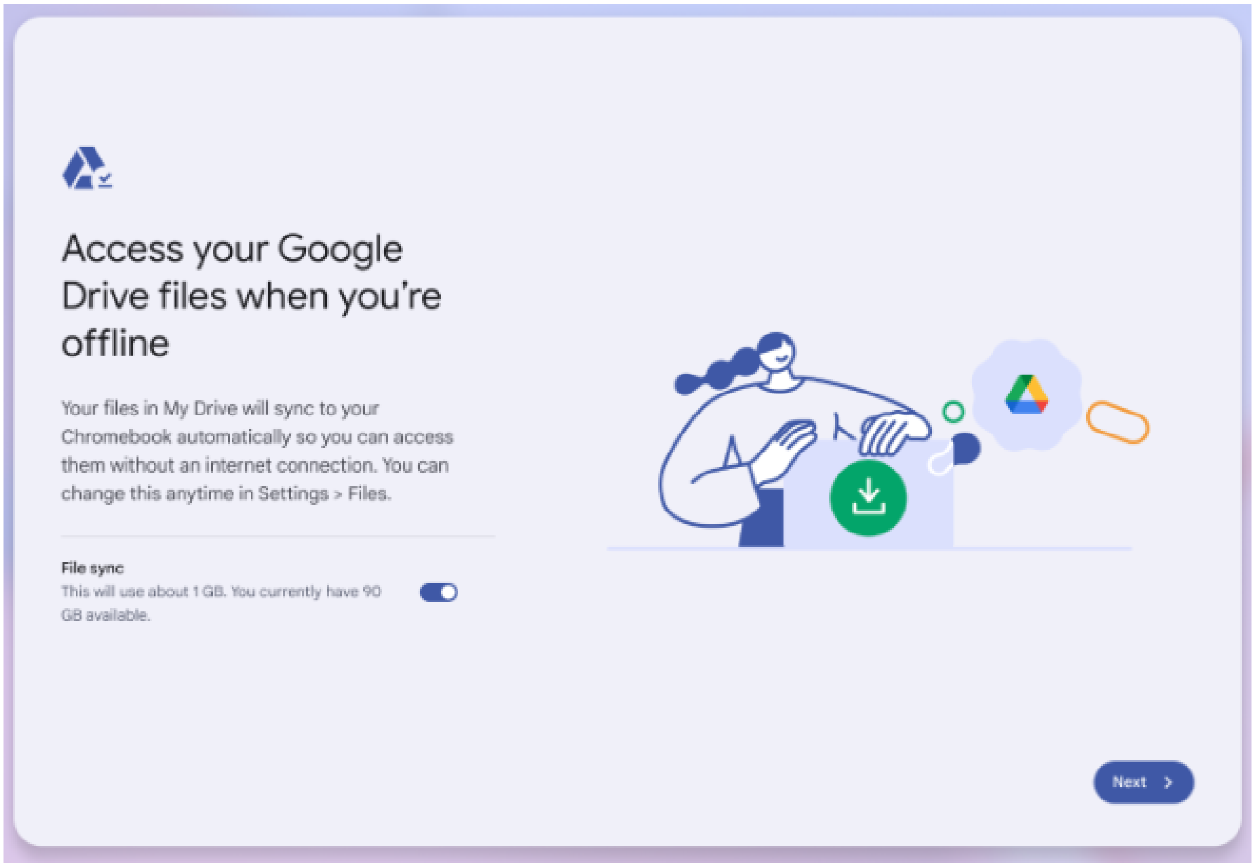
Templates

Specify URLs core to an agent's workflow and launch them automatically and on demand on an agent's device. We'll save the last known layout for each user's device

Automatically launch on startup
Templates will override Full restore settings on devices, unless set to always restore

Using Drive offline on Chromebook Plus devices

Enterprise users on Chromebook Plus devices can now easily make all of their files in the **My Drive** section of Google Drive available offline. You can control this using the DriveFileSyncAvailable enterprise policy.



Access your Google Drive files when you're offline

Your files in My Drive will sync to your Chromebook automatically so you can access them without an internet connection. You can change this anytime in Settings > Files.

File sync

This will use about 1 GB. You currently have 90 GB available.

Admin console updates

New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
PPAPISharedImagesForVideoDecoderAllowed	User & Browser, MGS	ChromeOS	Content
SafeBrowsingDeepScanningEnabled	User & Browser	Chrome(Linux, Mac, Windows), chromeOS	Chrome Safe Browsing

DriveFileSyncAvailable	User & Browser	ChromeOS	Content
ProfileSeparationDataMigrationSettings	User & Browser	Chrome(Linux, Mac, Windows)	Sign-In Settings
ProfileSeparationDomainExceptionList	User & Browser	Chrome(Linux, Mac, Windows)	Sign-In Settings
ProfileSeparationSettings	User & Browser	Chrome(Linux, Mac, Windows)	Sign-In Settings
ShowDisplaySizeScreenEnabled	User & Browser	ChromeOS	Sign-In Settings
ShowTouchpadScrollScreenEnabled	User & Browser	ChromeOS	Sign-In Settings
DeviceEphemeralNetworkPoliciesEnabled	Device	ChromeOS	Other Settings

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 early as 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 will start getting the choice screen with Chrome 120. 100% by Chrome 122.

Rename FirstPartySets Enterprise Policies to RelatedWebsiteSets

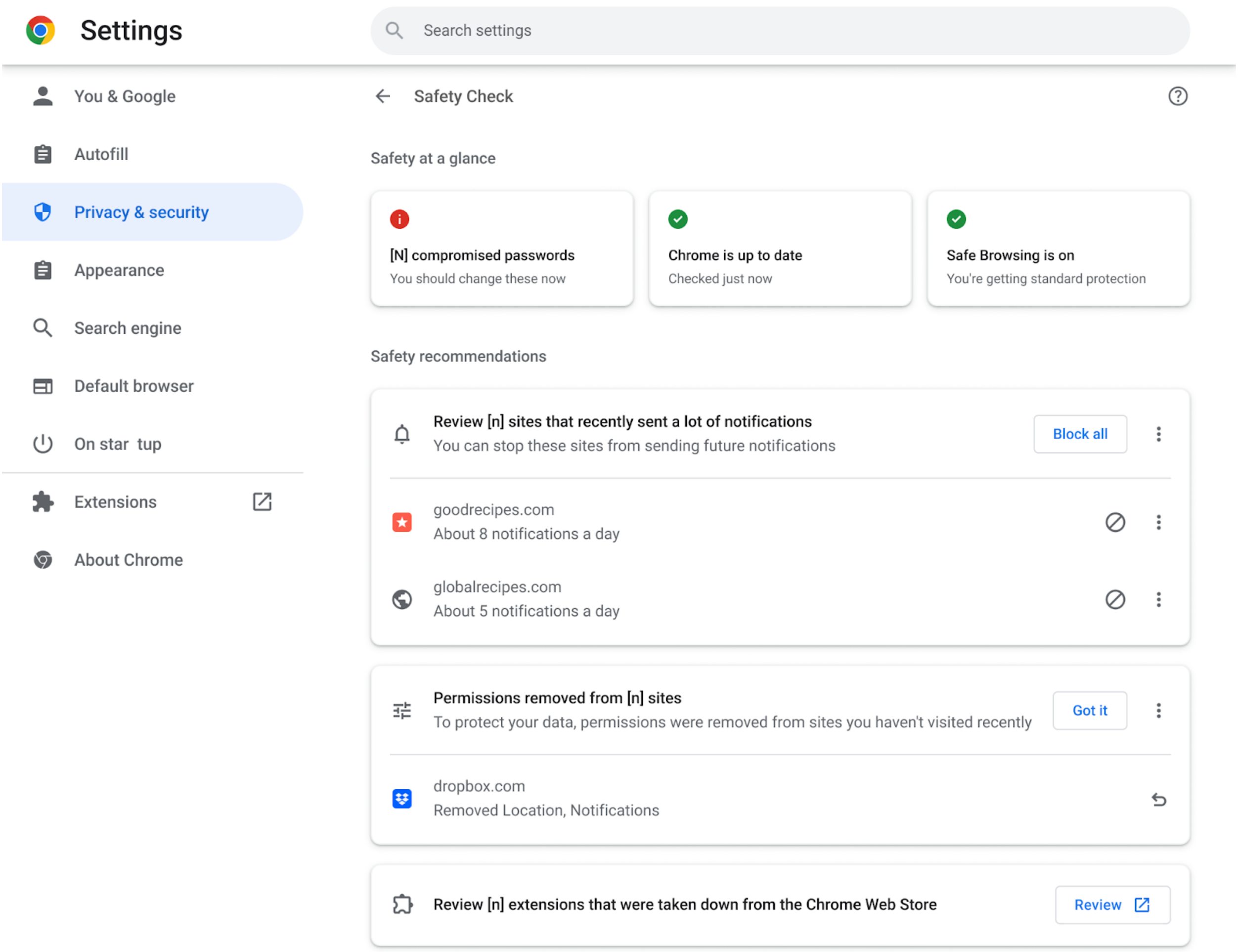
The FirstPartySetsEnabled and FirstPartySetsOverrides enterprise policies are renamed to **RelatedWebsiteSetsEnabled** and **RelatedWebsiteSetsOverrides** respectively. There is no change in the policies' behavior. The new policies become available from Chrome 120. Administrators should use them going 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**

Revamped Safety Check on Desktop

We plan to introduce 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**



Safety at a glance

[N] compromised passwords
You should change these now

Chrome is up to date
Checked just now

Safe Browsing is on
You're getting standard protection

Safety recommendations

Review [n] sites that recently sent a lot of notifications
You can stop these sites from sending future notifications

goodrecipes.com
About 8 notifications a day

globalrecipes.com
About 5 notifications a day

Permissions removed from [n] sites
To protect your data, permissions were removed from sites you haven't visited recently

dropbox.com
Removed Location, Notifications

Review [n] extensions that were taken down from the Chrome Web Store

Chrome Desktop responsive toolbar

As early as Chrome 120, Chrome Desktop customers across devices and input modes (for example, Mouse or Touch) will experience a toolbar that seamlessly responds to changing window sizes, when users manually select and resize a window or use OS-specific window management tools.

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

Chrome on Android will no longer support 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 will not support nor ship to users running Android Nougat.

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

Chrome Third-Party Cookie Deprecation

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. This will allow sites to meaningfully preview what it's like to operate in a world without third-party cookies. Most enterprise users will be excluded from this experiment group automatically. But for the few that might be affected, admins will be able to 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 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.

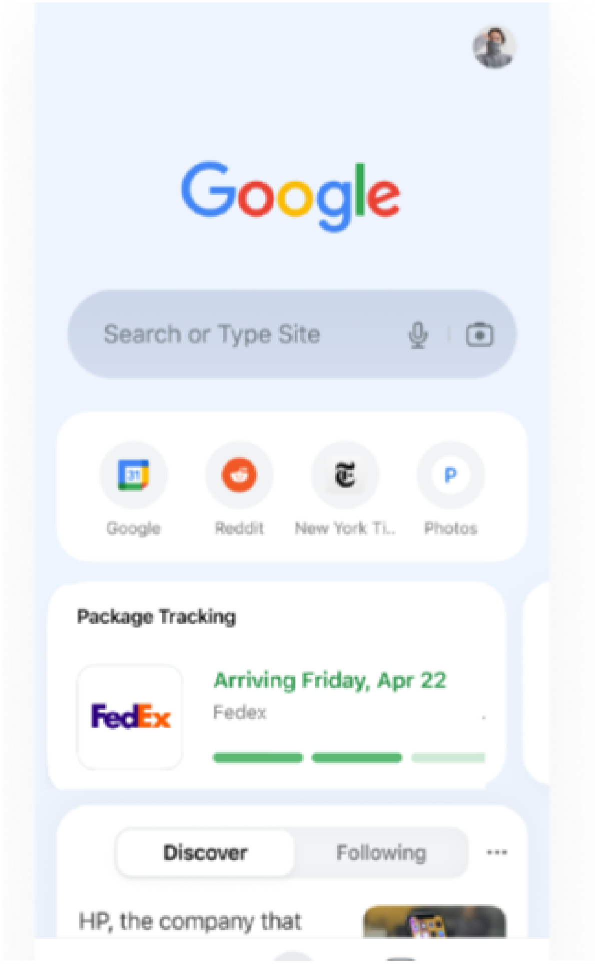
For more details on how to prepare, provide feedback and report potential site issues, refer to the *Mode B: 1% third-party cookie deprecation* blog section and the Preparing for the end of third-party cookies blog.

- **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.

Package tracking (iOS only)

Users will be able to 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 will be able to turn off the feature using a new policy called **ParcelTrackingEnabled**.

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



Network Service on Windows will be sandboxed

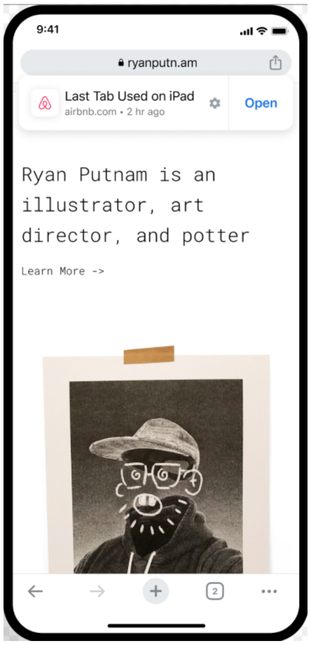
To improve security and reliability, the network service, already running in its own process, will be sandboxed on Windows. As part of this, third-party code that is currently able to tamper with the network service may be prevented from doing so. This might cause interoperability issues with software 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 120 on Windows:** Network Service sandboxed on Windows

Display banner allowing to resume last tab from other devices

To help signed-in users resume tasks when they have to switch devices immediately, Chrome will offer to pick up tabs recently used on the previous device. Admins will be able to control this feature using an existing enterprise policy called SyncTypesListDisabled.

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



Last Tab Used on iPad
airbnb.com • 2 hr ago

Ryan Putnam is an illustrator, art director, and potter

Learn More ->

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 120 on iOS:** Feature launches

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

Chrome will allow the use of the unprefixed version for `background-clip: text` and will make `-webkit-background-clip` an alias for `background-clip`. Also, it drops support for non-suffixed keywords (`content`, `padding` and `border`) for better round-trip with alias.

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

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. This functionality already exists on Windows, Mac, Linux, ChromeOS and Android. We are in the process of bringing this functionality to iOS.

- **Chrome 120 on iOS:** The earliest milestone for this capability is 120.

Chrome profile separation: new policies

Three new policies will be created to help enterprises configure enterprise profiles: **ProfileSeparationSettings**, **ProfileSeparationDataMigrationSettings**, **ProfileSeparationSecondaryDomainAllowlist**. These policies will be simpler to use and will replace 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`. You can read more in this blog post.

Assigning a data: URL in `SVGUseElement` can cause XSS. And this also led to a 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.
Enterprise admins can use the **PasswordSharingEnabled** policy to switch off the share feature for all their employees.

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

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 the advanced MIDI usage, for example, system exclusive (SysEx) message 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**

IP Protection Phase 0 for Chrome

As early as Chrome 122, Chrome might route traffic for some network requests to Google-owned resources through a privacy proxy. This is an early milestone in a larger effort to protect users' identities by masking their IP address from known cross-site trackers. More information is available in this explainer on GitHub. Enterprise policies will be in place to allow admins to turn off the feature before it’s launched.

- **Chrome 122 on ChromeOS, Linux, Mac, Windows, Android**

Apps & Extensions Usage Report: Highlight extensions removed from the Chrome Web Store

As early as 122, 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. 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.

- **Chrome 122 on LaCrOS, Linux, Mac, Windows**

Legacy Technology Report

As early as Chrome 122, 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 e.g. SameSite cookie changes, or older security protocols like TLS 1.1/1.1. This gives admins the ability to work with developers to plan required tech migrations before the deprecation goes into effect. If you're interested in helping us test this feature, you can sign up for our Trusted Tester program here.

- **Chrome 122 on LaCrOS, Linux, Mac, Windows**

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.

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

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. As mentioned earlier in our blog post , the Manifest V2 deprecation timelines are under review and the experiments scheduled for early 2023 are being postponed. During the timeline review, existing Manifest V2 extensions can still be updated, and still run in Chrome. However, all new extensions submitted to the Chrome Web Store must implement Manifest V3. 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. 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 98 on ChromeOS, LaCrOS, Linux, Mac, Windows: Chrome Web Store stops accepting new Manifest V2 extensions with visibility set to "Public" or "Unlisted". The ability to change Manifest V2 extensions from "Private" to "Public" or "Unlisted" is removed.
- Chrome 103 on ChromeOS, LaCrOS, Linux, Mac, Windows: Chrome Web Store stops accepting new Manifest V2 extensions with visibility set to "Private".
- 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.
- **Future milestone on ChromeOS, LaCrOS, Linux, Mac, Windows:** Remove ExtensionManifestV2Availability policy.

Upcoming ChromeOS changes

Set the screensaver duration

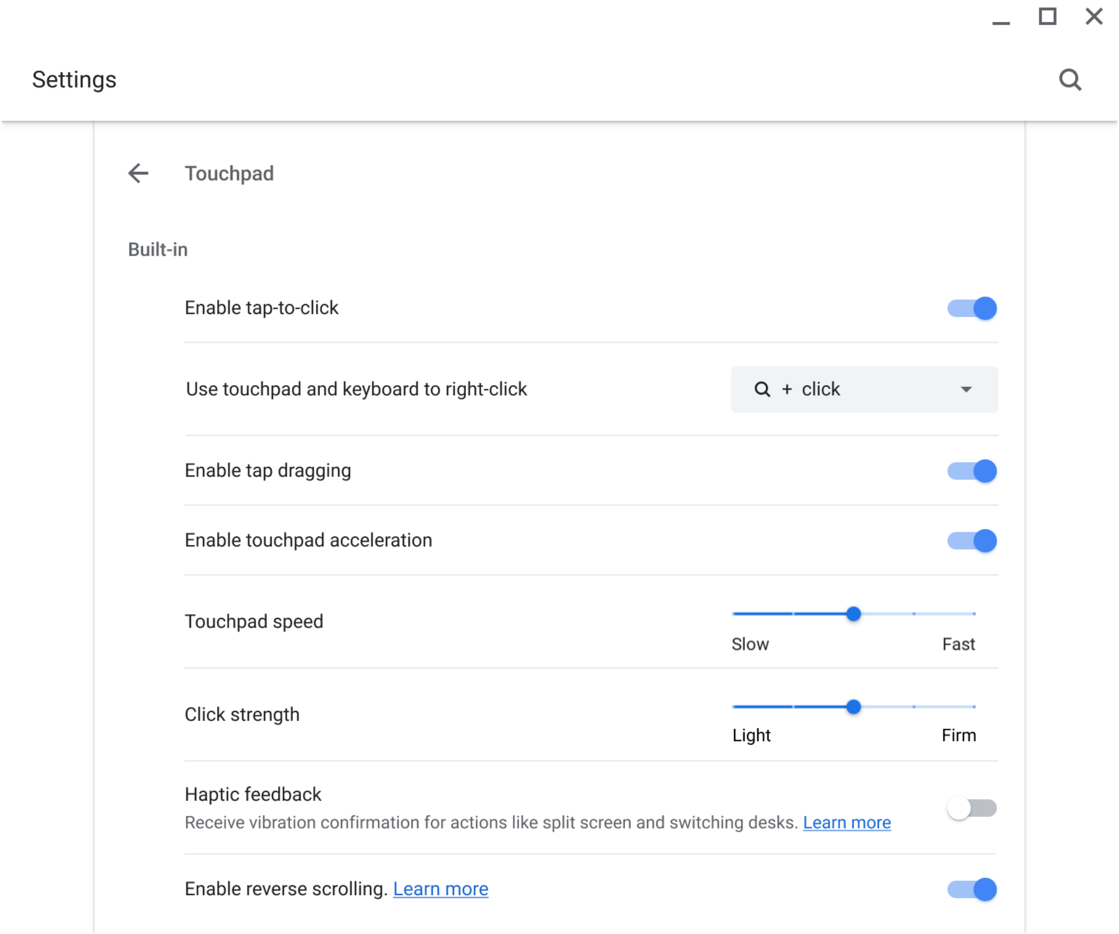
As early as ChromeOS 120, you will be able to set the duration for screensaver while charging. Users can now choose how long their screensaver runs while their device is charging (not on battery). You can control this using a new enterprise policy. The default setting is Forever, and can be reduced using drop-down options.

New controls for mouse scroll acceleration

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

Enhanced *Alt + click* behavior

In ChromeOS 120, you will be able to 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.



Settings

Touchpad

Built-in

Enable tap-to-click ●

Use touchpad and keyboard to right-click: 🔍 + click

Enable tap dragging ●

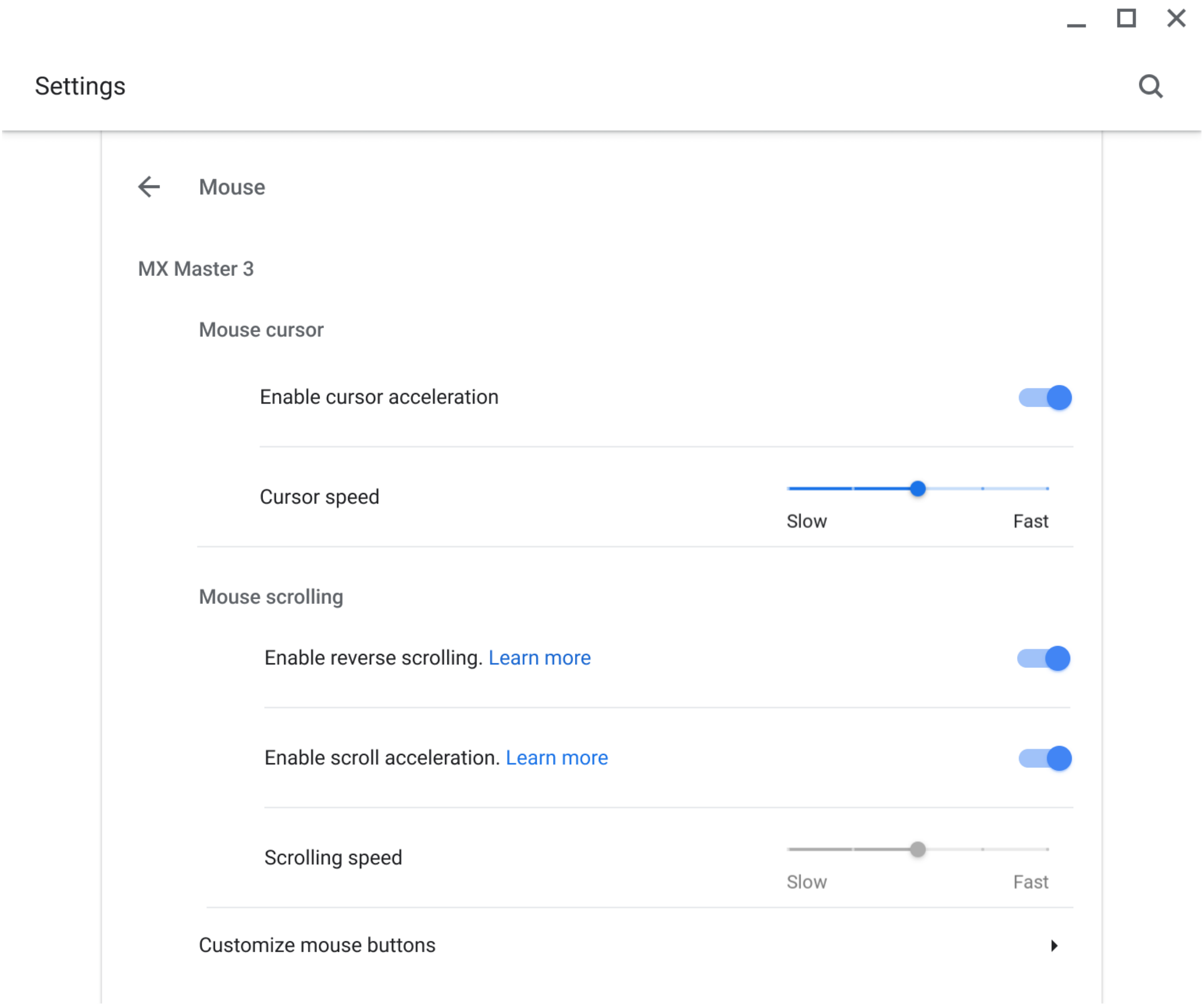
Enable touchpad acceleration ●

Touchpad speed: Slow — Fast

Click strength: Light — Firm

Haptic feedback ○
Receive vibration confirmation for actions like split screen and switching desks. Learn more

Enable reverse scrolling. Learn more ●



Settings

Mouse

MX Master 3

Mouse cursor

Enable cursor acceleration ●

Cursor speed Slow Fast

Mouse scrolling

Enable reverse scrolling. Learn more ●

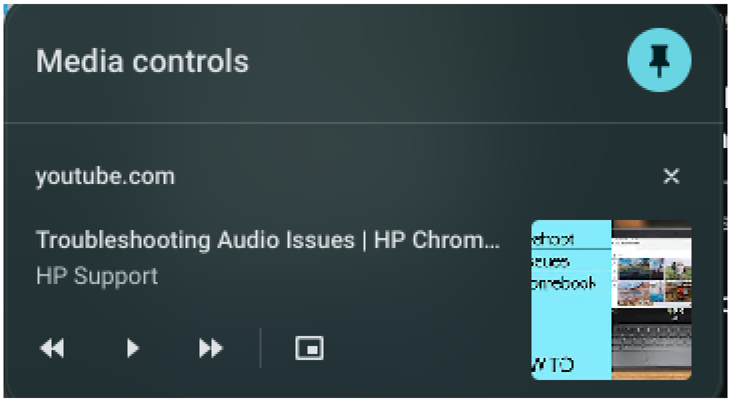
Enable scroll acceleration. Learn more ●

Scrolling speed Slow Fast

Customize mouse buttons

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.



Media controls

youtube.com

Troubleshooting Audio Issues | HP Chrom...

HP Support

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.

Previous release notes

Chrome version & targeted Stable channel release date	PDF
Chrome 118: October 04, 2023	PDF
Chrome 117: September 08, 2023	PDF
Chrome 116: August 09, 2023	PDF
Chrome 115: July 12, 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