Chrome 116 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 August 9, 2023.

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

Chrome 116 release summary

Chrome browser updates	**Security/ Privacy**	**User productivity/ Apps**	**Management**
Enterprises can sign up for security fix notifications	✓		
Chrome increases release velocity with security improvements planned for each week	✓		
Share Sheet migration		✓	
Google Search side panel		✓	
X25519Kyber768 key encapsulation for TLS	✓		
Improving performance: Memory Saver and Energy Saver modes		✓	✓
Anti-phishing telemetry expansion	✓		
Enabling BFCache for pages that set Cache-Control: no-store			✓
Idle Timeout policies on Desktop			✓
OS-native Passkey changes on Windows 11	✓		
New and updated policies in Chrome browser			✓
Removed policies in Chrome browser			✓
ChromeOS updates	**Security/ Privacy**	**User productivity/Apps**	**Management**
Data processor mode on ChromeOS (including Chrome browser running on managed ChromeOS)	✓		
Removal of permissive Chrome Apps webview behaviors	✓		

ChromeOS OCR in PDFs for screen reader users		✓	
Move ChromeVox settings pages to ChromeOS settings		✓	
Customizing input peripherals per device settings		✓	
Managing Android App permissions			✓
ChromeOS Kerberos integration enhancements			✓
Commercial launch of screensaver		✓	
Enhanced autocorrect features		✓	
Additional input method support for Linux apps			✓
URL-keyed anonymized data collection in Kiosk mode			✓
Admin console updates	**Security/ Privacy**	**User productivity/Apps**	**Management**
New and updated policies			✓
Upcoming Chrome browser changes	**Security/ Privacy**	**User productivity/Apps**	**Management**
Extensions Review panel			✓
Native Client Support updates		✓	
Updates to Clear Browsing Data on Android	✓		
Skip unload events		✓	
Require X.509 key usage extension for RSA certificates chaining to local roots	✓		
Network service will be sandboxed on Linux and ChromeOS	✓		

Bounce Tracking mitigations	✓		
Restricting the use of --load-extension	✓		
Service Worker static routing API		✓	
Enable access to WebUSB API from extension service workers		✓	
Simplified sign-in and sync experience		✓	
IP Protection Phase 0 for Chrome	✓		
Web MIDI permission prompt	✓		
Removal of the RendererCodeIntegrityEnabled policy			✓
Chrome 117 will no longer support macOS 10.13 and macOS 10.14			✓
New Chrome Desktop visual refresh in Chrome 117		✓	
Update to the lock icon	✓		
Storage Access API with Prompts		✓	
Extensions must be updated to leverage Manifest V3	✓	✓	✓
Removal ForceMajorVersionToMinorPositionInUserAgent policy			✓
Third party cookie deprecation trial	✓		
Chrome release schedule changes			✓
Chrome 119 to phase out support for Web SQL		✓	
Migrate away from data URLs in SVG <use> element	✓	✓	
Chrome Profile Separation		✓	✓

Removal LegacySameSiteCookieBehaviorEnabledForDomainList policy			✓
Intent to deprecate: Mutation Events		✓	
Upcoming ChromeOS changes	**Security/ Privacy**	**User productivity/Apps**	**Management**
ChromeOS battery state sounds			✓

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

Enterprises can sign up for security fix notifications

Using this sign-up form, you can opt-in to receive email notifications whenever there's a Chrome release that contains high or critical security fixes, including zero-day fixes. Chrome uses a fast release cycle to keep you ahead of bad actors, and so you can expect such a release approximately every week. By default, Chrome applies updates automatically when they're made available, so no action is required from admins who keep Chrome's default update behavior. You can read more about Chrome updates strategies for enterprises here.

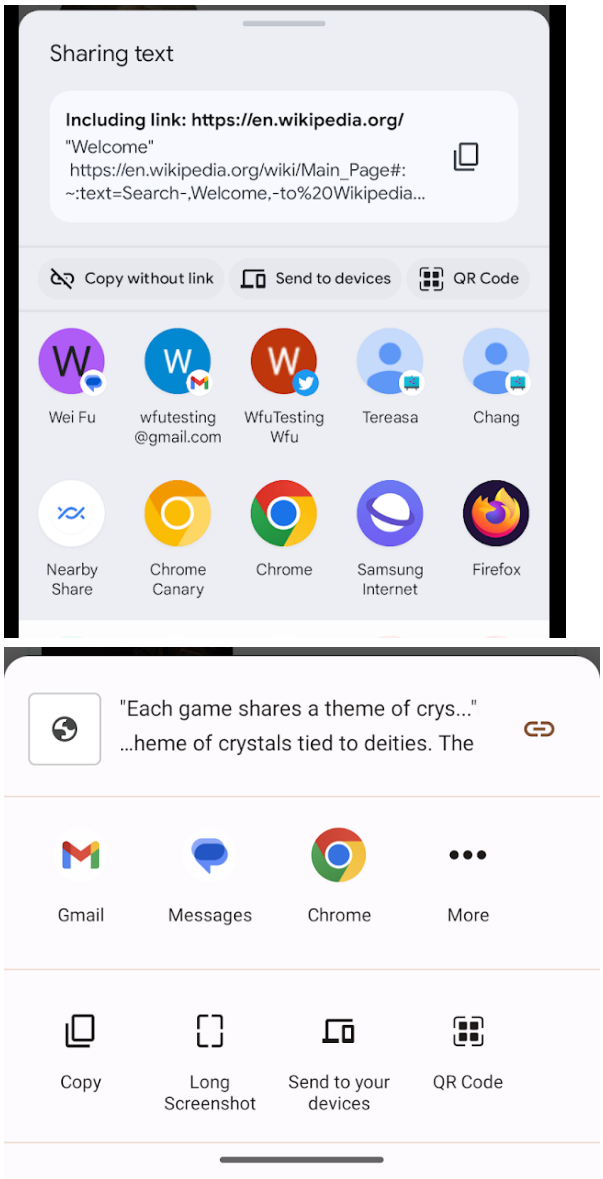
Chrome increases release velocity with security improvements planned for each week

In Chrome 115 and previous releases, Chrome maintained a four-week release cycle with a minor release halfway between each major release containing security improvements and minor bug fixes.

Major releases continue to be planned for approximately every four weeks, but starting in Chrome 116, minor releases are now planned every week. This allows us to deliver security improvements even faster. If you have auto-updates turned on (the default behavior of Chrome, and our recommendation), then no action is required.

Chrome might still release some unplanned updates in response to critical fixes, zero-day fixes, or other unforeseen circumstances. If you want to be notified of the security fixes contained in each release of Chrome, you can sign up for notifications here. Read more about Chrome Security and why we're making this change in our blog post.

Share Sheet migration



Chrome is migrating Share functionality from its custom share sheet to the Android system share sheet for Android U+ users. In this migration, we've deprecated some functionality such as stylized cards for shared highlights and a redundant button for short (non full-page) screenshots. On Pre-U Android, Chrome still shows the custom share sheet and users can navigate to the system share sheet using the **More (...)** button.

Google Search side panel

Chrome is introducing the Search side panel, a new contextual side panel experience that allows users to delve into the content of the page they're currently viewing. The new side panel gives users new tools to get more context about the page they're viewing. We launched the Search side panel to some users in Chrome 115 and subsequently plan to roll out to all users in Chrome 116. You can control access to the Search side panel using the GoogleSearchSidePanelEnabled policy.

X25519Kyber768 key encapsulation for TLS

As early as Chrome 116, Chrome introduces a post-quantum secure TLS key encapsulation mechanism X25519Kyber768, based on a NIST standard. This is exposed as a new TLS cipher suite. TLS automatically negotiates supported ciphers, so this change should be transparent to server operators. However, some TLS middleboxes might be unprepared for the size of a Kyber key encapsulation, or a new TLS ClientHello cipher code point, leading to dropped or hanging connections. This can be resolved by updating your middlebox, or disabling the key encapsulation mechanism via the temporary PostQuantumKeyAgreementEnabled enterprise policy. However, long term, post-quantum secure ciphers will be required in TLS and the enterprise policy will be removed. This cipher will be used for both TLS and QUIC connections.

Improving performance: Memory Saver and Energy Saver modes

In Chrome 108, we introduced features designed to improve the performance of Chrome and extend battery life under the following enterprise policies: TabDiscardingExceptions, BatterySaverModeAvailability and HighEfficiencyModeEnabled. In Chrome 116, we expand the capabilities of the Memory Saver feature to help users further understand and use tab discarding to their benefit.

Users with Memory Saver enabled (policy HighEfficiencyModeEnabled) now have increased visibility of discarded tabs in the tab strip and more insight into memory usage of active and inactive tabs.

Additionally, this release makes the management of exceptions (policy TabDiscardingExceptions) more intuitive for users who have access to manage their own exceptions:

1. In settings, users can add exceptions based on currently open tabs (in addition to manual entry which exists today)

2. In the page action chip of a discarded tab, users can opt the site out from future discarding.

Anti-phishing telemetry expansion

In this feature, we log user-interaction data to Chrome servers and to Safe Browsing servers, which will fill knowledge gaps about how users interact with Safe Browsing phishing warnings and phishing pages. This additional telemetry will help inform where we should concentrate our efforts to improve phishing protection because it will allow us to understand the user better. Admins can opt out by using the Enterprise policies MetricsReportingEnabled and SafeBrowsingProtectionLevel.

Enabling BFCache for pages that set Cache-Control: no-store

Documents with a `Cache-Control: no-store` header (CCNS) are blocked from entering BFCache. Chrome 116 will start BFCaching these documents, except for the ones with sensitive information (Github).

The AllowBackForwardCacheForCacheControlNoStorePageEnabled policy controls if a page with `Cache-Control: no-store` header can be stored in back/forward cache. The website setting this header might not expect the page to be restored from back/forward cache since some sensitive information could still be displayed after the restoration even if it is no longer accessible.

If the policy is enabled or unset, the page with `Cache-Control: no-store` header might be restored from back/forward cache unless the cache eviction is triggered, for example, when there is HTTP-only cookie change to the site.

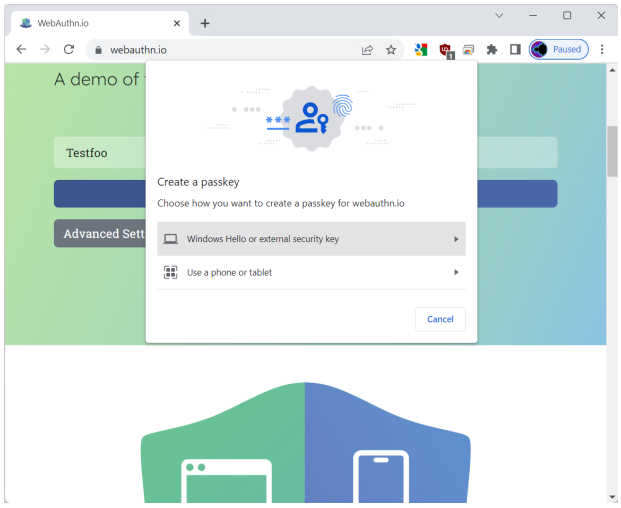
If the policy is disabled, the page with `Cache-Control: no-store` header will not be stored in back/forward cache.

Idle Timeout policies on Desktop

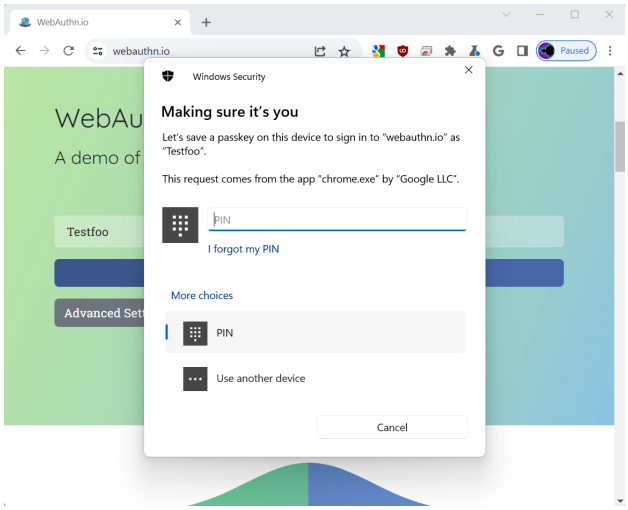
In Chrome 116, admins can now enforce taking an action, for example, closing the browser, clearing cookies or moving to the profile picker, after Chrome has been idle for some amount of time. You can use the IdleTimeout policy to set a timeout period and the IdleTimeoutActions policy to specify actions on timeout.

OS-native Passkey changes on Windows 11

An update to Windows 11 later in 2023 adds support for cross-device passkeys flows in Windows **webauthn.dll v6**. Chrome 116 recognises this version of Windows and stops offering its own cross-device support in Chrome UI, deferring to Windows instead. This results in users seeing a different UI, as shown below. This can be tested with Chrome 116 running on Windows Insider Dev Build 23486 or later.



Before



After

New and updated policies in Chrome browser

Policy	Description
NativeClientForceAllowed	Forces Native Client (NaCl) to be allowed to run.
SafeSitesFilterBehavior	Control SafeSites adult content filtering (now on Android)
PostQuantumKeyAgreementEnabled	Enable post-quantum key agreement for TLS
UserContextAwareAccessSignalsAllowlist	Enable the Chrome Enterprise Device Trust Connector attestation flow for a list of URLs on Managed Profiles
RSAKeyUsageForLocalAnchorsEnabled	Check RSA key usage for server certificates issued by local trust anchors
AllowBackForwardCacheForCacheControlNoStorePageEnabled	Allow pages with Cache-Control: no-store header to enter back/forward cache

Removed policies in Chrome browser

Policy	Description
EventPathEnabled	Re-enable the Event.path API

ChromeOS updates

Data processor mode on ChromeOS (including Chrome browser running on managed ChromeOS)

In ChromeOS 116, ChromeOS is releasing a "data processor mode" for a suite of ChromeOS features and services called "Essential Services", switching Google's role from that of a data controller over personal data, to primarily that of a data processor. Features and services for which Google remains solely a data controller are called "Optional Services." IT admins who manage ChromeOS devices used by managed Dutch Education accounts will see these new terms and features available to select from August 18, 2023.

These are the new tools available in data processor mode for ChromeOS:

- Data processor mode landing page in the Admin console
- The ability to turn-on/off individual Optional Services
- Tools to assist customers with Data Subject Access Requests (DSARs)
- A tool to assist customers with data subject deletion requests

Removal of permissive Chrome Apps webview behaviors

As early as Chrome 116, Chrome Apps webview usage have the following restrictions:

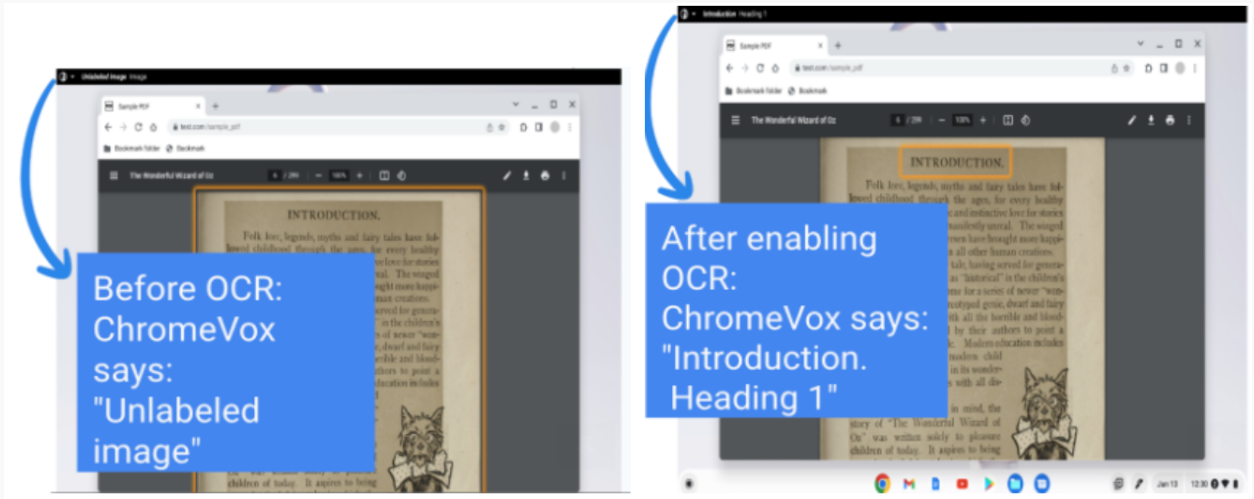
- Using the webview NewWindow event to attach to a webview element in another App window causes the window reference returned by the window.open call in the originating webview to be invalidated.

A temporary enterprise policy ChromeAppsWebViewPermissiveBehaviorAllowed is available to give enterprises time to address possible breakage related to these changes. To test whether this change is the cause of any breakage, without needing to set the enterprise policy, you can restore the previous behavior from Chrome 112 and earlier by navigating to chrome://flags and disabling chrome://flags/#enable-webview-tag-mparch-behavior.

This change was originally scheduled for Chrome 113, but was postponed. Previous release notes mentioned a change to the handling of SSL errors within webviews, but this is no longer part of this change.

ChromeOS OCR in PDFs for screen reader users

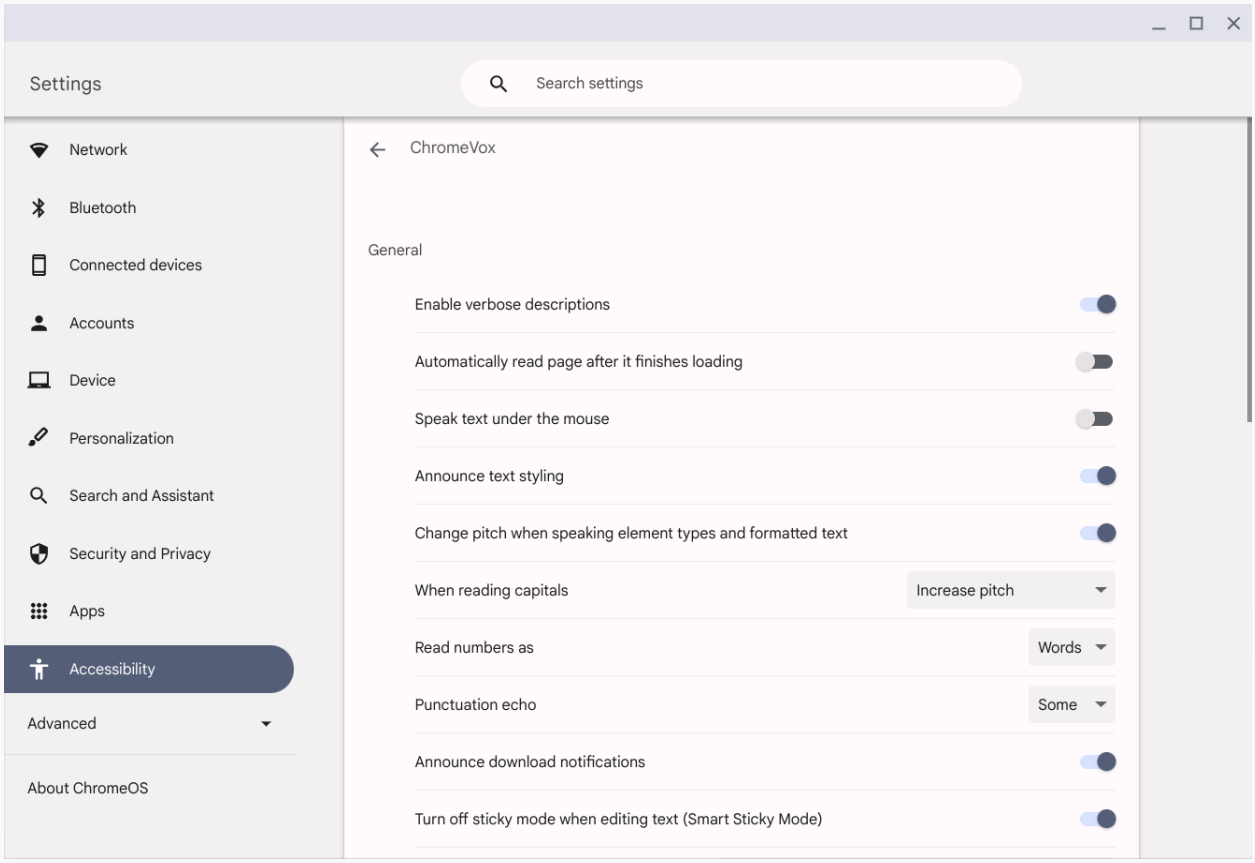
Through Optical Character Recognition (OCR), users can convert images to text, so that they can access and read them.



Left: Pre-OCR where ChromeVox says “Unlabeled Image”; Right: OCR now reads the content in the PDF

ChromeVox settings move to ChromeOS settings

In Chrome 116, you now access the existing settings for ChromeVox under the ChromeOS **Accessibility** settings pages.



Customizing input peripherals per device settings

Users can now manage settings for their input peripherals, such as their mouse and keyboard, at the device level and apply different values for different devices. This provides more control over the peripheral experience on ChromeOS.

Managing Android App permissions

In Chrome 116, users have a better view of what data Android apps can access by reviewing allowed app permissions on the Apps page in ChromeOS **Settings**. Now, users can see a detailed view of the data an Android app can access on the Apps page in **Settings**, and they can easily manage those permissions.

ChromeOS Kerberos integration enhancements

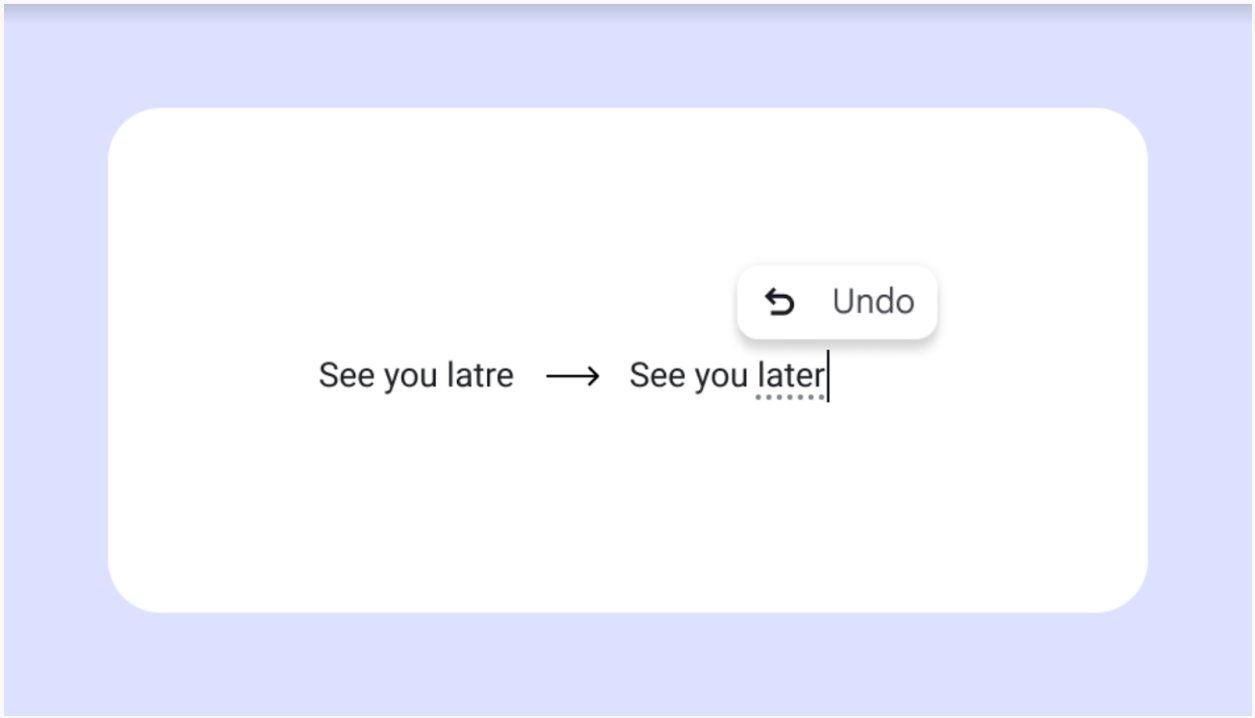
Starting with M116, we streamline the end user configuration flows for ChromeOS Kerberos customers. Many users use Kerberos on ChromeOS to access corporate resources. The new UI enhancements guide users through the configuration of their Kerberos accounts in a guided flow, similar to **Password Manager**. For details, see this help center article.

Commercial launch of screensaver

With M116, ChromeOS represents your organization even better. The commercial launch of screensaver for the login screen or MGS lock screen allows admins to customize the appearance of idle devices. Newly added admin settings include the abilities to turn on/off the screensaver, to provide a list of screensaver images, and to customize idle times.

Enhanced autocorrect features

We've enhanced Autocorrect in ChromeOS! Autocorrect is now enabled by default for English in compatible apps, automatically fixing typos, spelling, and other errors. In addition to the new Autocorrect for physical keyboards, this update also enhances the performance of the virtual keyboard's Autocorrect and other Assistive features.



Additional input method support for Linux apps

Linux on ChromeOS now supports complex input methods, such as Japanese and Korean. This means that you can now use the same input methods that you're already using in Chrome to type in your Linux applications. Not all applications are supported yet, but support for additional applications is coming soon.

URL-keyed anonymized data collection in Kiosk mode

The policy for URL-keyed anonymized data collection is now supported in Kiosk mode. This policy will be added to the Admin console in a future release.

Admin console updates

New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
RSAKeyUsageForLocalAnchorsEnabled	User, MGS	CrOS, Chrome, Android	Legacy Site Compatibility
AllowBackForwardCacheForCacheControlNoStorePageEnabled	User, MGS	CrOS, Chrome, Android	Security
PostQuantumKeyAgreementEnabled	User, MGS	CrOS, Chrome, Android	Security
PhysicalKeyboardPredictiveWriting	User, MGS	CrOS	User Experience
PhysicalKeyboardAutocorrect	User, MGS	CrOS	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

Extensions Review panel

A new review panel will be added in `chrome://extensions`, which will appear whenever there are potentially unsafe extensions that need the user's attention. The initial launch will highlight extensions that are malware, policy violating or are no longer available in the Chrome Web Store. The user can choose to remove or keep these extensions.

There will also be a count of risky extensions needing review that is presented in the Chrome **Privacy & Security** settings page.

The **ExtensionsUnpublishedAvailability** policy will disable extensions that have been unpublished by the developer or violate Chrome Web Store policy. Note that these extensions might also appear in the Extensions Module's review panel but only if they are not installed by policy. The user can choose to remove or keep them.

Native Client Support updates

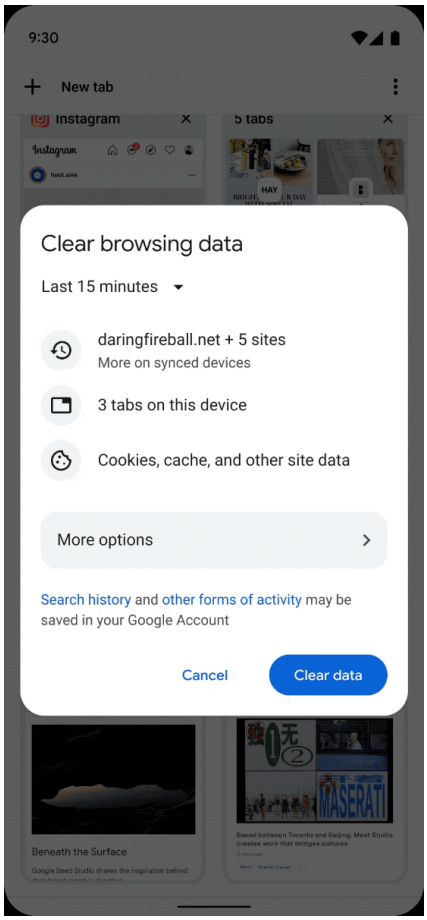
As early as Chrome 117, we will remove Native Client NaCl support from extensions on Windows, macOS, Linux. An enterprise policy will be available, **NativeClientForceAllowed**, which will allow Native Client to continue to be used until Chrome 119.

Updates to Clear Browsing Data on Android

We’re making it easier to find and use the browsing data deletion tools that Chrome offers.

We’re adding more entry points to Clear Browsing Data, including on the main Chrome menu. We’re also introducing a new quick deletion affordance to enable users to quickly delete their

recent history. We'll maintain and further enhance the more granular 'Advanced' Clear Browsing Data page on Privacy Settings.



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.

As early as Chrome 117, 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 an API and a group policy which will allow you to selectively keep the behavior unchanged.

Require X.509 key usage extension for RSA certificates chaining to local roots

X.509 certificates used for HTTPS should contain a key usage extension that declares how the key in a certificate may be used. Such instructions ensure certificates are not used in an unintended context, which protects against a class of cross-protocol attacks on HTTPS and other protocols. For this to work, HTTPS clients must check that server certificates match the connection's TLS parameters, specifically that the key usage flag for "digitalSignature" and possibly "keyEncipherment" (depending on TLS ciphers in use) are asserted when using RSA.

Chrome 117 will begin enforcing that the key usage extension is set properly on RSA certificates chaining to local roots. Key usage is already required for ECDSA certificates, and for publicly trusted certificates. Enterprises can test and temporarily disable key usage enforcement using the RSAKeyUsageForLocalAnchorsEnabled policy (available in Chrome 116).

Network service will be sandboxed on Linux and ChromeOS

As early as Chrome 117, the network service will be sandboxed on Linux and ChromeOS to improve security. On Linux, it's possible that third party software (likely data loss prevention or antivirus software) is injecting code into Chrome's processes and will be blocked by this change. This may result in Chrome crashing for your users.

If this happens, you should work with the vendor of the third party software to stop it from injecting code into Chrome's processes. In the meantime, you will be able to use the NetworkServiceSandboxEnabled policy to defer the sandboxing. This is a temporary measure intended to help enterprises surprised by the change; the policy will be removed in a future version of Chrome.

Bounce Tracking mitigations

As early as Chrome 116, Chrome will launch bounce tracking mitigations. Bounce tracking mitigations will only take effect when the policy is set to true (Block 3rd party cookies). You can use the BlockThirdPartyCookies policy to control this feature. Alternatively, if 3rd party cookies are blocked by default you can exempt specific sites by using the CookiesAllowedForUrls policy.

Restricting the use of --load-extension

The `--load-extension` command-line switch provides a very low bar for cookie theft malware to load malicious extensions without an installation prompt. Chrome will gradually phase out this switch to reduce this attack vector for malware. Starting in Chrome 116, `--load-extension` will be ignored for users that have enabled Enhanced Safe Browsing.

Service Worker static routing API

Chrome 116 will release the Service Worker static routing API; it enables developers to optimize how Service Workers are loaded. Specifically, it 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.

Enable access to WebUSB API from extension service workers

As early as Chrome 117, we will enable access to WebUSB API from extension service workers as a migration path for Manifest V2 extensions that currently access the API from a background page.

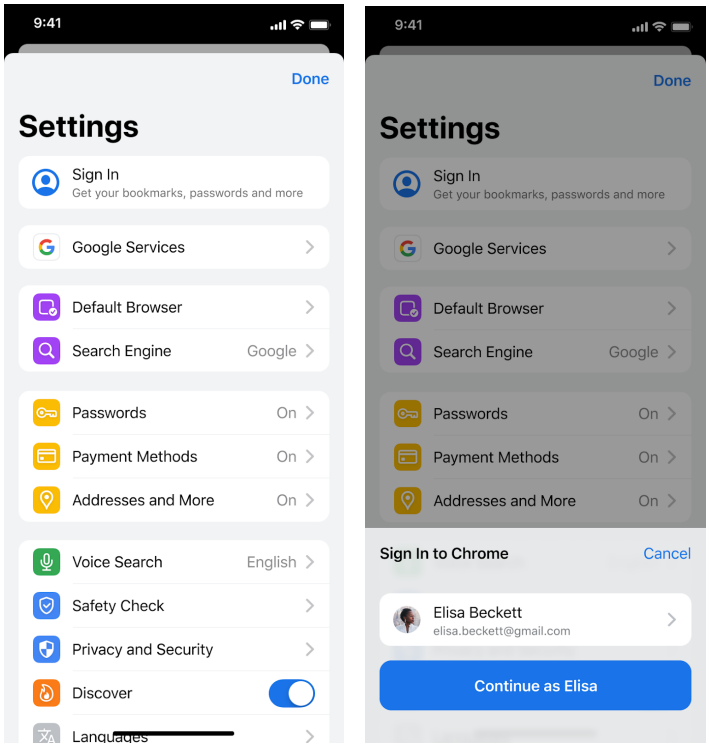
WebUSB policies can also be applied to extension origins to control this behavior. See DefaultWebUsbGuardSetting, WebUsbAskForUrls, WebUsbBlockedForUrls, and WebUsbAllowDevicesForUrls for more details.

Simplified sign-in and sync experience

Starting in Chrome 117, some users may experience a simplified and consolidated version of sign-in and sync in Chrome. Chrome sync will no longer be shown as a separate feature in settings or elsewhere. Instead, users can sign in to Chrome to use and save information like passwords, bookmarks and more in their Google Account, subject to the relevant enterprise policies.

As before, the functionality previously part of Chrome sync that saves and accesses Chrome data in the Google Account can be turned off fully (via SyncDisabled) or partially (via SyncTypesListDisabled). Sign-in to Chrome can be required or disabled via BrowserSignin as before.

Note that the changes do not affect users' ability to sign in to Google services on the web (like Gmail) without signing in to Chrome, their ability to stay signed out of Chrome, or their ability to control what information is synced with their Google Account.



IP Protection Phase 0 for Chrome

Beginning in Chrome 118, Chrome may 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 (including enterprise policies) will be provided in the near future.

Web MIDI permission prompt

Starting Chrome 118, the Web MIDI API access will be gated behind a permissions prompt. Currently, the use of SysEx messages with the Web MIDI API requires explicit user permission. With the planned implementation, even access to the Web MIDI API without SysEx support will require user permission. Both permissions will be requested in a bundled permissions prompt.

Three new policies **DefaultMidiSetting**, **MidiAllowedForUrls** and **MidiBlockedForUrls** will be available to allow administrators to pre-configure user access to the API.

Network Service on Windows will be sandboxed

As early as Chrome 118, 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.

Removal of the RendererCodeIntegrityEnabled policy

As early as Chrome 117, the RendererCodeIntegrityEnabled policy will be removed. We recommend that you verify any potential incompatibilities with third party software by no

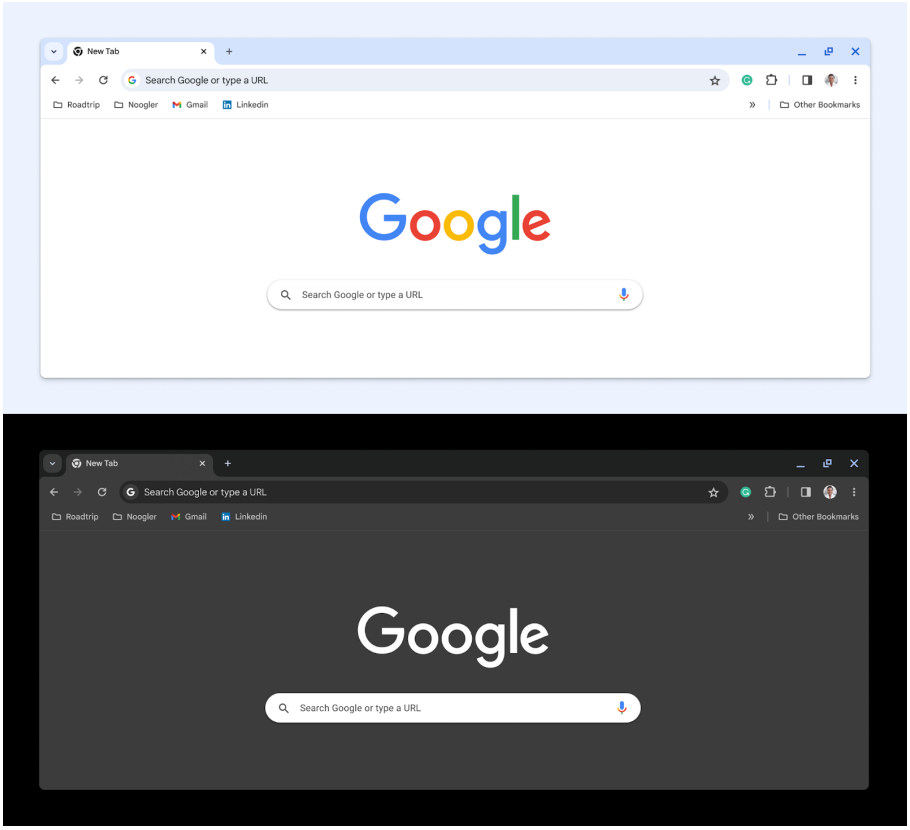
longer applying the policy in advance of this release. You can report any issues you encounter by submitting a bug here.

Chrome 117 will no longer support macOS 10.13 and macOS 10.14

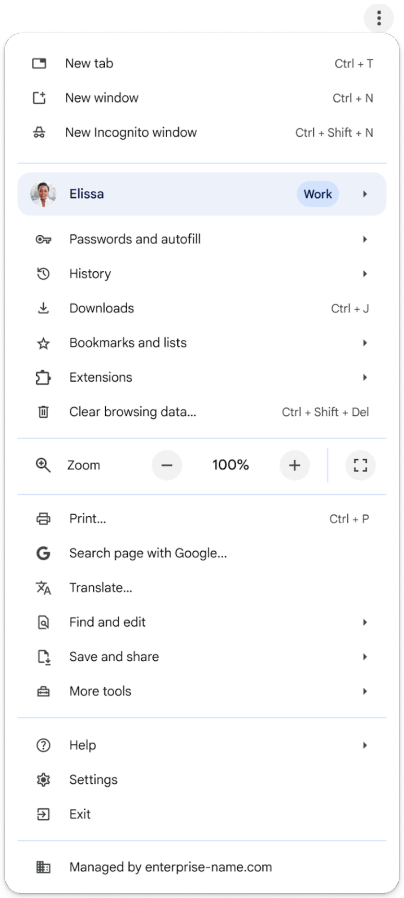
Chrome 117 will no longer support macOS 10.13 and macOS 10.14, which are already outside of their support window with Apple. Users have to update their operating systems in order to continue running Chrome browser. Running on a supported operating system is essential to maintaining security. If run on macOS 10.13 or 10.14, Chrome continues to show an infobar that reminds users that Chrome 117 will no longer support macOS 10.13 and macOS 10.14.

New Chrome Desktop visual refresh in Chrome 117

With Google's design platform moving to Google Material 3, we have an opportunity to modernize our desktop browser across OS's, leveraging updated UI elements or styling, enhancing personalization through a new dynamic color system, and improving accessibility. The first wave of UI updates will roll out in Chrome 117.



The three dot Chrome menu will also be refreshed, providing a foundation to scale personalization and customization experiences in Chrome by enabling customers proximate access to tools and actions.. The menu will be updated in phases starting in Chrome 117.



Update to the lock icon

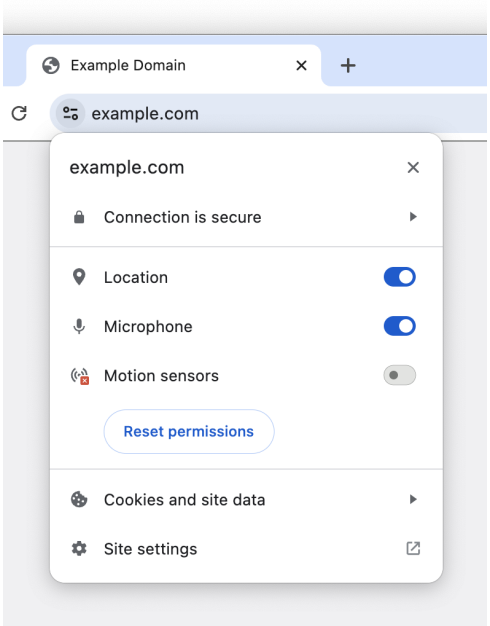
We plan to replace the lock icon with a variant of the tune icon, which is commonly used to indicate controls and settings. Replacing the lock icon with a neutral indicator prevents the misunderstanding that the lock icon is associated with the trustworthiness of a page, and emphasizes that security should be the default state in Chrome. Our research has also shown that many users never understood that clicking the lock icon showed important information and controls. We think the new icon helps make permission controls and additional security information more accessible, while avoiding the misunderstandings that plague the lock icon.

The new icon is scheduled to launch in Chrome 117 as part of a general design refresh for desktop platforms. Chrome will continue to alert users when their connection is not secure. You can see the new tune icon now in Chrome Canary for Desktop if you enable Chrome Refresh 2023 at chrome://flags#chrome-refresh-2023, but keep in mind this flag enables

work that is still actively in-progress and under development, and does not represent a final product.

We will also replace the icon on Android. On iOS, the lock icon is not tappable, so we will be removing the icon.

You can read more in this blog post.



Storage Access API with Prompts

The Storage Access API provides a means for authenticated cross-site embeds to check their blocking status and request access to storage if they are blocked. Targeting Chrome 117 for Desktop, we will support the Storage Access API by implementing all the behaviors listed in the specification, i.e. with user prompts, and additionally having its own user-agent-specific behaviors.

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, More details on the transition to Manifest V3, 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.

Starting with Chrome 110, an Enterprise policy ExtensionManifestV2Availability has been 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 until at least January 2024.

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.

For more details, refer to the Manifest V2 support timeline.

Removal ForceMajorVersionToMinorPositionInUserAgent policy

Chrome 118 plans to remove the ForceMajorVersionToMinorPositionInUserAgent policy. This policy was introduced in Chrome 99 to control whether the User-Agent string major version would be frozen at 99, in case of User-Agent string parsing bugs when the version changed to 100. Fortunately, we did not need to deploy this feature and only encountered a few minor 3-digit version parsing issues that have all since been fixed. Given that, we intend to remove this policy.

If you have any feedback about this policy removal, or are aware of intranet breakage that depends on the policy, please comment on this bug.

Chrome release schedule changes

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

Chrome 119 to phase out support for Web SQL

Starting in Chrome 119, to improve user data security, Chrome will remove support for Web SQL. The Web SQL Database standard was first proposed in April 2009 and abandoned in November 2010. As of today, Chrome is the only major browser with support for Web SQL. The W3C encouraged those needing web databases to adopt Indexed Database or SQLite WASM.

The timeline for the deprecation will be:

- Chrome 115 - Deprecation message added
- Chrome 117 - 123 - Deprecation trial
- Chrome 119 - Ship removal

More details about the deprecation and removal can be found on the Chromestatus page. An enterprise policy WebSQLAccess is available until Chrome 123 to enable Web SQL to be available.

Migrate away from data URLs in SVG <use> element

The SVG spec was recently updated to remove support for data: URLs in SVG <use> element. This improves security of the Web platform as well as compatibility between browsers as Webkit does not support data: URLs in SVG <use> element. We expect to remove support for data: URLs in SVG <use> element in Chrome 119, scheduled to ship in November 2023. You can read more in this blog post. For enterprises that need additional time to migrate, the **DataUrlInSvgUseEnabled** policy will be available temporarily to re-enable Data URL support for SVG <use> element.

Chrome profile separation

As early as Chrome 119, three new policies will be created to help enterprises configure enterprise profiles: **ProfileSeparationSettings**, **ProfileSeparationDataMigrationSettings**, **ProfileSeparationSecondaryDomainAllowlist**.

Removal LegacySameSiteCookieBehaviorEnabledForDomainList policy

In Chrome 79, we introduced the LegacySameSiteCookieBehaviorEnabledForDomainList policy to revert the SameSite behavior of cookies (possibly on specific domains) to legacy behavior. The LegacySameSiteCookieBehaviorEnabledForDomainList policy's lifetime has been extended and will now be removed in Chrome 127.

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. Mutation Events will stop functioning in Chrome 127, around July 30, 2024.

Upcoming ChromeOS changes

ChromeOS battery state sounds

As early as Chrome 117, we will add audible sounds to indicate battery status. Users will be able to turn on and off these sounds and Admins will be able to control them through policies.

When the device is not plugged in, you will hear warning sounds if:

- Battery level goes down to 15 minutes of charge time left, and another one when there is 5 minutes left.

When the device is plugged in, you will hear an information beep when:

- Battery level - 0-15% (low)
- Battery level - 16-79% (med)
- Battery level - 80-100% (high)

In the case where the device is connected to a low power charger, you'll hear warnings when the battery goes down to 10%, then again at 5%.

Previous release notes

Chrome version & targeted Stable channel release date	PDF
Chrome 115: July 12, 2023	PDF
Chrome 114: May 24, 2023	PDF
Chrome 113: Jan 10, 2023	PDF
Chrome 112: Mar 29, 2023	PDF
Archived release notes	

Additional resources

- For emails about future releases, sign up here.
- To try out new features before they're released, sign up for the trusted tester program.
- Connect with other Chrome Enterprise IT admins through the Chrome Enterprise Customer Forum.
- How Chrome releases work—Chrome Release Cycle
- Chrome Browser downloads and Chrome Enterprise product overviews—Chrome Browser for enterprise
- Chrome version status and timelines—Chrome Platform Status | Google Update Server Viewer
- Announcements: Chrome Releases Blog | Chromium Blog
- Developers: Learn about changes to the web platform.

Still need help?

- Google Workspace, Cloud Identity customers (authorized access only)—Contact support
- Chrome Browser Enterprise Support—Sign up to contact a specialist
- Chrome Administrators Forum
- Chrome Enterprise Help Center