chrome enterprise

Chrome 115 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 July 12, 2023.

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

Chrome 115 release summary

Chrome browser updates	**Security/ Privacy**	**User productivity/Apps**	**Management**
Google Search side panel		✓	
Secure DNS auto-upgrade for some Quad9Secure DNS users	✓		
HTTP requests upgraded to HTTPS	✓		
Support for Encrypted Client Hello (ECH)	✓		
Disable extensions unpublished from Chrome Web Store			✓
Updates to initial_preferences			✓
Bookmarks and reading list improvements on iOS		✓	
Update for secure DNS queries on Cox ISP servers	✓		
Reading mode		✓	
Removal of SHA1 in server signatures in TLS	✓		
Policy Sync dependency handling			✓
Skia renderer for PDF rendering	✓		✓
One Time Permissions desktop		✓	
Privacy Sandbox Developer enrollment form			✓
Update on BrowsingDataLifetime policy			✓
Set Up Chrome module for iOS		✓	
Carousel on the new tab page		✓	
New and updated policies in Chrome browser			✓
Removed policies in Chrome browser			✓
ChromeOS updates	**Security/ Privacy**	**User productivity/Apps**	**Management**

App Streaming on ChromeOS		✓	
Floating windows on ChromeOS		✓	
Freeze cast for cast moderator		✓	
Enhanced signature options for PDF toolkit		✓	
Passpoint: Seamless, secure connection to Wi-Fi networks		✓	
Expand Language Packs to Text-to-Speech		✓	
New keyboard Shortcut app		✓	
Admin console updates	**Security/ Privacy**	**User productivity/Apps**	**Management**
New Chrome Browser Cloud Management card			✓
ChromeOS Settings page redesign		✓	
Chrome Setup Guides		✓	
Printing reports now available in Chrome Management Reports API			✓
New policies in the Admin console			✓
Upcoming Chrome browser changes	**Security/ Privacy**	**User productivity/Apps**	**Management**
X25519Kyber768 key encapsulation for TLS	✓		
Improving performance: Memory Saver and Energy Saver modes			✓
Anti-phishing telemetry expansion	✓		
Network Service on Windows will be sandboxed	✓		
Enabling BFCache for pages that set Cache-Control: no-store	✓		
Idle Timeout policies			✓
Windows 11 changes affecting Chrome in		✓	

~September			
Native Client Support updates	✓		
Skip unload events	✓		
Extensions Review panel			✓
Require X.509 key usage extension for RSA certificates chaining to local roots			
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		✓	
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 refresh and Chrome menu in Chrome 117		✓	
Update for lock icon	✓	✓	
Extensions must be updated to leverage Manifest V3		✓	✓
Removal ForceMajorVersionToMinorPositionInUserAgent policy			✓
Chrome 119 to phase out support for Web SQL	✓		
Removal LegacySameSiteCookieBehaviorEnabledForDomainList policy			✓
Intent to deprecate: Mutation Events			✓

Upcoming ChromeOS changes	**Security/ Privacy**	**User productivity/Apps**	**Management**
ChromeOS battery state sounds			✓
Removal of permissive Chrome Apps webview behaviors	✓		

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

Google Search side panel

In Chrome 115, Google introduces 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 features a search box that allows text-based and visual queries, questions related to the page, and links to more details about the current site. We launch 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.

Secure DNS auto-upgrade for some Quad9Secure DNS users

Starting in Chrome 115, for a small subset of Chrome users, secure DNS queries are used instead of insecure DNS queries to perform host name resolution using Quad9 Secure (9.9.9.9) DNS servers. This change affects behavior for a given client under the following conditions only:

- The client is running on a system that has been configured to use the Quad9 Secure (9.9.9.9) DNS servers.
- The DnsOverHttpsMode enterprise policy is set to “Automatic” (the default value is “Off”).
- The ChromeVariations policy is set to enable all variations.
- The client is randomly selected to be part of the 1% of clients where this behavior is enabled.

HTTP requests upgraded to HTTPS

As early as Chrome 115, some users might see HTTP requests automatically upgraded to HTTPs. Any page that can't load via HTTPS is automatically reverted back to HTTP. For standard server configurations, this shouldn't have any visible effect, but it improves your users' security.

Some server configurations might cause issues, for example, if different content is served via HTTP and HTTPS. Users can bypass the automatic upgrading by explicitly navigating to an `http://` URL in the Omnibox, or by changing the **Insecure Content** site setting to enabled, accessible via Page Info and `chrome://settings/content`. You can control this behavior with the HttpsUpgradesEnabled policy, and allowlist specific sites with the HttpAllowlist policy.

In the long term, you should ensure that your organization's servers support HTTPS and serve the same content on both HTTP and HTTPS. If you don't intend to support HTTPS (for example, on an intranet behind a firewall), servers shouldn't respond to port 443, and firewalls should close the connection rather than leave it hanging. You can test HTTPS upgrading in your environment by enabling `chrome://flags#https-upgrades`. If you come across any issues, you can report them to us.

Starting in Chrome 115, Chrome automatically enables HTTPS-First Mode based on the user's browsing history. It automatically enables the HTTPS-First Mode interstitial on sites that regularly load over HTTPS. Sites that regularly use plaintext HTTP are unaffected. In practice, this change protects users from downgrade attacks, but is invisible to users.

Support for Encrypted Client Hello (ECH)

Chrome 115 starts rolling out support for ECH on sites that opt in, as a continuation of our network-related efforts to improve our users’ privacy and safety on the web, for example, Secure DNS. This change was originally planned for Chrome 107, but had to be postponed.

If your organization’s infrastructure relies on the ability to inspect SNI, for example, filtering, logging, and so on, you should test it. You can enable the new behavior by navigating to `chrome://flags` and enabling the `#encrypted-client-hello` flag.

On Windows and Linux, you also need to enable Secure DNS for the flag to have an effect.

If you notice any incompatibilities, you can use the EncryptedClientHelloEnabled enterprise policy to disable support for ECH.

Disable extensions unpublished from Chrome Web Store

In Chrome 115, we release the Enterprise policy ExtensionUnpublishedAvailability to allow you to disable extensions that have been unpublished from the Chrome Web Store.

Updates to initial_preferences

We've removed the following fields from the `initial_preferences` sample file:

- Removed from example because they're no longer valid:
    - sync_promo.show_on_first_run_allowed
    - suppress_first_run_bubble
    - suppress_first_run_Default_browser_prompt
- Removed from example because they can be controlled by a recommended policy:
    - homepage
    - homepage_is_newtabpage
    - show_home_button
    - session
    - bookmark_bar
    - import_* except for import_bookmarks_from_file
    - make_chrome_default_*
- Removed from example because they're not applicable to enterprise usage, or only applicable to for user-level install:
    - ping_delay
    - do_not_launch_chrome
    - do_no_register_for_update_launch

Bookmarks and reading list improvements on iOS

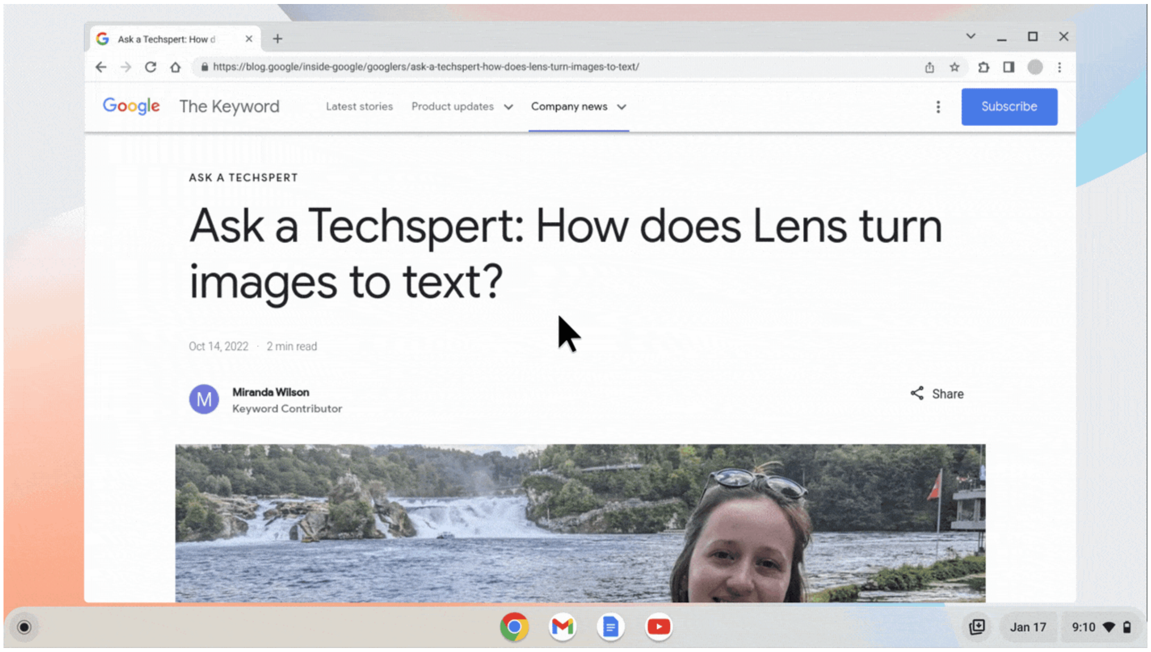
On Chrome 115 on iOS, some users who sign in to Chrome from bookmark manager or reading list surfaces can now use and save bookmarks and reading list items in their Google Account. Relevant enterprise policies, such as BrowserSignin, SyncDisabled, SyncTypesListDisabled, EditBookmarksEnabled and ManagedBookmarks continue to work as before, to configure whether users can use and save items in their Google Account.

Update for secure DNS queries on Cox ISP servers

For clients running on systems that use the Cox ISP DNS servers, if the DnsOverHttpsMode policy is set to *Automatic*, Chrome uses secure DNS queries instead of insecure DNS queries, starting in Chrome 115 (and in earlier versions, starting on 5/16/2023, if the ChromeVariations policy is set to enable all variations).

Reading mode

As more content is read online, Chrome 115 adds a new feature to help improve the online reading experience. Introducing reading mode, a new feature on Chrome browser, which enhances the reading experience on the web for everyone. Reading mode reduces distracting elements through a resizable and customizable reader view in the Chrome browser side panel, enabling readers to focus on the primary content. Users can also customize the font, text size, spacing, theme or background color, and more, making for a more cohesive, intuitive, and comfortable reading experience.



https://blog.google/inside-google/googlers/ask-a-techspert-how-does-lens-turn-images-to-text/

ASK A TECHSPERT

Ask a Techspert: How does Lens turn images to text?

Oct 14, 2022 · 2 min read

Miranda Wilson
Keyword Contributor

Removal of SHA1 in server signatures in TLS

Chrome 115 removes support for signature algorithms using SHA-1 for server signatures during the TLS handshake. SHA1, which has known collisions, has been deprecated by the IETF, and should be avoided, where possible.

This does not affect SHA-1 support in server certificates, which was already removed. SHA-1 in client certificates continues to be supported.Enterprises that rely on SHA1 signature schemes in TLS can use the InsecureHashesInTLSHandshakesEnabled policy to continue to accept SHA1 in server signatures.

Policy Sync dependency handling

Currently, we require admins to set SyncDisabled for any data-deletion policy (BrowsingDataLifetime, ClearBrowsingDataOnExitList). In Chrome 115, we automatically disable sync for the respective data types and no longer require admins to additionally set the SyncDisabled policy. We will gradually roll out this feature behind a flag. You can enable this behavior at `chrome://flags#data-retention-policies-disable-sync-types-needed`.

Skia renderer for PDF rendering

Chrome 115 adds a new enterprise policy, PdfUseSkiaRendererEnabled, to override user choice on whether to enable Skia renderer. When Skia renderer is enabled, it switches the PDF render device from AGG (Anti-Grain Geometry) to Skia. Skia renderer provides enhanced technical support and uses different algorithms for drawing graphics. Any resulting visual differences are expected to be very minor.

One Time Permissions desktop

When users are prompted for a permission they can currently select Allow or Deny, both options are stored permanently. This feature adds an *Allow this time* option for geolocation, camera and microphone permissions. This fine-tunes the permission granted to a newly introduced session, which we believe more accurately represents a one-time permission session, without affecting any common scenarios. In Chrome 115, we start slowly rolling out this feature to a subset of users.

Privacy Sandbox Developer enrollment form

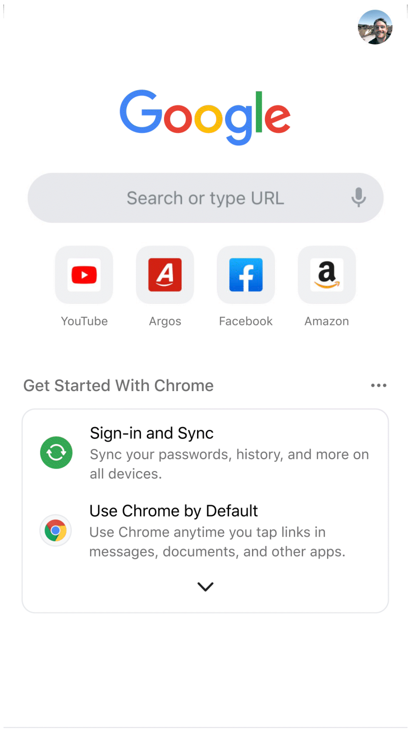
To access the Privacy Sandbox relevance and measurement APIs on Chrome and Android, developers need to enroll with the Privacy Sandbox. The developer enrollment process verifies companies before they can use the APIs, as an additional layer of protection for user privacy. As part of this enrollment process, we require developers to agree to restrictions around the usage of these services to prevent re-identification of users across sites.

Update on BrowsingDataLifetime policy

We have updated the documentation for BrowsingDataLifetime to state that *download_history* and *hosted_app_data* are not supported on Android.

Set Up Chrome **module for iOS**

On iOS, some new users in Chrome 115 see the new *Set Up Chrome* module. This module provides options, in the center of the new tab page, to allow new users to view and complete items that help them set up and get the most out of Chrome, on their own time. The items listed in the module are optional, and the module displays temporarily for up to a few weeks after installing the app. At this time, this is only available for iOS.



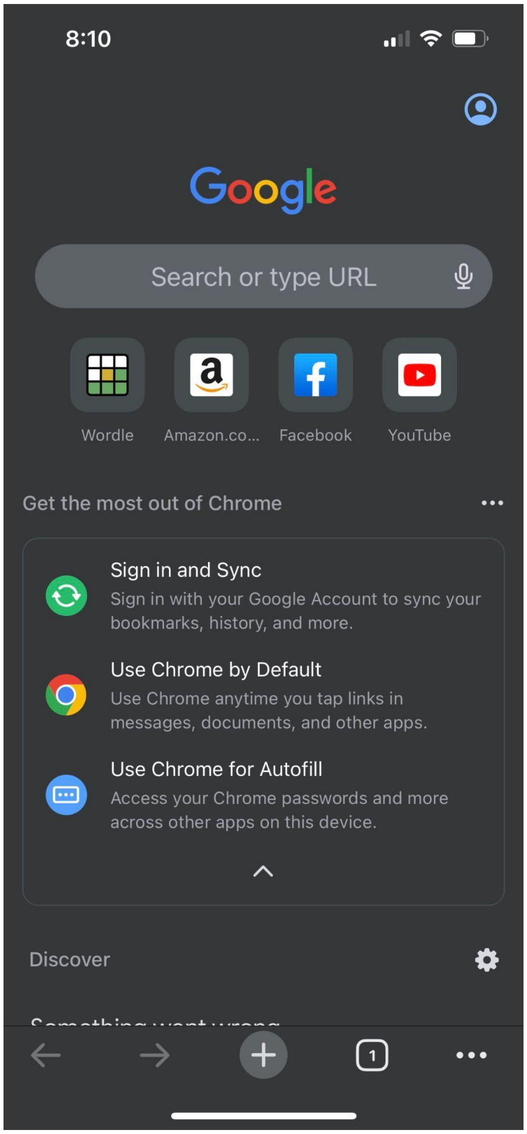
Get Started With Chrome

Sign-in and Sync

Sync your passwords, history, and more on all devices.

Use Chrome by Default

Use Chrome anytime you tap links in messages, documents, and other apps.



Get the most out of Chrome

Sign in and Sync
Sign in with your Google Account to sync your bookmarks, history, and more.

Use Chrome by Default
Use Chrome anytime you tap links in messages, documents, and other apps.

Use Chrome for Autofill
Access your Chrome passwords and more across other apps on this device.

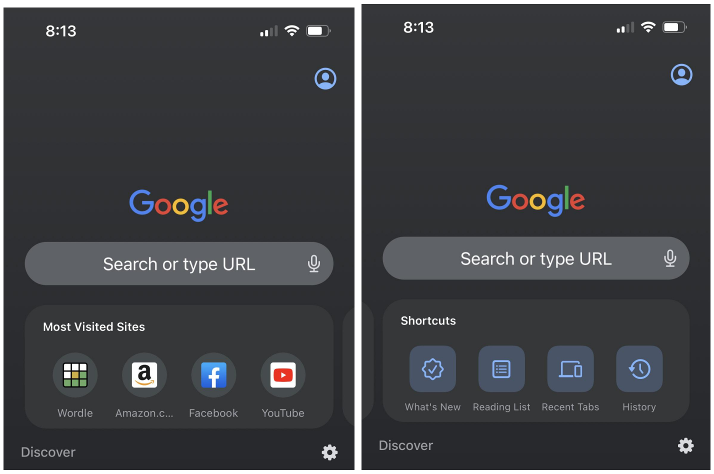
Something went wrong

Carousel on the Google *New tab* page

A new carousel on the Google **New tab** page allows users to swipe between certain modules. This is a limited-availability feature for some new users. The carousel can display in two ways:

1. With the **Most Visited Sites** and **Shortcuts** module, or
2. With the **Shortcuts** module.

For example, a user might see **Most Visited Sites** but can swipe to see **Shortcuts**.



New and updated policies in Chrome browser

Policy	Description
ExtensionUnpublishedAvailability	Control availability of extensions unpublished on the Chrome Web Store.
SafeSitesFilterBehavior	Filter top level sites (but not embedded iframes) for adult content (now available on Android).
PdfUseSkiaRendererEnabled	Use the default renderer based on the field trial configuration.
GoogleSearchSidePanelEnabled	Enable Google Search Side Panel on all web pages.

Removed policies in Chrome browser

Policy	Description
ForceEnablePepperVideoDecoderDevAPI	Enable support for the PPB_VideoDecoder(Dev) API.
PPAPISharedImagesSwapChainAllowed	Allow modern buffer allocation for Graphics3D APIs PPAPI plugin.

UseMojoVideoDecoderForPepperAllowed	Allow Pepper to use a new decoder for hardware accelerated video decoding.

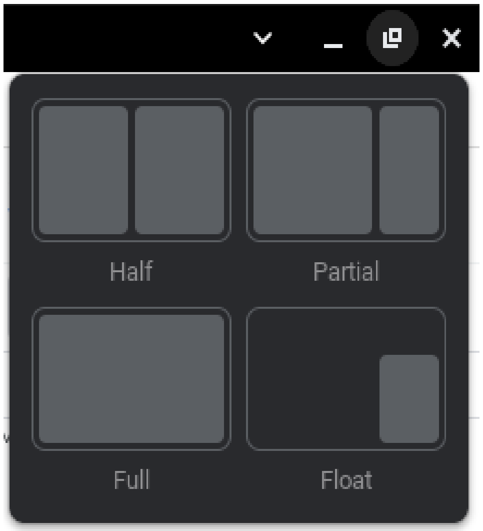
ChromeOS updates

App Streaming on ChromeOS

As early as ChromeOS 115, App Streaming enhances the Phone Hub experience, by allowing users to see and interact with streamed apps running on their Pixel phone. When a user receives a mirrored conversation notification from their Pixel phone, a simple tap on that notification kicks off an app stream directly to the user's ChromeOS desktop. This is part of a Google-wide ambient computing effort.

Floating windows on ChromeOS

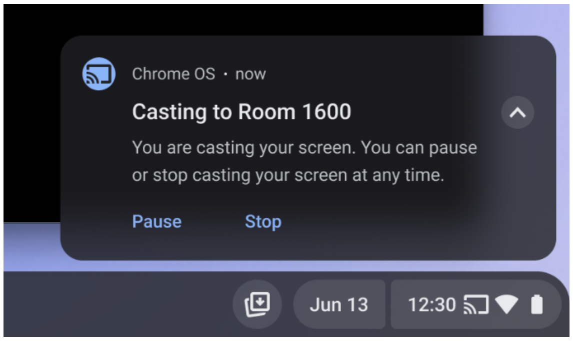
In Chrome 115, a new **Window layout** menu in ChromeOS helps to accelerate common actions like split-screening two windows. In addition, we're adding a new window state, **Float**, which allows users to set a window as always-on-top.



Pause cast for cast moderator

While using cast moderator, sometimes users need a quick way to pause what they are casting. In ChromeOS 115, with **Pause cast**, you can now pause what you cast to the shared screen on a still image, while you do something else on your computer.

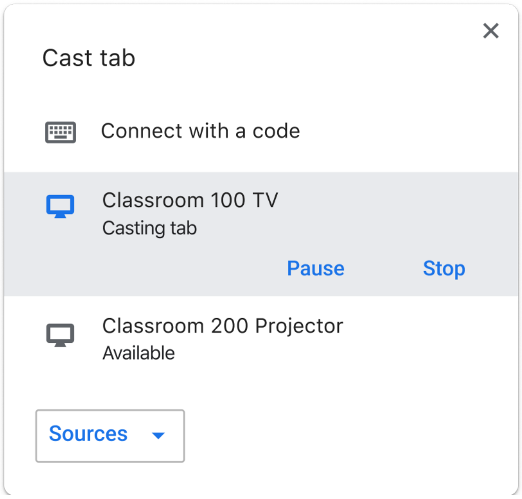
In ChromeOS Quick Settings or from Chrome browser Cast menu, select **Pause** to display the last casted screen on the cast receiver. While paused, other actions you perform on your computer are NOT cast to the cast receiver. When cast is resumed, your computer starts mirroring to the cast receiver again.



Chrome OS • now

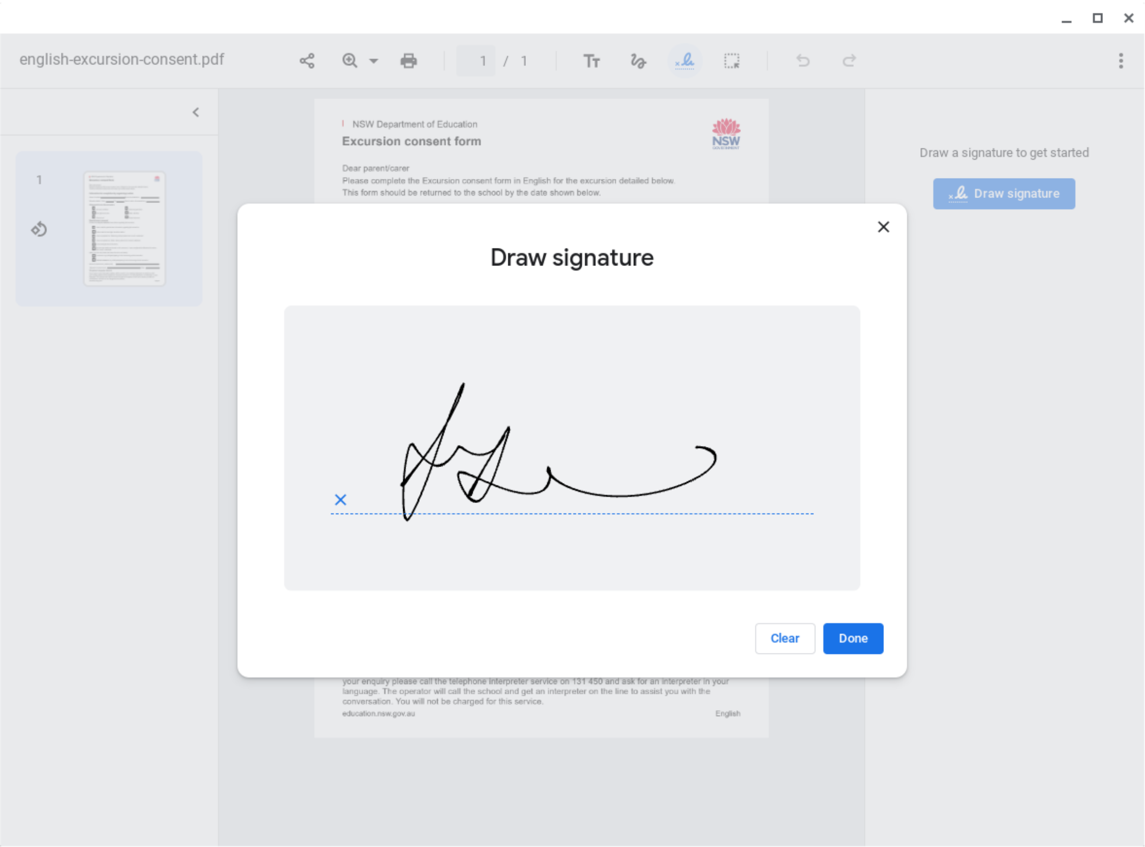
Casting to Room 1600

You are casting your screen. You can pause or stop casting your screen at any time.



Enhanced signature options for PDF toolkit

In ChromeOS 115, the Gallery PDF toolkit makes it easier for users to sign their documents, allowing for the creation of a free-hand signature that is saved in the app for subsequent use. Gallery is the ChromeOS media multi-tool that provides users with fast, consistent, and discoverable ways to view, tweak, and route various media types.



english-excursion-consent.pdf
1 / 1
1
Draw a signature to get started
Draw signature
Draw signature
Clear
Done

NSW Department of Education

Excursion consent form

Dear parent/carer
Please complete the Excursion consent form in English for the excursion detailed below.
This form should be returned to the school by the date shown below.

your enquiry please call the telephone interpreter service on 131 450 and ask for an interpreter in your language. The operator will call the school and get an interpreter on the line to assist you with the conversation. You will not be charged for this service.

education.nsw.gov.au English

Passpoint: Seamless, secure connection to Wi-Fi networks

Passpoint streamlines Wi-Fi access and eliminates the need for users to find and authenticate a network each time they visit. Once a user accesses the Wi-Fi network offered at a location, the Passpoint-enabled client device will automatically connect upon subsequent visits.

Wi-Fi Passpoint is now supported on ChromeOS through supported Android applications. Wi-Fi Passpoint is a set of Wi-Fi mechanisms defined by the Wi-Fi Alliance that facilitate and automate the provisioning and configuration of secure Wi-Fi networks while also minimizing user intervention. Once provisioned, whenever a compatible and secured Wi-Fi network is in range, ChromeOS can automatically connect to it without the need for user interaction.

Expand Language Packs to Text-to-Speech

Some Google Text-to-Speech voices that were previously preinstalled are now downloaded over the network when they are needed. This frees up some space on the ChromeOS device.

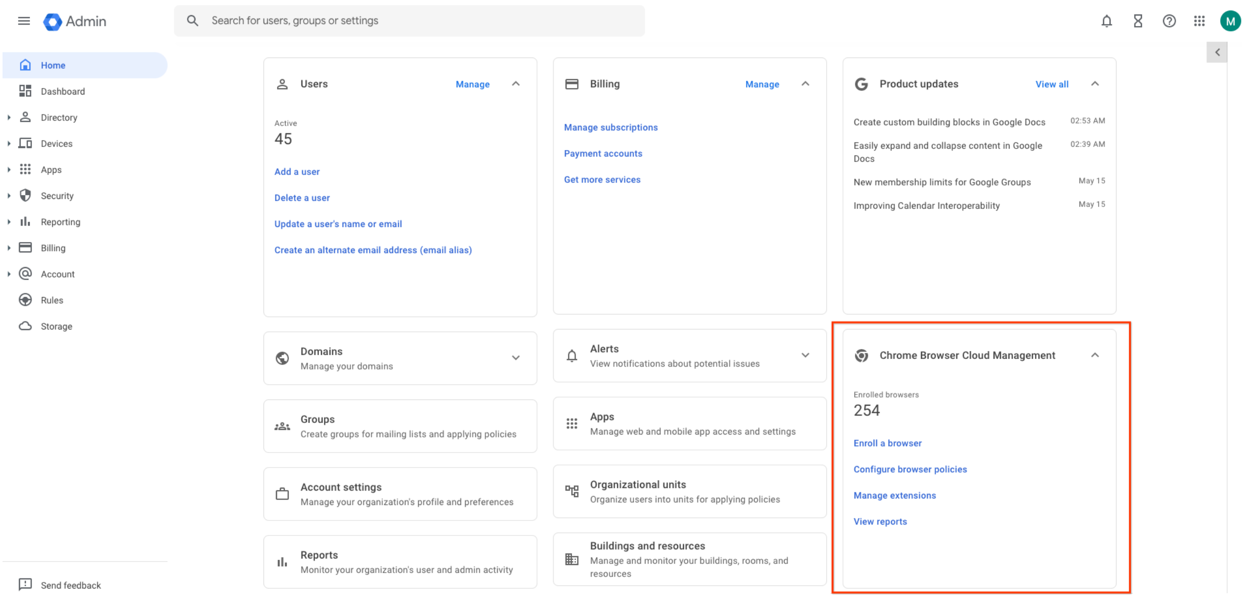
New keyboard Shortcut app

The new Shortcut App offers a new navigation and taxonomy, easier in-app search functionalities and a refreshed shortcut visualization.

Admin console updates

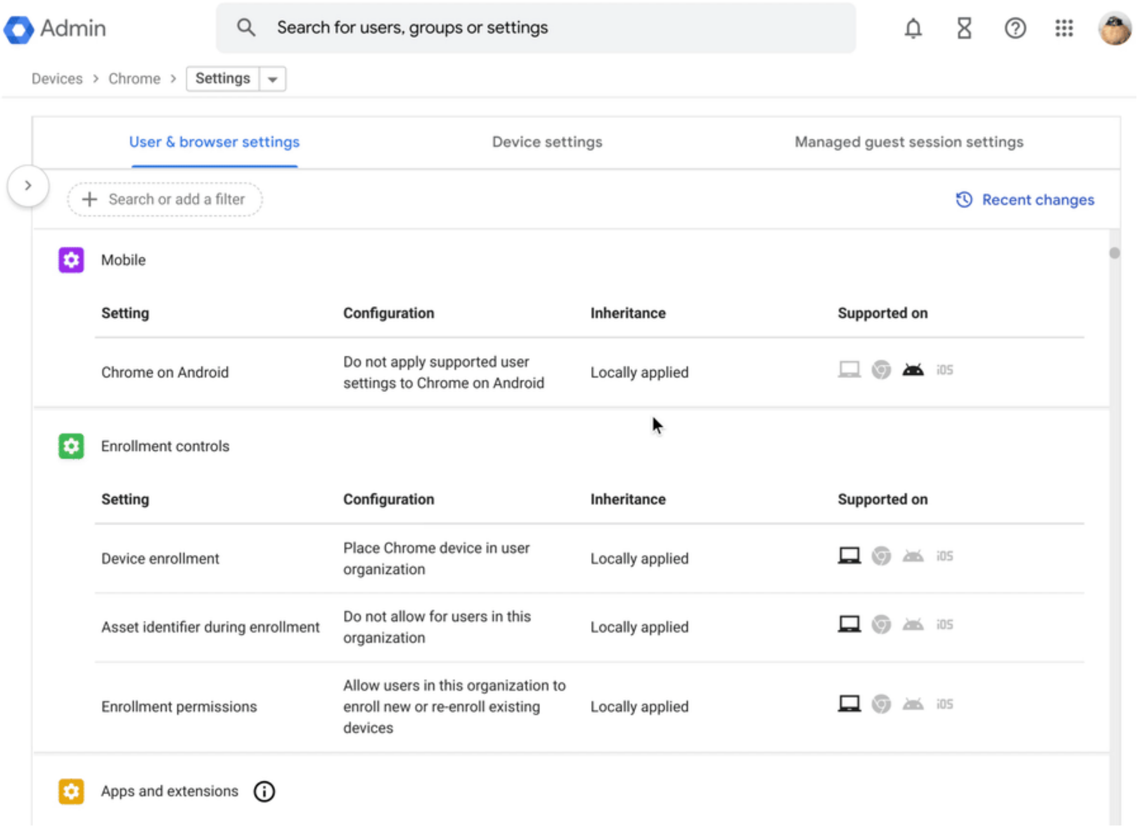
New Chrome Browser Cloud Management card

Chrome 115 launches a new **Chrome Browser Cloud Management** card on the homepage of the Google Admin console. You can now easily access and find popular Chrome browser management tasks, directly on the homepage.


Admin
Search for users, groups or settings
M
Home
Dashboard
Directory
Devices
Apps
Security
Reporting
Billing
Account
Rules
Storage
Send feedback
Users
Manage
Active
45
Add a user
Delete a user
Update a user's name or email
Create an alternate email address (email alias)
Billing
Manage
Manage subscriptions
Payment accounts
Get more services
Product updates
View all
Create custom building blocks in Google Docs
02:53 AM
Easily expand and collapse content in Google Docs
02:39 AM
New membership limits for Google Groups
May 15
Improving Calendar Interoperability
May 15
Domains
Manage your domains
Alerts
View notifications about potential issues
Chrome Browser Cloud Management
Enrolled browsers
254
Enroll a browser
Configure browser policies
Manage extensions
View reports
Groups
Create groups for mailing lists and applying policies
Apps
Manage web and mobile app access and settings
Account settings
Manage your organization's profile and preferences
Organizational units
Organize users into units for applying policies
Reports
Monitor your organization's user and admin activity
Buildings and resources
Manage and monitor your buildings, rooms, and resources

Chrome Settings page redesign

We've heard your feedback, and we're excited to share that all admins now see a redesigned experience across **Users & browsers**, **Device**, and **Managed guest session** settings pages to make it easier to manage policies. Look out for:



Admin
Search for users, groups or settings
Devices > Chrome > Settings
User & browser settings
Device settings
Managed guest session settings
Search or add a filter
Recent changes

Mobile

Setting	Configuration	Inheritance	Supported on
Chrome on Android	Do not apply supported user settings to Chrome on Android	Locally applied	💻 ◎ 🤖 iOS

Enrollment controls

Setting	Configuration	Inheritance	Supported on
Device enrollment	Place Chrome device in user organization	Locally applied	💻 ◎ 🤖 iOS
Asset identifier during enrollment	Do not allow for users in this organization	Locally applied	💻 ◎ 🤖 iOS
Enrollment permissions	Allow users in this organization to enroll new or re-enroll existing devices	Locally applied	💻 ◎ 🤖 iOS

Apps and extensions

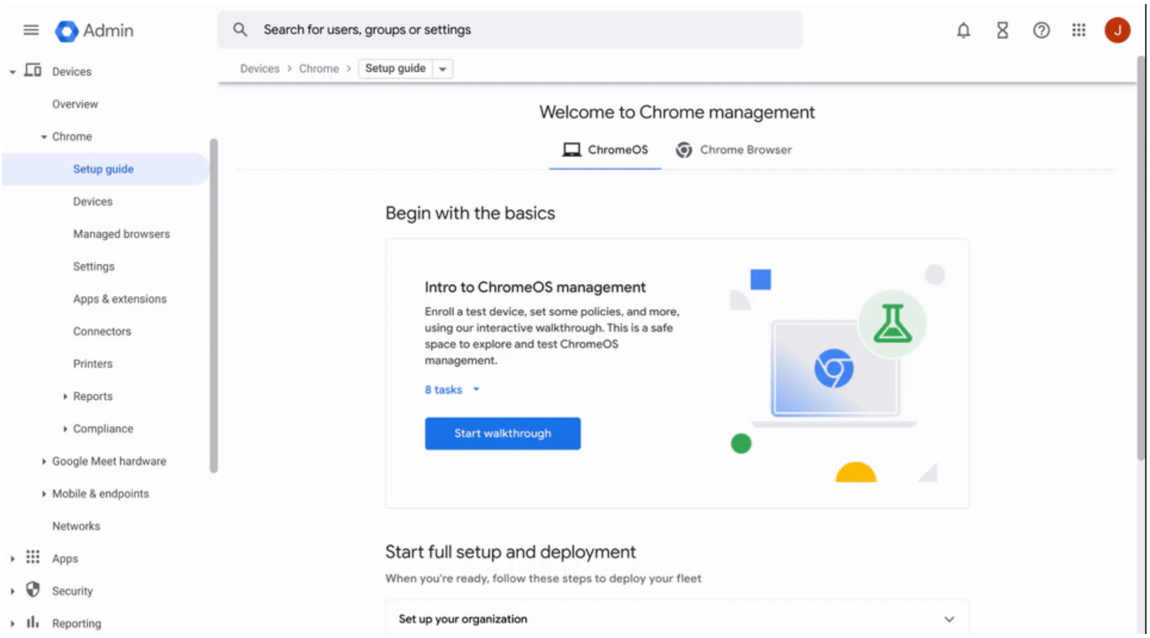
- A more scannable, read-only table to view setting configurations across your organization.
- Dedicated policy views for admins to focus on individual settings.
- Updated policy descriptions that pull directly from live Help Center content; no more toggling between windows to learn more about a policy. This includes *supported-on* information for platform and version for all policies.

Chrome Setup Guides

The Chrome Setup Guides section now includes new, interactive content to help with performing common ChromeOS journeys in the Admin console. These new journeys include:

- Creating test organizational units
- Adding users for testing

- Turning on ChromeOS reporting
- Enrolling a test device
- Setting device policies
- Setting user policies
- Installing apps and extensions
- Adding a Wi-Fi network



Welcome to Chrome management

Begin with the basics

Intro to ChromeOS management

Enroll a test device, set some policies, and more, using our interactive walkthrough. This is a safe space to explore and test ChromeOS management.

Start full setup and deployment

When you're ready, follow these steps to deploy your fleet

To access the new Chrome Setup Guides:

- Log in to the Admin console.
- On the left , select **Devices**>**Chrome**>**Setup Guides**.

Printing reports now available in Chrome Management Reports API

We have added additional endpoints to Chrome Management Reports API that allow access to printing reports. The new endpoints provide per-user and per-printer summary printing reports, as well as a listing of all print jobs submitted to managed printers. The data provided by the new endpoints corresponds to the data in the **Print Usage** page of the Admin console. This update exposes the same data in the third-party Reports API.

New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
Enable AutoFill for addresses	User & Browser Settings	M88	User experience > Address form Autofill
Enable AutoFill for credit cards	User & Browser Settings	M88	User experience > Credit card form Autofill

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

X25519Kyber768 key encapsulation for TLS

As early as Chrome 116, Chrome will introduce a post-quantum secure TLS key encapsulation mechanism X25519Kyber768, based on a NIST standard. This will be 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.

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 will 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) will have increased visibility of discarded tabs in the tab strip and more insight into memory usage of active and inactive tabs.

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

1. In settings, users will be able to 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 will have the option to 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 phishy 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.

Network Service on Windows will be sandboxed

As early as Chrome 116, 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.

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.

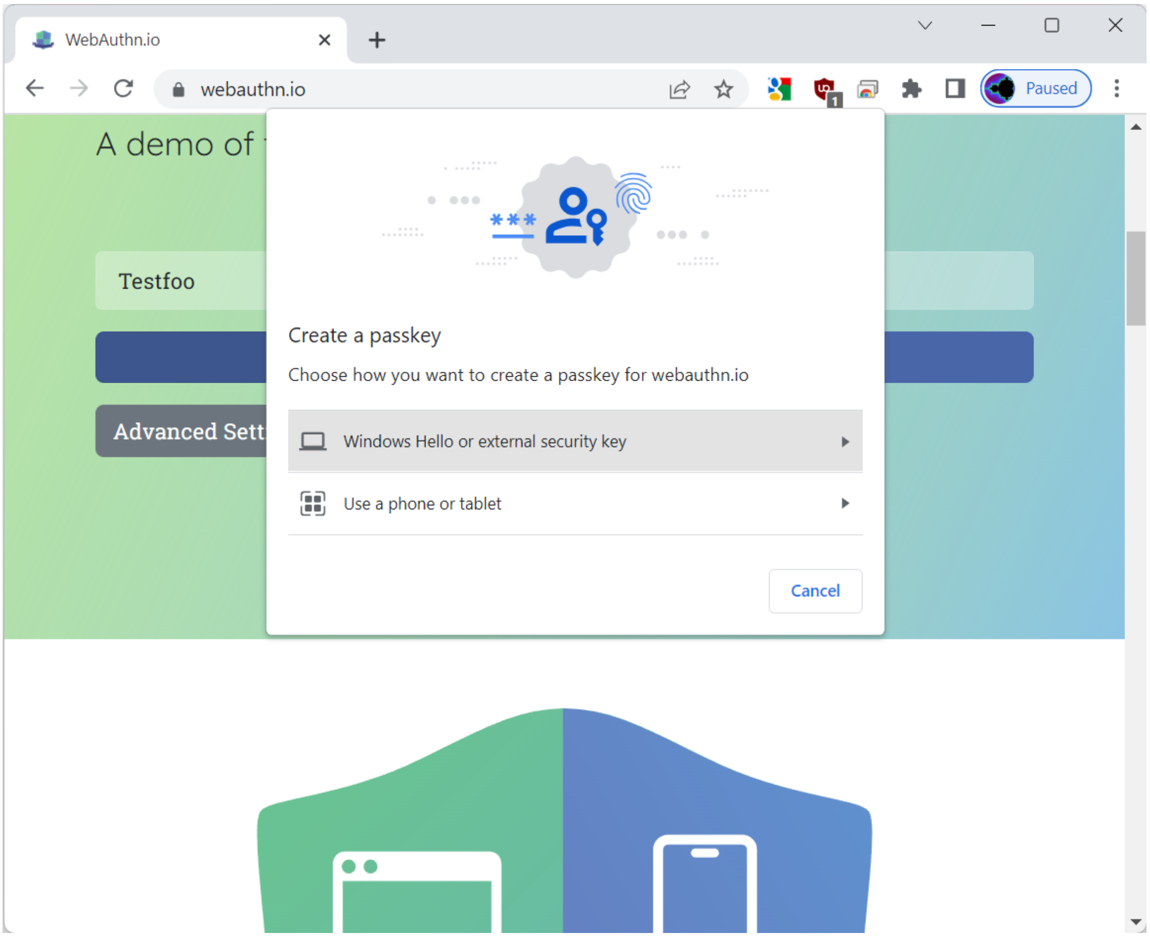
Idle Timeout policies

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

Windows 11 changes affecting Chrome in ~September

An update to Windows 11 later in 2023 will add support for cross-device passkeys flows in Windows **webauthn.dll v6**. Chrome 116 will recognise this version of Windows and stop offering its own cross-device support in Chrome UI, deferring to Windows instead. This will result 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.

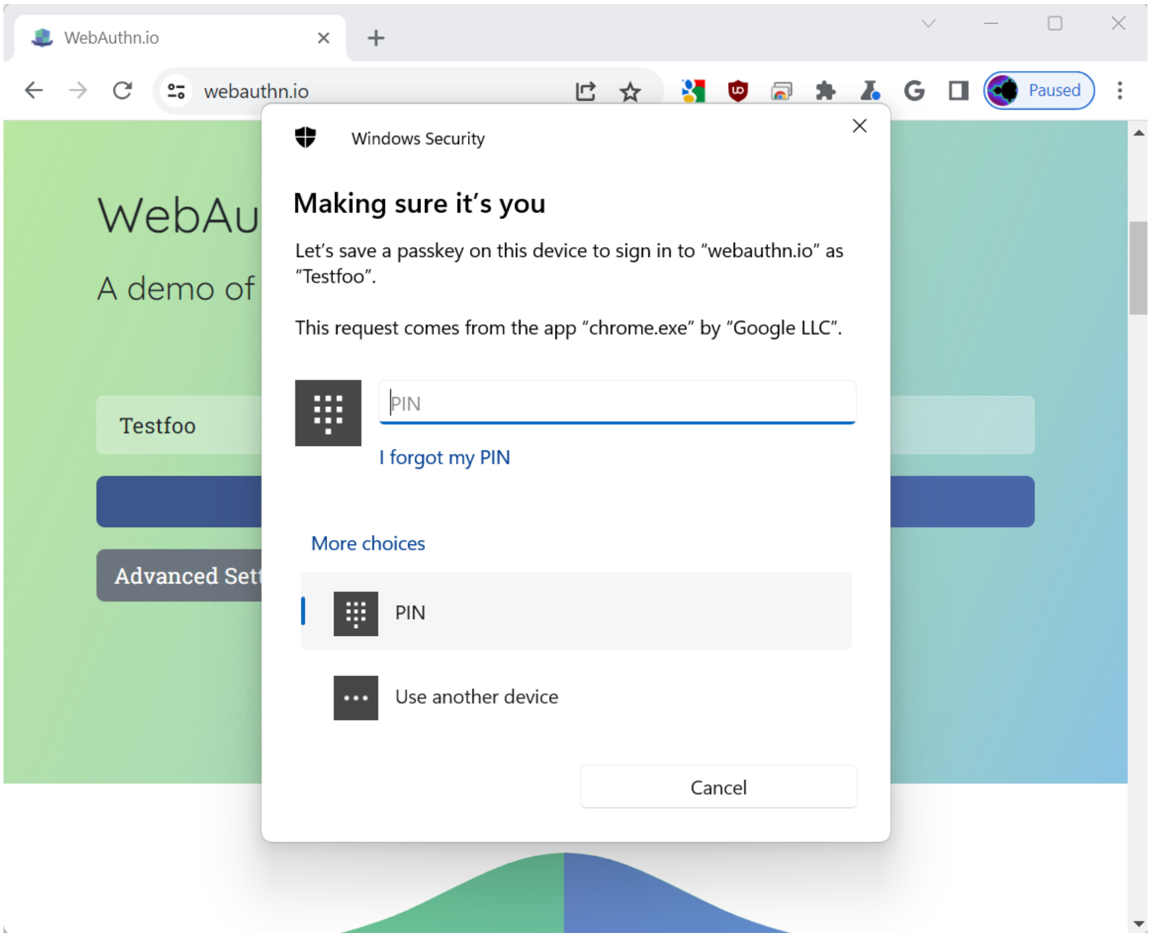
Before:



Create a passkey

Choose how you want to create a passkey for webauthn.io

After:



Making sure it's you

Let's save a passkey on this device to sign in to "webauthn.io" as "Testfoo".

This request comes from the app "chrome.exe" by "Google LLC".

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.

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.

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.

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).

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.

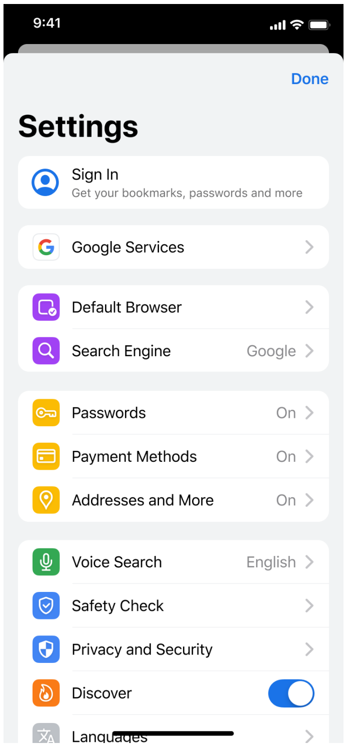
WebUSB policies can also be applied to extension origins to control this behavior. See DefaultWebUsbGuardSetting, WebUsbAskForUrls, WebUsbBlockedForUrls, and WebUsbAllowDevicesForUrls for more details.

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.



9:41

Done

Settings

Sign In
Get your bookmarks, passwords and more

Google Services

Default Browser

Search Engine — Google

Passwords — On

Payment Methods — On

Addresses and More — On

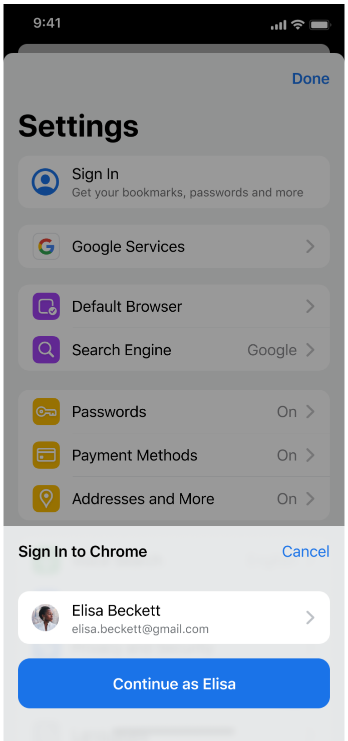
Voice Search — English

Safety Check

Privacy and Security

Discover

Languages



9:41

Done

Settings

Sign In
Get your bookmarks, passwords and more

Google Services

Default Browser

Search Engine — Google

Passwords — On

Payment Methods — On

Addresses and More — On

Sign In to Chrome — Cancel

Elisa Beckett
elisa.beckett@gmail.com

Continue as Elisa

Web MIDI permission prompt

Starting Chrome 117, 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.

Removal of the RendererCodeIntegrityEnabled policy

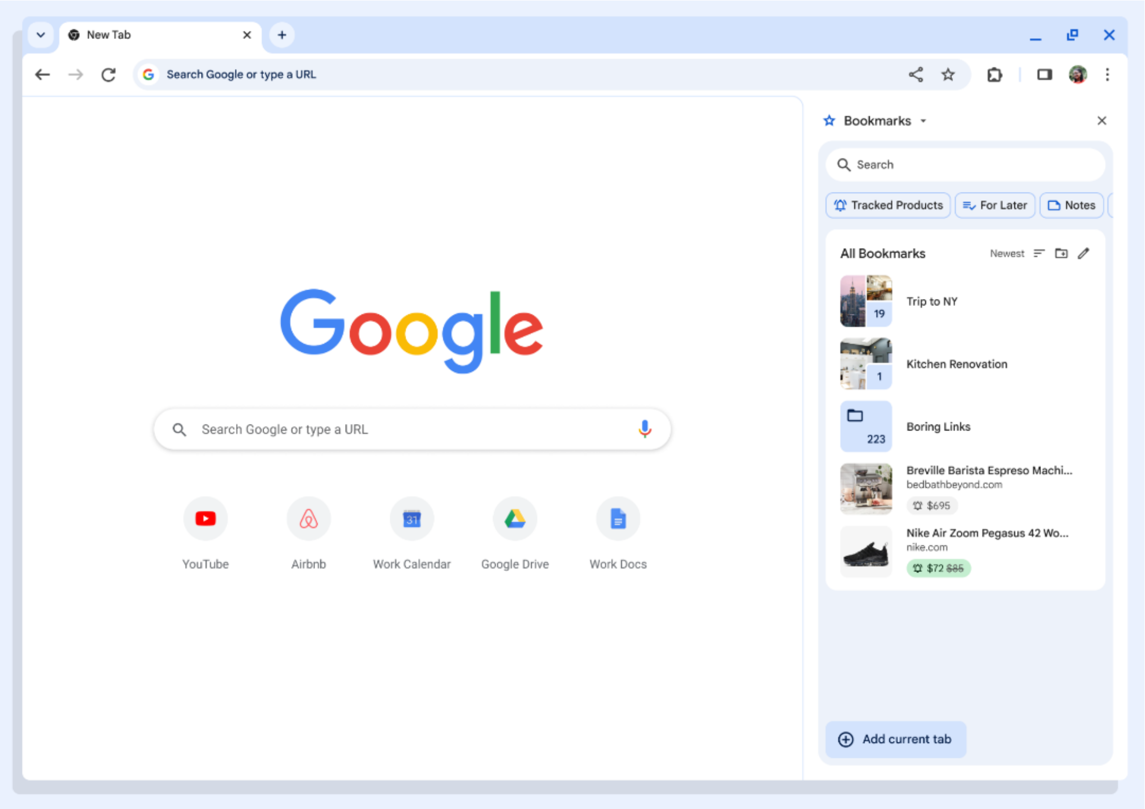
As early as Chrome 117, the RendererCodeIntegrityEnabled policy will be removed. We recommend that you verify any potential incompatibilities with third party software by no longer applying the policy in advance of this release. You can report any issues you encounter by submitting a bug here.

Chrome 117 will no longer support macOS 10.13 and macOS 10.14

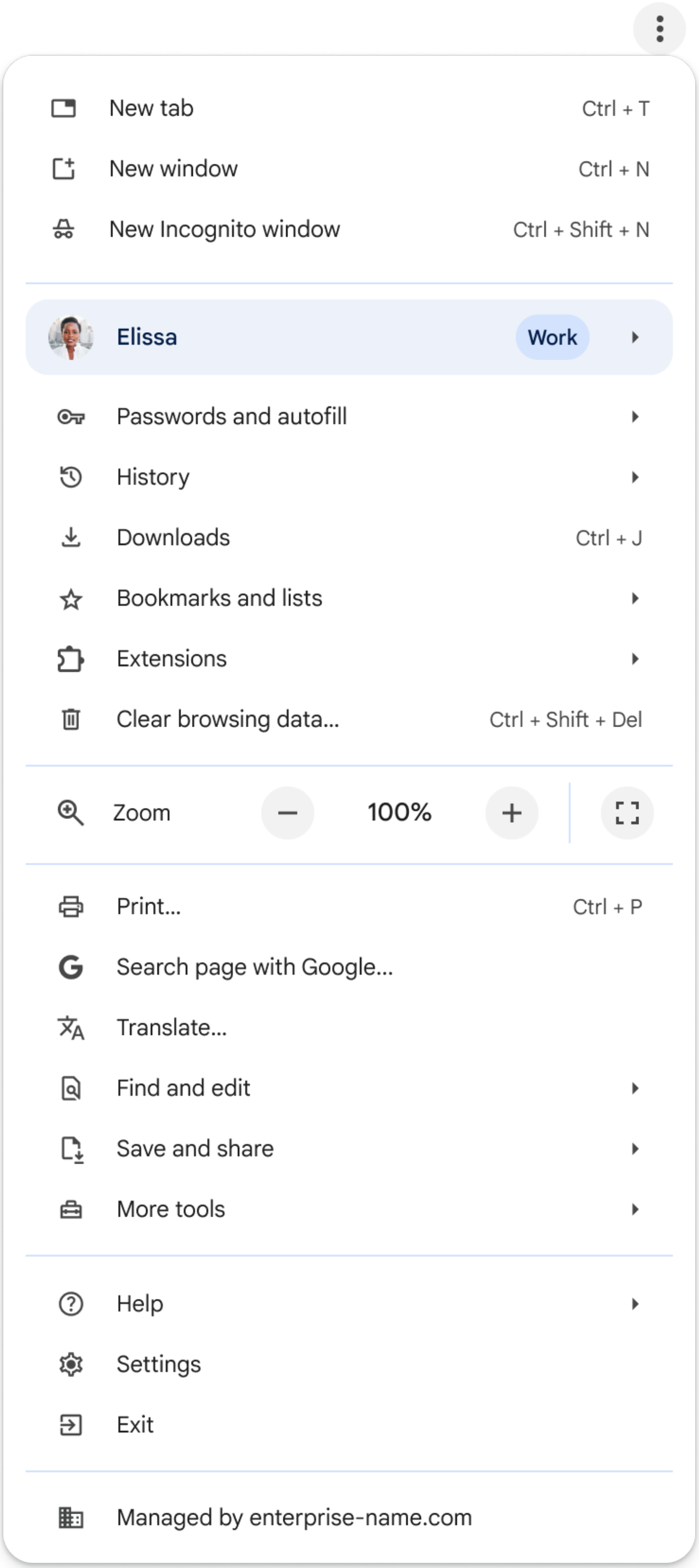
Chrome 117 will no longer support macOS 10.13 and macOS 10.14, which are already outside of their support window with Apple. Users have to update their operating systems in order to continue running Chrome browser. Running on a supported operating system is essential to maintaining security. If run on 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 refresh and Chrome menu 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 desktop Chrome UI, communications, and personalization. The menu will be updated in phases starting in Chrome 117 with the Desktop Refresh.


New tab Ctrl + T
New window Ctrl + N
New Incognito window Ctrl + Shift + N
Elissa Work
Passwords and autofill
History
Downloads Ctrl + J
Bookmarks and lists
Extensions
Clear browsing data... Ctrl + Shift + Del
Zoom – 100% +
Print... Ctrl + P
Search page with Google...
Translate...
Find and edit
Save and share
More tools
Help
Settings
Exit
Managed by enterprise-name.com

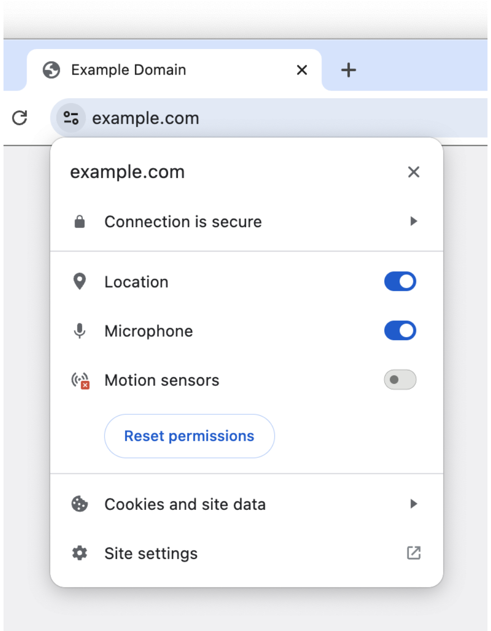
Update for lock icon

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 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.

On iOS, the lock icon is not tappable, so we will be removing the icon.

You can read more in this blog post.



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 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 - Add deprecation message
- Chrome 118 - 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.

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. LegacySameSiteCookieBehaviorEnabledForDomainList policy will be removed in Chrome 121.

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

Removal of permissive Chrome Apps webview behaviors

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

- SSL errors within webview show an error page that does not provide the user the option to unsafely proceed.
- The use of 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 will be 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, the previous behavior from Chrome 112 and earlier can also be restored 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.

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 114: May 24, 2023	PDF
Chrome 113: Jan 10, 2023	PDF
Chrome 112: Mar 29, 2023	PDF
Chrome 111: Mar 01, 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