Chrome 114 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 May 24, 2023.

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

Chrome 114 release summary

Chrome browser updates	**Security/ Privacy**	**User productivity/ Apps**	**Management**
Chrome Root Store updates	✓		
Support for Private State Tokens	✓		
Inactive Tabs in Chrome app on iPhone and iPad		✓	
Lock profile cookie files on disk	✓		
Rebranding and updates to Google Password Manager		✓	
Improved *Check passwords* on iOS			
Saving and retrieving notes in Password Manager now easier		✓	
Password manager policy disables password import			✓
Updates to Bookmarks on Desktop		✓	
Unpacking nested archives for download protection	✓		
Separate storage of settings synced to account	✓		
Side Panel API	✓		
Pick up where you left off on Android		✓	
Chrome Enterprise profiles signout			✓
Update chip on desktop		✓	
New and updated policies in Chrome browser			✓
Removed policies in Chrome browser			✓
ChromeOS updates	**Security/ Privacy**	**User productivity/ Apps**	**Management**
Cursive pre-installed for Enterprise and Education accounts		✓	

Passpoint: Seamless, secure connection to Wi-Fi networks	✓	✓	
Mandatory extensions for Incognito navigation	✓		
Audio controls visibility		✓	
ChromeVox earcons		✓	
Admin console updates	**Security/ Privacy**	**User productivity/ Apps**	**Management**
Chrome Browser Cloud Management (CBCM) subscription			✓
New policies in the Admin console			✓
Upcoming Chrome browser changes	**Security/ Privacy**	**User productivity/ Apps**	**Management**
HTTP requests upgraded to HTTPS in Chrome 115	✓		
Chrome policy: disable extensions unpublished from Chrome Web Store (CWS)			✓
Skip unload events	✓		
master_preferences->initial_preferences migration			✓
Release cycle changes			✓
Bookmarks and Reading List improvements on iOS		✓	
Update for Secure DNS / Cox ISP users	✓		
Reading mode		✓	
Anti-phishing telemetry expansion	✓		
Deprecating the use of SHA1 in server signatures in TLS	✓		
Policy Sync dependency handling			✓
Web MIDI permission prompt	✓		

X25519Kyber768 key encapsulation for TLS	✓		
Network Service on Windows will be sandboxed	✓		
Restricting the use of --load-extension	✓		
Enable access to WebUSB API from extension service workers in Chrome 116	✓		
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		✓	✓
Chrome 119 to phase out support for Web SQL	✓		
Upcoming ChromeOS changes	**Security/ Privacy**	**User productivity/ Apps**	**Management**
App Streaming on Chrome OS		✓	
Google Photos Shared Albums		✓	
Removal of permissive Chrome Apps webview behaviors	✓		
Upcoming Admin console changes	**Security/ Privacy**	**User productivity/ Apps**	**Management**
New Chrome Browser Cloud Management card			✓

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.

Chrome browser updates

Chrome Root Store updates

As early as Chrome 114, to improve user security and provide a consistent experience across different platforms, Chrome switches to its own default root store and built-in certificate verifier on:

- Android
- Linux
- ChromeOS

The ChromeRootStoreEnabled policy allows selective disabling of the Chrome Root Store in favor of the platform root store. You can set this policy to Disabled to force the use of the platform root store, otherwise it is enabled by default. The policy will be made available on **Android, Linux, and ChromeOS** until Chrome 120.

The Chrome Root Store is already enabled by default on:

- Windows
- MacOS

The ChromeRootStoreEnabled policy has been removed from **Windows and Mac** in Chrome 113. Support for trusted leaf certificates and the Windows Trusted People store was added for Chrome 111. Support for name constraints on local trust anchors was added back in Chrome 112.

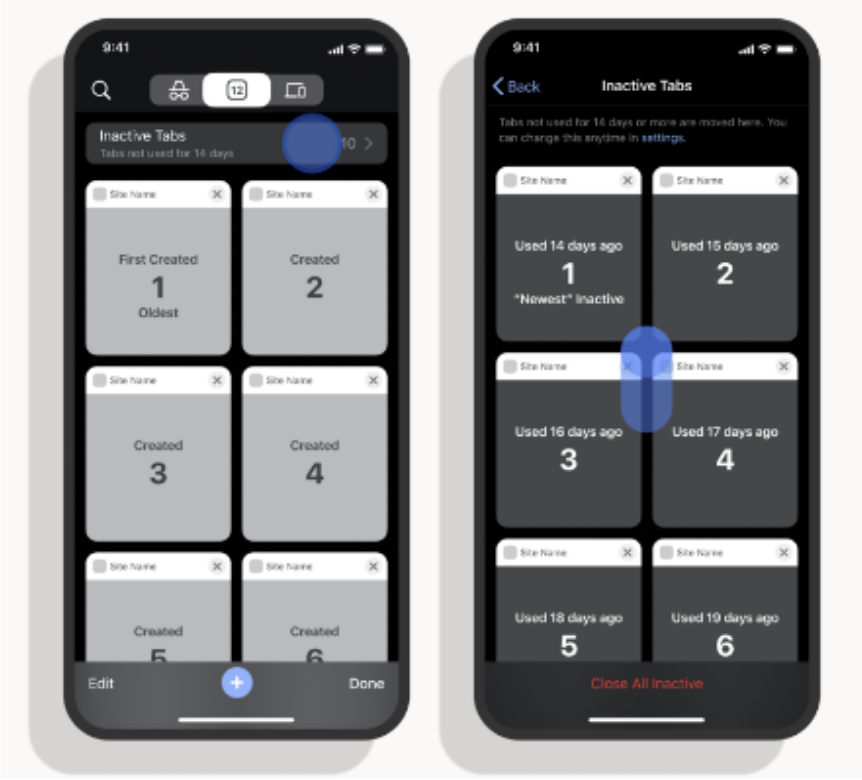
Chrome continues to use custom local roots installed to the operating system's trust store. See our article about the Chrome Root Program for more information. We do not anticipate any changes to how enterprises currently manage their fleet and trusted enterprise CAs, such as through group policy, macOS Keychain Access, or system management tools like Puppet.

Support for Private State Tokens

Chrome 114 makes the Private State Tokens API available for use by websites. Private State Tokens enable trust in a user's authenticity to be conveyed from one context to another, to help sites combat fraud and distinguish bots from real humans—without the exchange of user identifying information. Availability of Private State Tokens is controlled using a new setting in Chrome settings called **Auto-verify**. Read more in this developer blog post.

Inactive Tabs in Chrome app on iPhone and iPad

In Chrome 114, old tabs are now grouped under a new *Inactive Tabs* section in the **Tab** grid view. Chrome users can access the inactive tabs section to view all old tabs or close them using the new bulk tab functionality. Alternatively, users can simply click to bring back an inactive tab.



Lock profile cookie files on disk

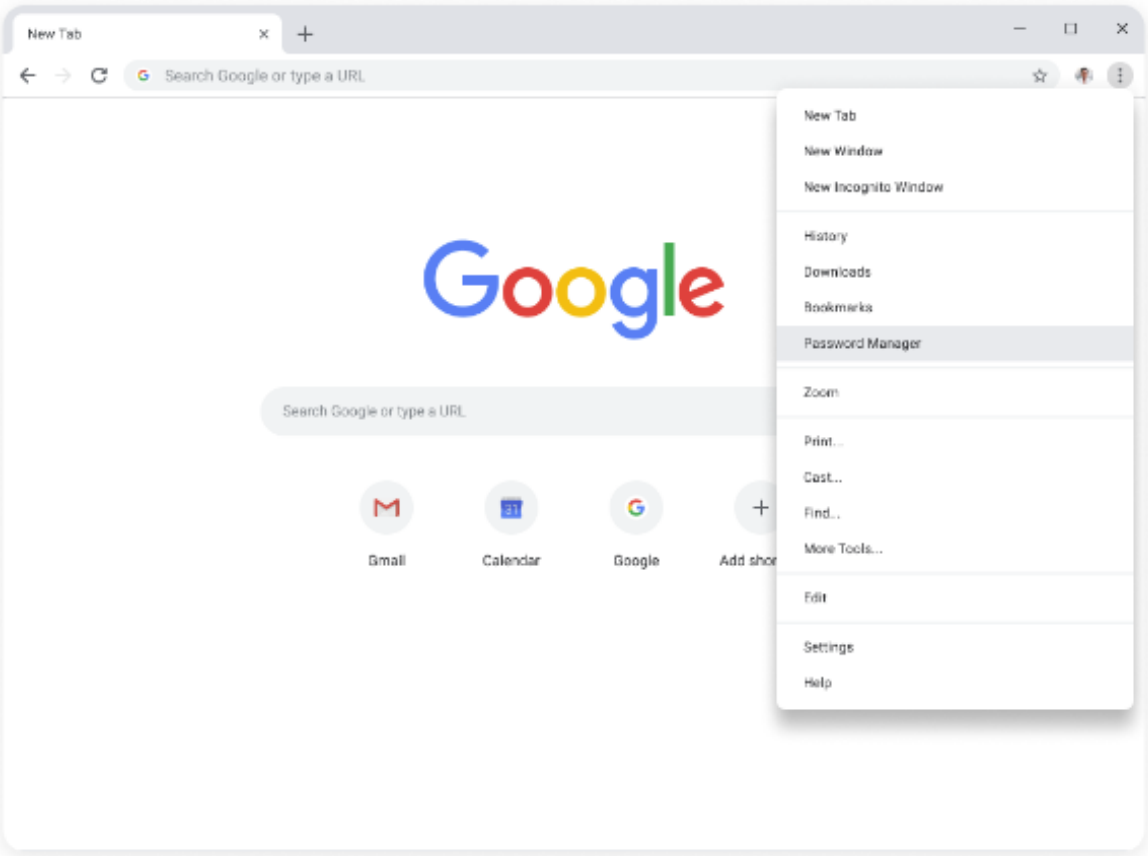
To help protect Chrome users against malware attempting to steal cookie information, Chrome 114 on Windows holds an exclusive lock on the profile cookie files on disk. To ensure this behavior does not interfere with any sanctioned software on your system, you can run Chrome with the `-enable-features=LockProfileCookieDatabase` command-line flag on the Dev or Beta channel of Chrome 114.

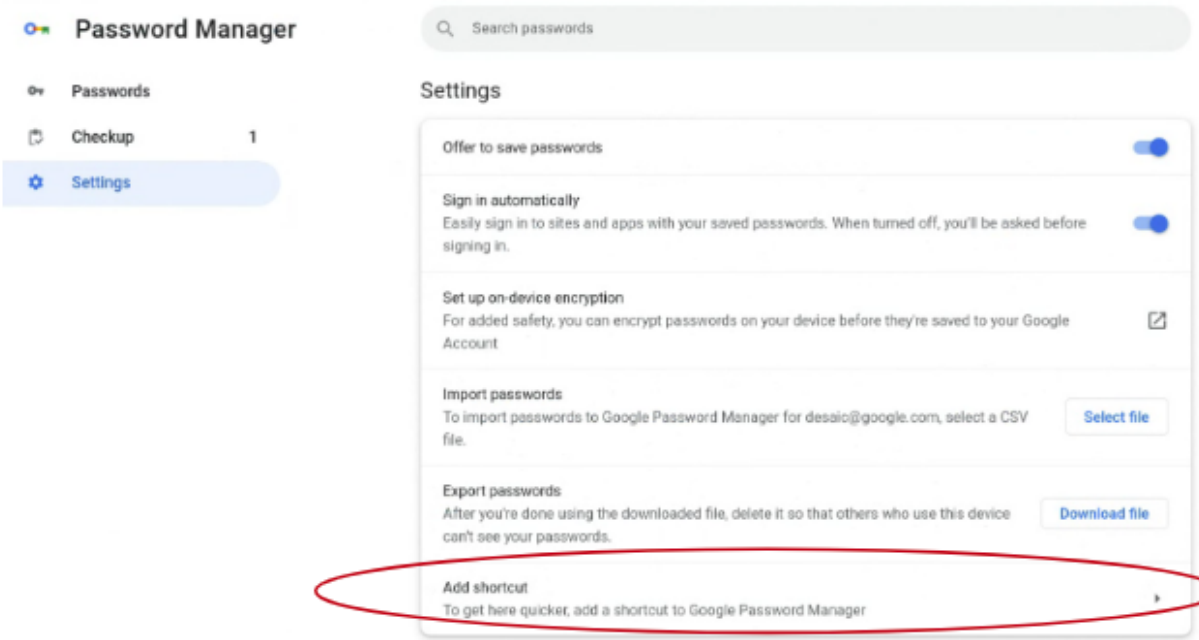
Rebranding and updates in Google Password Manager

In Chrome 114, the password manager is rebranded as **Google Password Manager**.

Google Password Manager offers more functionality and is easier to access using the three dot menu. The upgraded **Google Password Manager**:

- groups similar passwords together
- has an improved checkup flow
- and you can add the password manager shortcut to your desktop.


New Tab
Search Google or type a URL
New Tab
New Window
New Incognito Window
History
Downloads
Bookmarks
Password Manager
Zoom
Print...
Cast...
Find...
More Tools...
Edit
Settings
Help
Google
Search Google or type a URL
Gmail
Calendar
Google

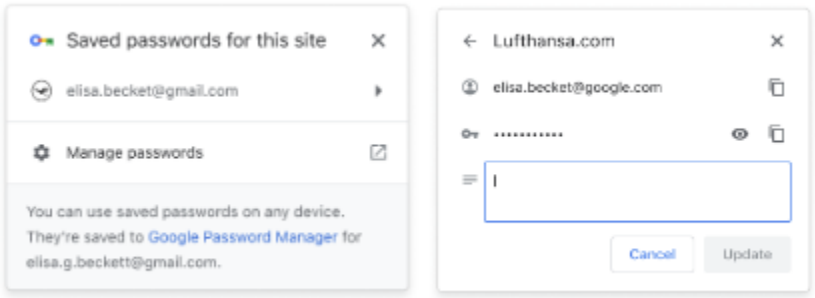

Password Manager
Search passwords
Passwords
Checkup 1
Settings
Settings
Offer to save passwords
Sign in automatically
Easily sign in to sites and apps with your saved passwords. When turned off, you'll be asked before signing in.
Set up on-device encryption
For added safety, you can encrypt passwords on your device before they're saved to your Google Account
Import passwords
To import passwords to Google Password Manager for desaic@google.com, select a CSV file.
Select file
Export passwords
After you're done using the downloaded file, delete it so that others who use this device can't see your passwords.
Download file
Add shortcut
To get here quicker, add a shortcut to Google Password Manager

Improved *Check passwords* on iOS

The **Check passwords** feature of Password Manager on iOS includes a list of passwords flagged by Google as unsafe. On other platforms, these are further categorized as: compromised, weak, or reused. Chrome 114 now introduces these granular categories on iOS.

Saving and retrieving notes in Password Manager now easier

Chrome 114 revamps the password management user journey, triggered from the key icon in the omnibox. It replaces the current list of passwords with a new list that allows navigating to the password details view. In the password details view, users can copy the username or password, unmask the password and edit the stored note.

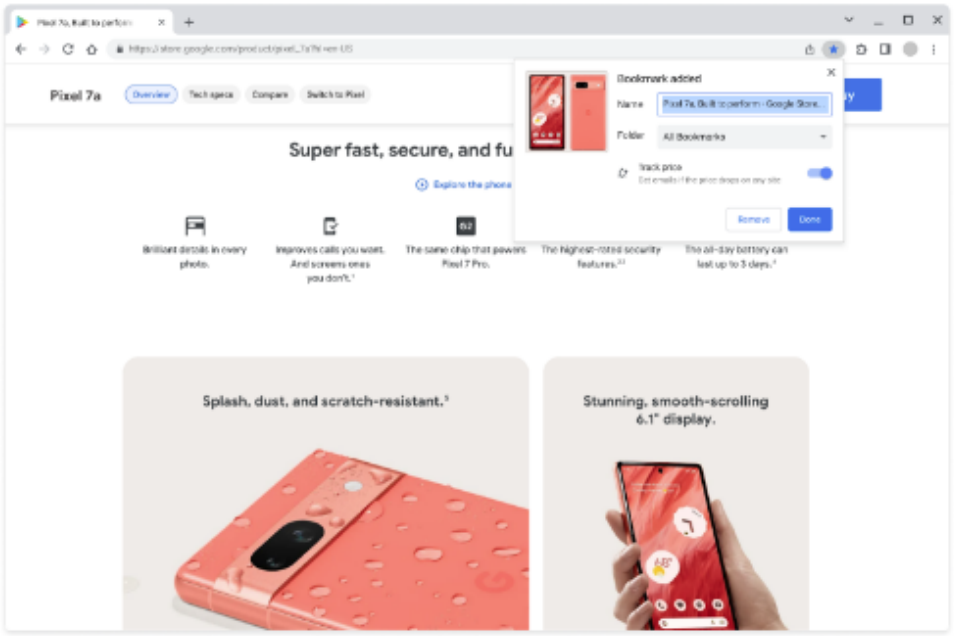


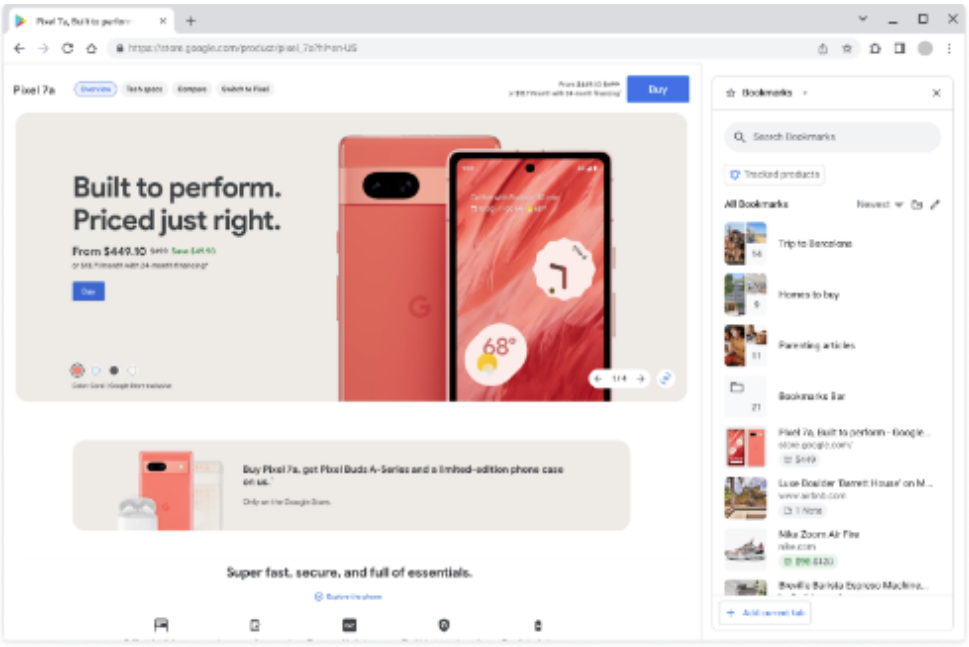
Password manager policy disables password import

We recently fixed an issue that previously allowed users to import passwords even though the Password Manager was disabled by Enterprise policy. Users can no longer import passwords when the PasswordManagerEnabled policy is set to false.

Updates to Bookmarks on Desktop

Starting in Chrome 114, some users see an updated experience of the Bookmarks side panel, including features such as filtering, sorting, and editing.





Unpacking nested archives for download protection

Starting in Chrome 114, users with Safe Browsing set to Standard or Enhanced protection now begin recursively unpacking downloads of nested archives. This extends the

long-standing protections Chrome offers against malware and unwanted software, and specifically combats techniques abused by distributors of cookie theft malware. The SafeBrowsingProtectionLevel policy allows you to enable or disable Safe Browsing, including this feature.

Separate storage of settings synced to account

For Chrome users on iOS and Android who have Sync enabled, settings synced to their Google account are now kept separate from the local Chrome settings, which were set when Sync was off. This allows for strictly less data sharing than previously: local settings don't get automatically uploaded when turning on Sync, and no settings from the account are left behind on the device when Sync is turned off. This feature is still disabled by default and you can enable it using the flag `chrome://flags#enable-preferences-account-storage`.

As an admin, you can control who can save and sync data related to managed Google accounts.There are two existing policies to disable Sync functionality, which continue to apply:

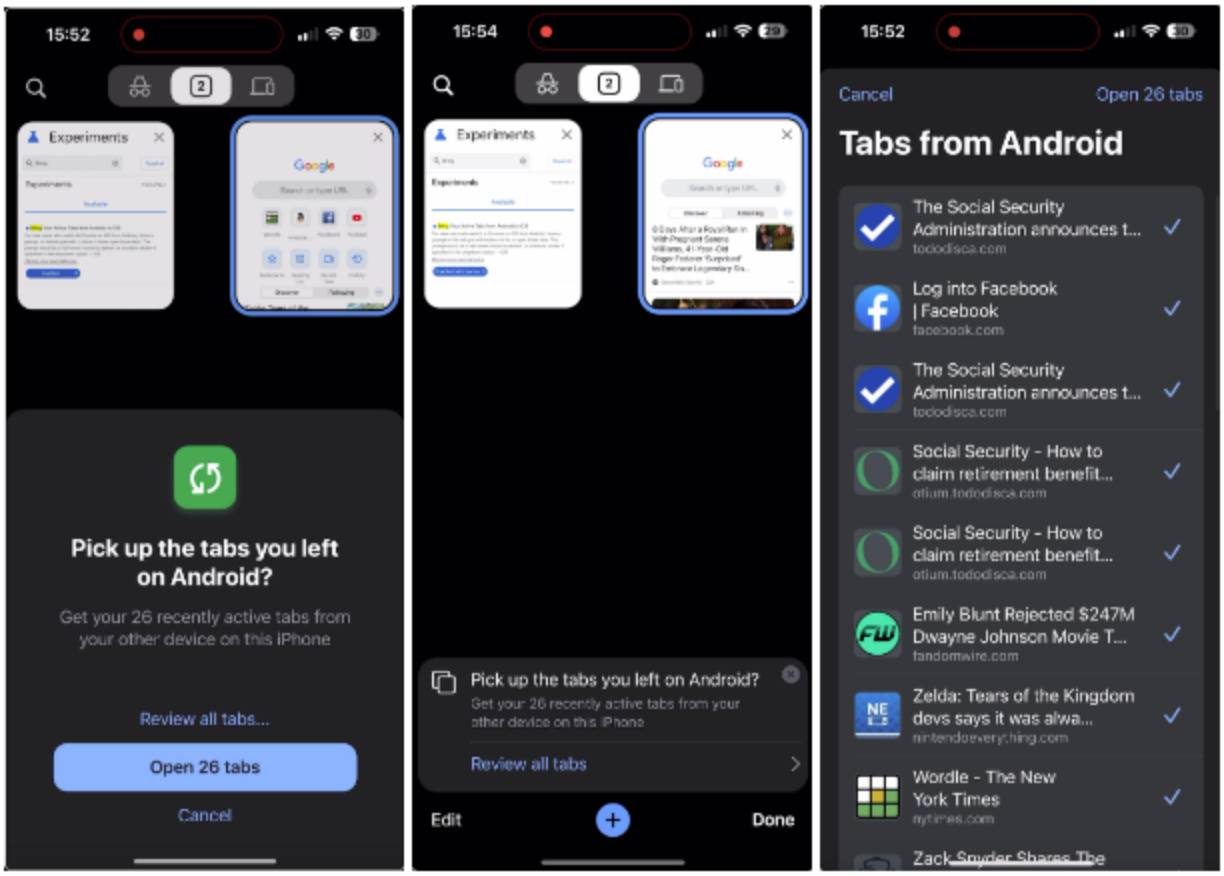
1. SyncDisabled: Disables the entire Chrome Sync infrastructure, including settings.
2. SyncTypesListDisabled: Disables specified individual Sync data types. The existing value *preferences* covers settings.

Side Panel API

Manifest V3 extensions can now add their own side panel to Chrome's built-in side panel UI. See the SidePanel API Chrome developers article for usage and examples.

Pick up where you left off on Android

Chrome on iOS now lets new users re-open multiple tabs that were recently active and open on their Android device. This means that they can easily resume journeys on their new iOS instance of Chrome.

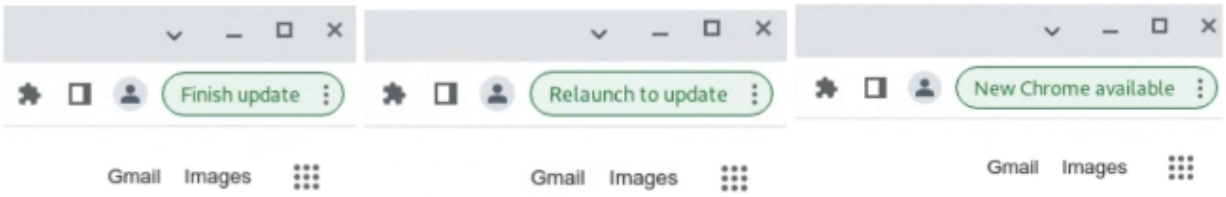


Chrome Enterprise profiles signout

A bug has been fixed where managed profiles became unmanaged and triggered the profile separation dialog all over again for a previously managed profile. This fix ensures that managed profiles do not inadvertently get signed out from Chrome.

Update chip on desktop

In Chrome 114, we are experimenting with new strings in the *Update chip on desktop.* We have refreshed the update strings in the three-dots menu to encourage users to apply updates (and restart) quicker.



New and updated policies in Chrome browser

Policy	Description
ChromeRootStoreEnabled	Determines whether the Chrome Root Store and built-in certificate verifier will be used to verify server certificates. Now available on Mac, Linux and ChromeOS.
InsecureHashesInTLSHandshakesEnabled	Insecure Hashes in TLS Handshakes Enabled

Removed policies in Chrome browser

Policy	Description
CECPQ2Enabled	CECPQ2 post-quantum key-agreement enabled for TLS
ChromeAppsEnabled	Extend support for Chrome Apps on Microsoft® Windows®, macOS, and Linux

ChromeOS updates

Cursive pre-installed for Enterprise and Education accounts

Cursive, a stylus-first notes app, is now available for Chromebook. It will be pre-installed for all Enterprise and Education accounts on stylus-enabled Chromebooks. If you want to block access to the app, you can prevent Chromebooks in your enterprise from accessing *cursive.apps.chrome*.

Passpoint: Seamless, secure connection to Wi-Fi networks

Starting as early as ChromeOS 114, Passpoint will streamline Wi-Fi access and eliminate 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.

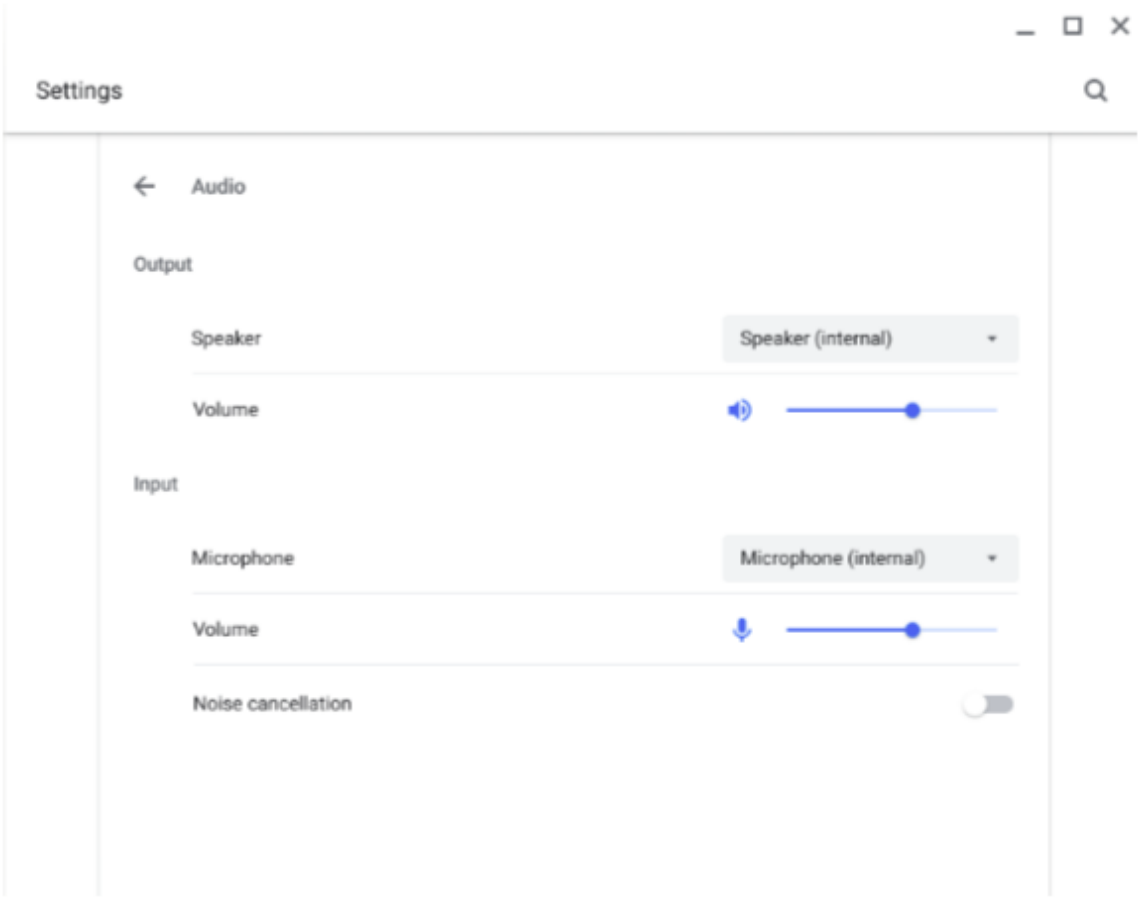
Mandatory extensions for Incognito navigation

In Chrome OS 114, **Extensions** allow admins to enforce security features and customizations in their OU but they cannot be enforced in Incognito mode without user consent. This can be a problem as users can bypass extension-set features, for example, proxies by using Incognito mode for navigation.

The MandatoryExtensionsForIncognitoNavigation policy allows you to configure a list of extensions that users need to explicitly allow to run in Incognito, to use Incognito mode for navigation.

Audio controls visibility

Settings on ChromeOS now have a more native OS settings experience housed in the **Settings** app, available through App Launcher or the cog icon in the Quick Settings menu. In ChromeOS 114, users can now find all sound controls in the ChromeOS Settings app.



ChromeVox earcons

ChromeVox is the built-in screen reader on Chromebooks. In ChromeOS 114, an audio indicator (an *earcon*) now plays when a user with ChromeVox enabled uses the ChromeVox keyboard shortcut to toggle selection on or off.

Admin console updates

Chrome Browser Cloud Management (CBCM) subscription

In Chrome 114, the Chrome Browser Cloud Management subscription is automatically added to all organizations previously using CBCM without the subscription. This change does not

add any new cost to your existing account and you don't need to do anything. There is no action required on your end (learn more).

New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
WebRtcTextLogCollectionAllowed	User	Chrome (Linux, Mac, Windows) ChromeOS	User experience
InsecureHashesInTLSHandshakesEnabled	User, Managed Guest Session	Chrome (Android) Chrome (Linux, Mac, Windows) ChromeOS	Security
CalendarIntegrationEnabled	User	ChromeOS	Content
ChromeAppsWebViewPermissiveBehaviorAllowed	User	Chrome (Linux, Mac, Windows) ChromeOS	Legacy Site Compatibility
WallpaperGooglePhotosIntegrationEnabled	User	ChromeOS	Sign-in 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

HTTP requests upgraded to HTTPS in Chrome 115

As early as Chrome 115, some users may 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 improves your users' security.

Some server configurations may cause issues, for example if different content is served via HTTP and HTTPS. Users can disable automatic upgrading for a specific site by changing the **Insecure Content** site setting to enabled, accessible via Page Info or `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 internal 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`. Please report any issues you encounter.

Chrome policy: disable extensions unpublished from Chrome Web Store (CWS)

As early as Chrome 115, we will release the Enterprise policy **ExtensionUnpublishedAvailability** to disable extensions that have been unpublished from the Chrome Web Store.

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, as early as Chrome 115. 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.

master_preferences to initial_preferences migration

As part of Chrome's ongoing transition to use more inclusive naming, the example in the Enterprise bundle has been renamed from `master_preferences` to `initial_prefereces`. While there are no changes in Chrome's interpretation of the file, the following fields are no longer present in the `initial_preferences` example 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

Release cycle changes

Chrome 115 stable release will be moved from June 27 to July 18. All dates after this have been adjusted to account for this delay. Please see the Chromium Dash Schedule for updated dates.

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 will be able to use and save bookmarks and reading list items in their Google Account. Relevant enterprise policies such as BrowserSignin, SyncDisabled, SyncTypesListDisabled, EditBookmarksEnabled and ManagedBookmarks will continue to work as before and can be used to configure whether users use and save items in their Google Account.

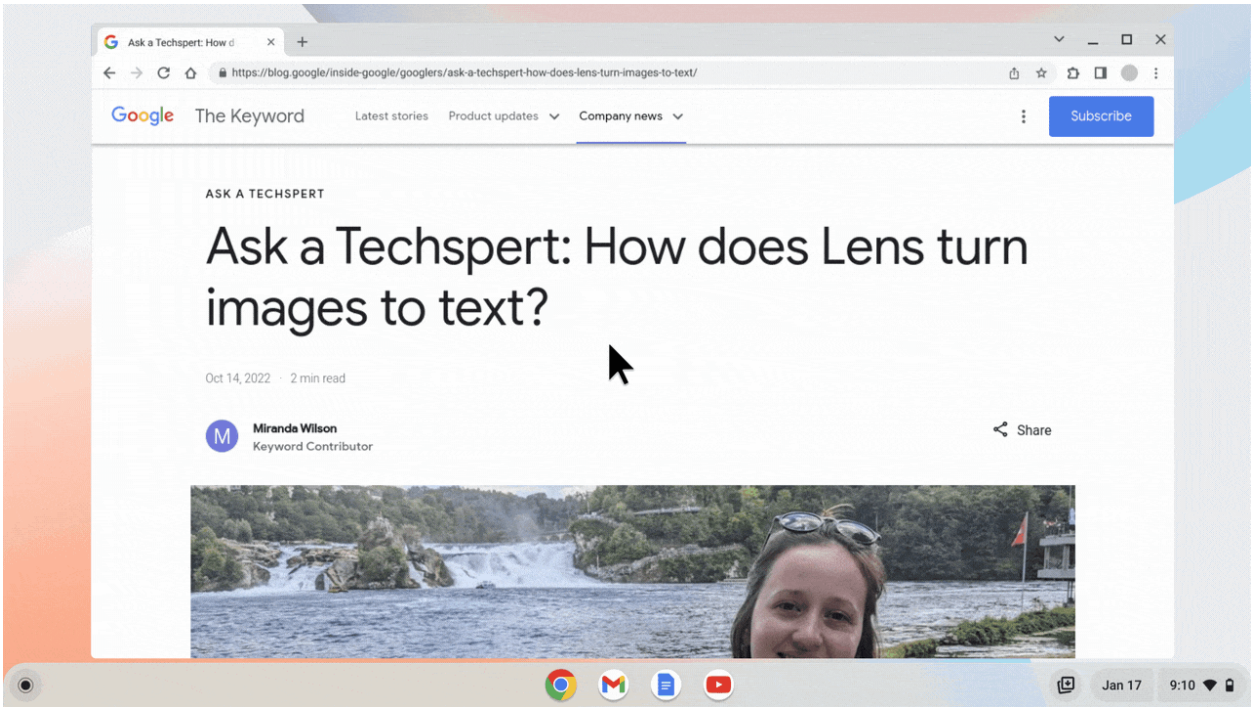
Update for Secure DNS / Cox ISP users

For clients running on systems that use the Cox ISP DNS servers, if the DnsOverHttpsMode policy is set to "Automatic", then secure DNS queries will be used by Chrome 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, we're adding a new feature to help improve the online reading experience. Introducing reading mode, a new feature on Chrome browser, 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/background color, and more, making for a more cohesive, intuitive, and comfortable reading experience.



Anti-phishing telemetry expansion

In this feature, we log user-interaction data to Chrome servers and to Safe Browsing servers that 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.

Deprecating the use of SHA1 in server signatures in TLS

Chrome 115 is removing support for signature algorithms using SHA-1 for server signatures during the TLS handshake. This does not affect SHA-1 support in server certificates, which

was already removed, or in client certificates, which continues to be supported. SHA1 has known collisions, has been deprecated by the IETF, and should be avoided.

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). Starting in Chrome 115, we will automatically disable sync for the respective data types and will no longer require admins to set the dependent policy.

Web MIDI permission prompt

Starting Chrome 116, the Web MIDI API access will be gated behind a permissions prompt. Currently, the use of SysEx messages with the Web MIDI API requires an 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 users' access to the API.

X25519Kyber768 key encapsulation for TLS

As early as Chrome 116, Chrome is introducing 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 may 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 enterprise policy. However, long term, post-quantum secure ciphers will be required in TLS.

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.

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.

Enable access to WebUSB API from extension service workers in Chrome 116

As early as Chrome 116, 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.

Removal of the RendererCodeIntegrityEnabled policy

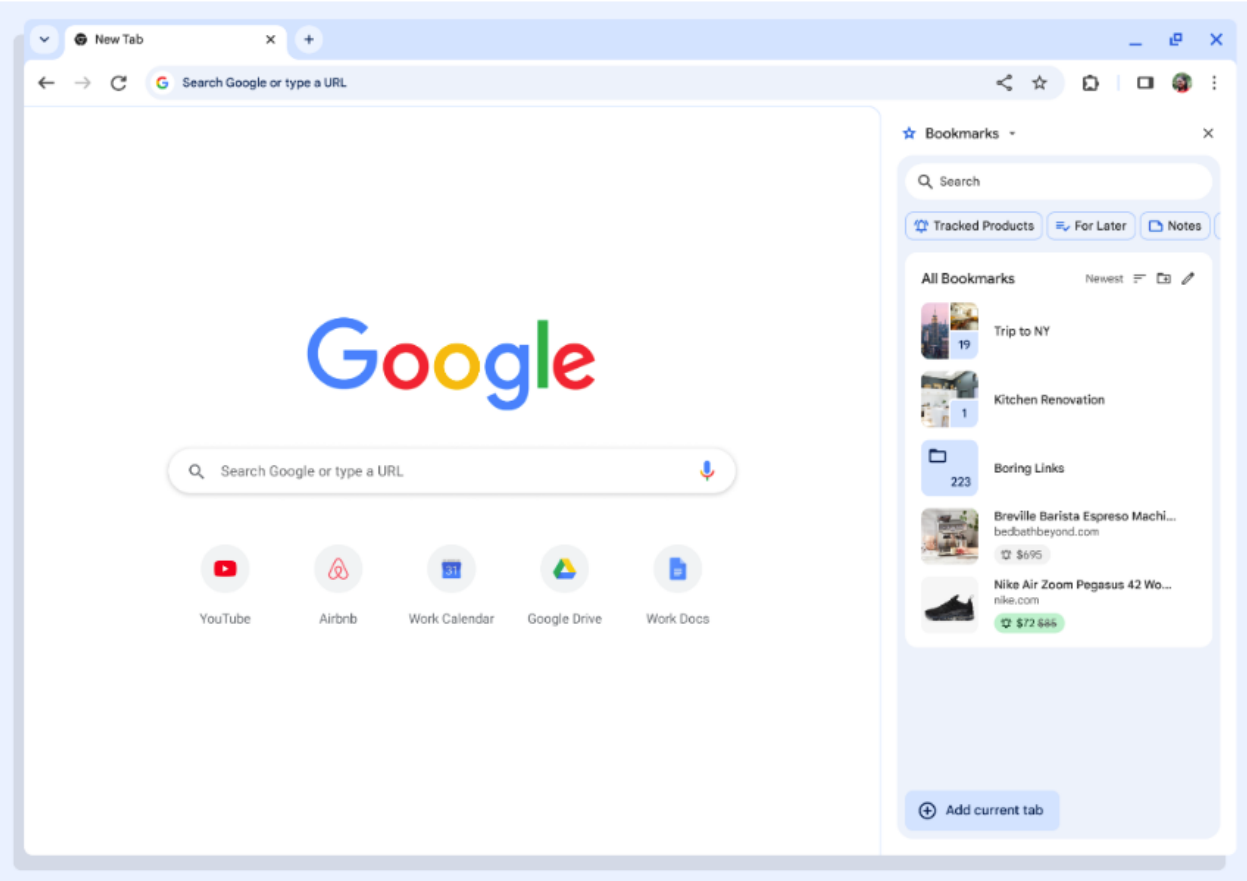
As early as Chrome 117, the RendererCodeIntegrityEnabled policy will be removed. You can verify whether your third party software works by no longer applying the policy. You can report any issues you encounter by submitting a bug here.

Chrome 117 will no longer support macOS 10.13 and macOS 10.14

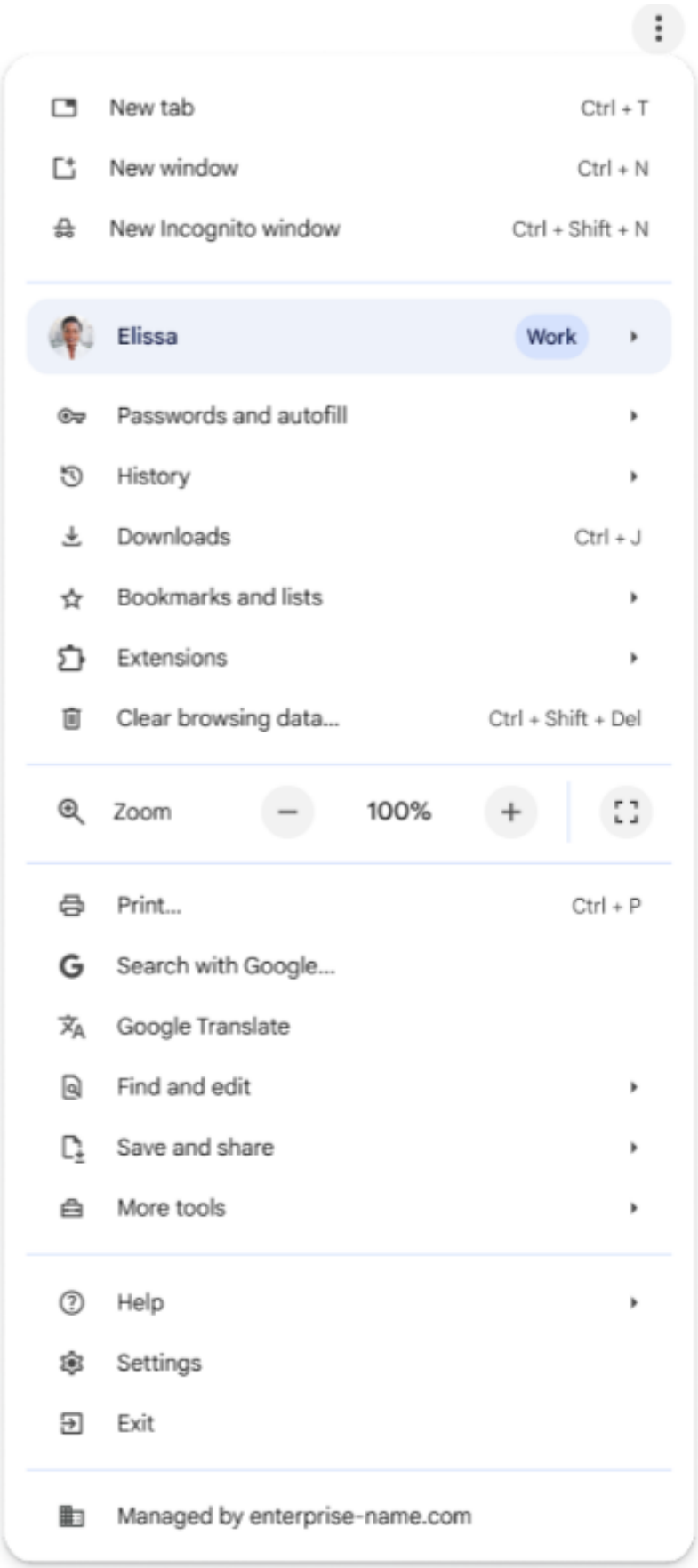
Chrome 117 will no longer support macOS 10.13 and macOS 10.14, which are already outside of their support window with Apple. Users have to update their operating systems in order to continue running Chrome browser. Running on a supported operating system is essential to maintaining security. Starting in Chrome 114, you'll see 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 with Google...
Google Translate
Find and edit
Save and share
More tools
Help
Settings
Exit
Managed by enterprise-name.com

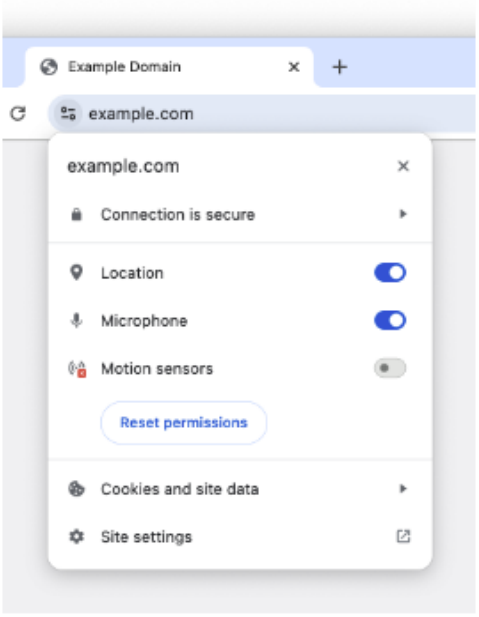
v

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, which releases in early September 2023, 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.

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.

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.

Upcoming ChromeOS changes

App Streaming on ChromeOS

As early as ChromeOS 115, App Streaming will enhance 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 will kick off an app stream directly to the user's ChromeOS desktop. This is part of a Google-wide ambient computing effort.

Google Photos Shared Albums

In ChromeOS 104, we let users use Google Photos for Wallpapers and Screensavers, but we restricted access to Shared Albums due to privacy concerns. In Chrome 115, we will address these privacy concerns to allow users to select photos from Shared Albums.

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.

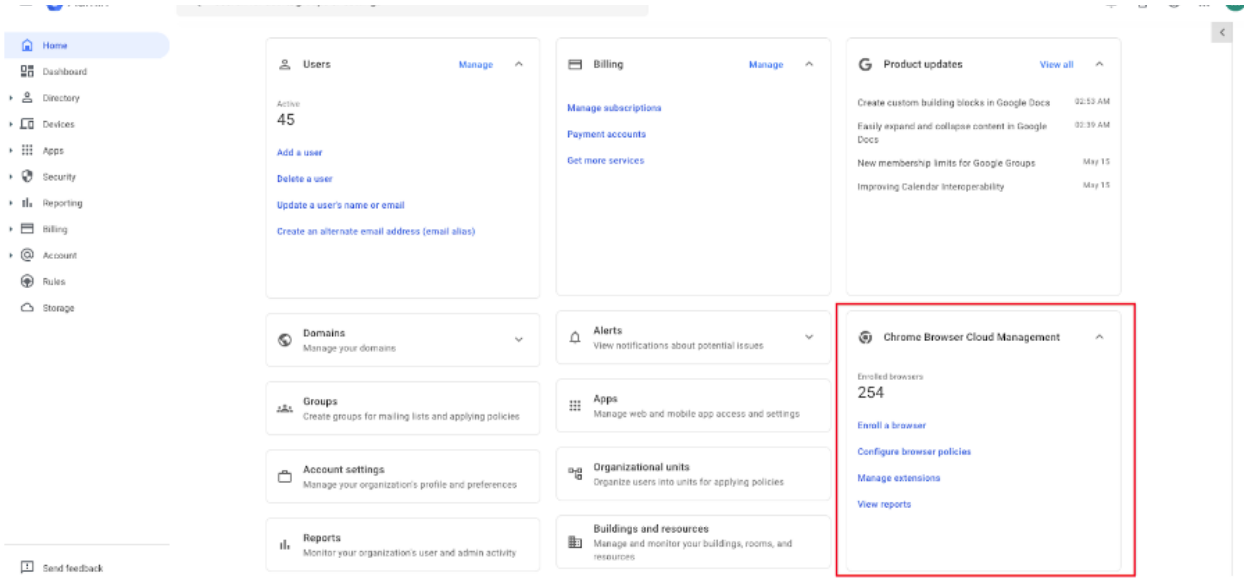
A temporary enterprise policy ChromeAppsWebViewPermissiveBehaviorAllowed will be available to give enterprises time to address possible breakage related to these changes. To test whether this change is the cause of any breakage, without needing to set the enterprise policy, the previous behavior from 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.

Upcoming Admin Console changes

New Chrome Browser Cloud Management card

Chrome is launching a new Chrome Browser Cloud Management card on the homepage of the Google Admin console. You will be able to easily access and find popular Chrome browser management tasks, directly on the homepage.



Previous release notes

Chrome version & targeted Stable channel release date	PDF
Chrome 113: Jan 10, 2023	PDF
Chrome 112: Mar 29, 2023	PDF
Chrome 111: Mar 01, 2023	PDF
Chrome 110: Feb 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