Chrome 112 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 March 29, 2023.

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

Chrome 112 release summary

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	**Security/ Privacy**	**User productivity /Apps**	**Management**
Enable access to WebHID API from extension service workers		✓	
Unused site permissions module in safety check	✓		
Default to origin-keyed agent clustering	✓		
Chrome apps no longer supported on Windows, Mac, and Linux		✓	
Auto-upgrade mixed content to HTTPS	✓		
Chrome Root Store updates and removal of the ChromeRootStoreEnabled policy	✓		✓
Updated onboarding experience		✓	
Policy troubleshooting page available on Android		✓	
Changes to HTTPS policies			✓
Add websites and PWAs to the home screen on iOS		✓	
New Chrome Sync data types available in Takeout	✓		
Autofill on iOS		✓	
Android WebView phases out X-Requested-Header starting from version 112	✓		
Web auth flow to use browser tab instead of App window	✓		
Chrome for Testing		✓	

Price tracking on iOS		✓	
New and updated policies in Chrome browser			✓
ChromeOS updates	**Security/ Privacy**	**User productivity /Apps**	**Management**
Screencast supports multi-language transcription in recordings		✓	
Fast Pair saved devices		✓	
Introducing the Rupee symbol on US-English keyboards in India		✓	
Screen Capture shows clicks and keyboard shortcuts		✓	
Admin console updates	**Security/ Privacy**	**User productivity /Apps**	**Management**
New Chrome browser insights			✓
New policies in the Admin console			✓
Upcoming Chrome browser changes	**Security/ Privacy**	**User productivity /Apps**	**Management**
Changes to phishing protection on Android as early as Chrome 113	✓		
Deprecation trial for unpartitioned 3rd party Storage, Service Workers, and Communication APIs	✓		
Extensions must be updated to leverage Manifest V3		✓	✓
First-Party Sets user controls	✓		
Removal of permissive Chrome Apps webview behaviors	✓		
Collect additional data for off-store extensions in telemetry reports	✓		
Launching FastCheckout for Checkout experiences		✓	
Updated Password Management Experience on iOS in		✓	

Chrome 113			
New inactive tabs section in the Chrome app on iPhone and iPad		✓	
Image-set css changes	✓		
Support for Private State Tokens	✓		
Enable access to WebUSB API from extension service workers in Chrome 113		✓	
Changes to Google Password Manager in Chrome 114		✓	
Updates to Bookmarks on Desktop		✓	
Network Service on Windows will be sandboxed	✓		
Chrome 117 will no longer support macOS 10.13 and macOS 10.14	✓		
Upcoming ChromeOS changes	**Security/ Privacy**	**User productivity /Apps**	**Management**
Cursive pre-installed for Enterprise and Education accounts		✓	
Screensaver preview		✓	
Passpoint: Seamless, secure connection to Wi-Fi networks	✓	✓	
Upcoming Admin console changes	**Security/ Privacy**	**User productivity /Apps**	**Management**
Risk Assessment card		✓	✓
Device Token Management policy for device token deletion			✓

Current Chrome version release notes

Chrome browser updates

Enable access to WebHID API from extension service workers

Chrome 112 enables access to the WebHID API from extension service workers, as a migration path for Manifest V2 extensions that currently access the API from a background page.

Unused site permissions module in safety check

Chrome's safety check can confirm the overall security and privacy of the browsing experience. It tells you if any passwords saved in Chrome have been compromised, flags dangerous extensions, and helps you ensure that your security protections are up to date.

Starting with Chrome 112, safety check includes auto-revocation of unused site permissions on Chrome. Chrome resets permissions from sites that users have not visited for a while. Chrome revokes permissions automatically and offers options to opt out or re-grant. Permissions granted by enterprise policies are not affected.

Default to origin-keyed agent clustering

Starting in Chrome 112, websites can no longer set `document.domain`. Websites now need to use alternative approaches such as `postMessage()` or Channel Messaging API to communicate cross-origin. If a website relies on same-origin policy relaxation via `document.domain` to function correctly, it now needs to send an `Origin-Agent-Cluster: ?0` header along with all documents that require that behavior. You can read more in this blog post.

Note: `document.domain` has no effect if only one document sets it.

The OriginAgentClusterDefaultEnabled enterprise policy allows you to extend the current behavior.

Chrome apps no longer supported on Windows, Mac, and Linux

As previously announced, we are phasing out support for Chrome apps in favor of Progressive Web Apps (PWAs) and web-standard technologies. The deprecation schedule was adjusted to provide enterprises who used Chrome apps additional time to transition to other technologies, and Chrome apps will now stop functioning in Chrome 112 or later on Windows, Mac, and Linux. If you need additional time to adjust, a policy ChromeAppsEnabled will be available to extend the lifetime of Chrome Apps an additional 2 milestones.

Starting in Chrome 105, if you're force-installing any Chrome apps, users are shown a message stating that the app is no longer supported. The installed Chrome Apps are still launchable.

Starting with Chrome 112, Chrome Apps on Windows, Mac and Linux no longer work. To fix this, remove the extension ID from the force-install extension list, and if necessary, add the corresponding **install_url** to the web app force install list. For common Google apps, the **install_urls** are listed below:

Property	**Extension ID** (Chrome App)	**install_url** (PWA / Web App)
Gmail	pjkljhegncpnkpknbcohdijeoejaedia	https://mail.google.com/mail/installwebapp?usp=admin
Docs	aohghmighlieiainnegkcijnfilokake	https://docs.google.com/document/installwebapp?usp=admin
Drive	apdfllckaahabafndbhieahigkjlhalf	https://drive.google.com/drive/installwebapp?usp=admin
Sheets	felcaaldnbdncclmgdcncolpebgiejap	https://docs.google.com/spreadsheets/installwebapp?usp=admin
Slides	aapocclcgogkmnckokdopfmhonfmgoek	https://docs.google.com/presentation/installwebapp?usp=admin
Youtube	blpcfgokakmgnkcojhhkbfbldkacnbeo	https://www.youtube.com/s/notifications/manifest/cr_install.html

Auto-upgrade mixed content to HTTPS on iOS

Chrome 112 on iOS starts automatically upgrading passive mixed content (HTTP image, audio and video on HTTPS pages) to HTTPS, when possible. Previously, Chrome on iOS blocked passive mixed content. All other Chrome platforms auto-upgrade passive mixed content, when possible. An enterprise policy, MixedContentAutoupgradeEnabled, is available to disable mixed content auto-upgrading on HTTPS sites on iOS. The policy will be removed in Chrome 116.

Chrome Root Store updates and removal of the ChromeRootStoreEnabled policy

Chrome 112 now enforces name constraints on root certificates. This matches the behavior prior to the launch of the Chrome Root Store in Chrome 106. If you previously disabled the Chrome Root Store to work around this issue, you can test again with Chrome 112. If you relied on Chrome not enforcing name constraints, we have provided a temporary EnforceLocalAnchorConstraintsEnabled policy to disable this behavior. This policy will be removed in the future.

As early as Chrome 113, to improve user security and provide a consistent experience across different platforms, Chrome will switch to its own default root store and built-in certificate verifier on Android, Linux, and ChromeOS. 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. The Chrome Root Store is already default enabled on Windows and Mac.

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.

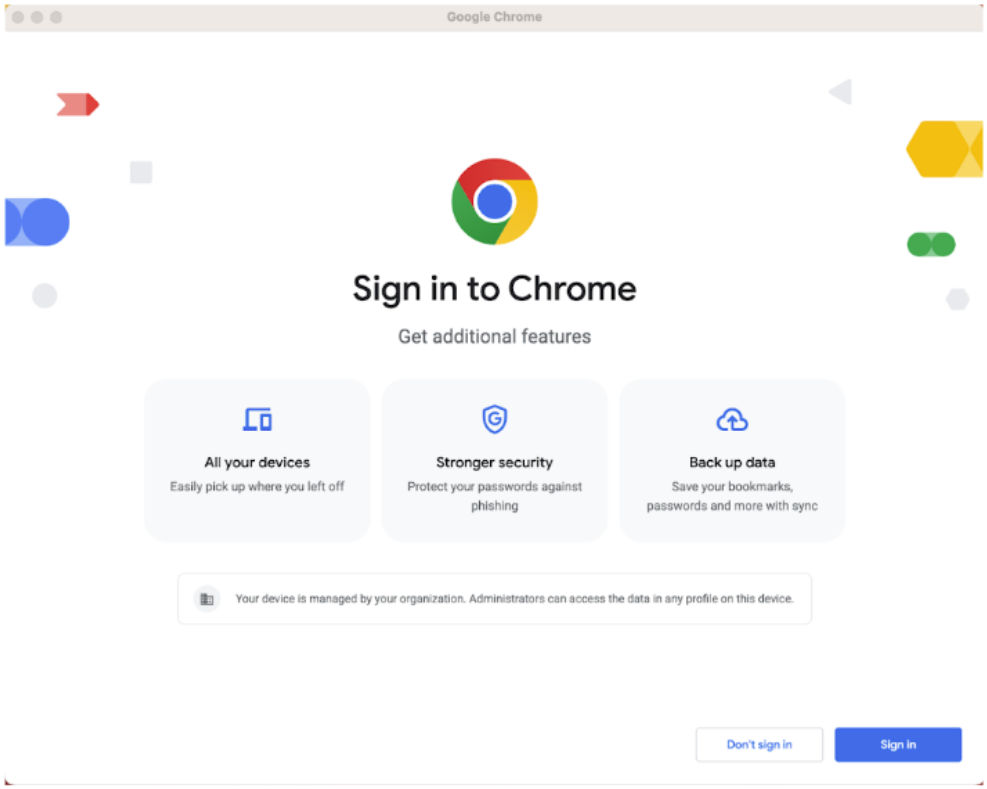
The ChromeRootStoreEnabled policy allows selective disabling of the Chrome Root Store in favor of the platform root store. You can set this policy to Disabled to force the use of the platform root store, otherwise it is enabled by default. The policy will be made available on **Android, Linux, and ChromeOS**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

The ChromeRootStoreEnabled policy will be removed from **Windows and Mac** on Chrome 113. Support for trusted leaf certificates and the Windows Trusted People store was added

for Chrome 111. If you previously disabled the Chrome Root Store to work around either of these issues, you can test again with Chrome 112.

Updated onboarding experience

In Chrome 112, some users see a simplified onboarding experience with a more intuitive way to sign into Chrome. Enterprise policies like BrowserSignin, SyncDisabled, RestrictSigninToPattern and SyncTypesListDisabled continue to be available as before to control whether the user can sign into Chrome and turn on sync. You can use the PromotionalTabsEnabled policy to skip onboarding altogether.



Policy troubleshooting page available on Android

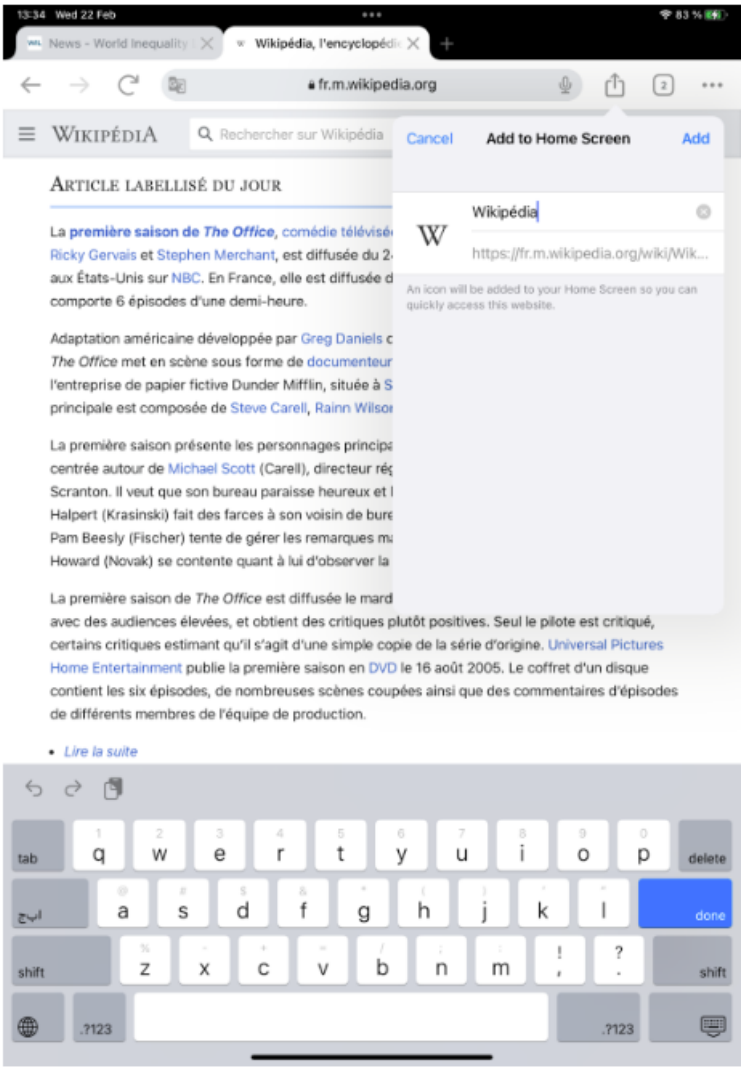
`chrome://policy/logs` is a new page that admins can use to help troubleshoot enterprise policies on Android. On iOS, this will become available in Chrome 113.

Changes to HTTPS policies

The HttpsOnlyMode policy now supports *force_enabled*. This enables the **Always use secure connections** setting on `chrome://settings/security` and prevents the user from disabling it. The setting causes a bypassable error interstitial to be displayed before any navigation to a non-HTTPS site. Users can always bypass the error interstitial, and the decision to bypass is remembered for one week. We've also added the HttpAllowlist policy, which you can use to define a list of hosts or hostname patterns that are allowed to be non-HTTPS without an error interstitial. For example, you can use the HttpAllowlist policy to allowlist internal sites that might be HTTP-only.

Add websites and PWAs to the home screen on iOS

Starting in Chrome 112, you can bookmark a website on the iOS device's home screen. If the website offers a Progressive Web Apps (PWAs), then this action adds the app to the home screen. Otherwise, the bookmark opens in the default browser when you tap it. This feature is available to iOS16.4 and above.



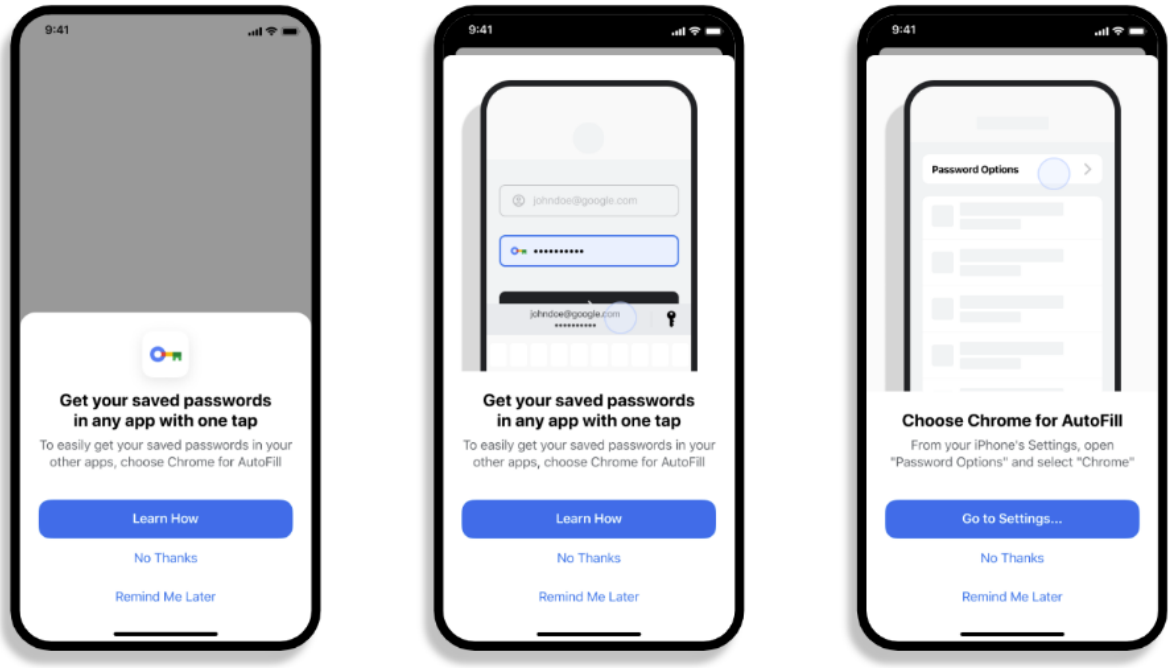
New Chrome Sync data types available in Takeout

In Chrome 112, additional Chrome data is available to export in Takeout and Domain Wide Takeout (DWT). The following data types are available: AUTOFILL, PRIORITY_PREFERENCE, WEB_APP, DEVICE_INFO, TYPED_URL, ARC_PACKAGE, OS_PREFERENCE, OS_PRIORITY_PREFERENCE, PRINTER.

You can control which data types are synced to Chrome Sync using the SyncTypesListDisabled enterprise policy. Instructions on allowing or blocking Takeout can be found in this help center article.

Autofill on iOS

In Chrome 112, some iOS users see a prompt to choose Chrome for Autofill in their iOS settings. The user can choose to learn more, dismiss the prompt forever, or be reminded again later. The prompt can appear after the user has copied a password from the Chrome password manager, saved a password, or logged into a website using an existing saved password. An enterprise policy, CredentialProviderPromoEnabled, is available to disable any appearance of the prompt.



Android WebView phases out the X-Requested-Header starting from version 112

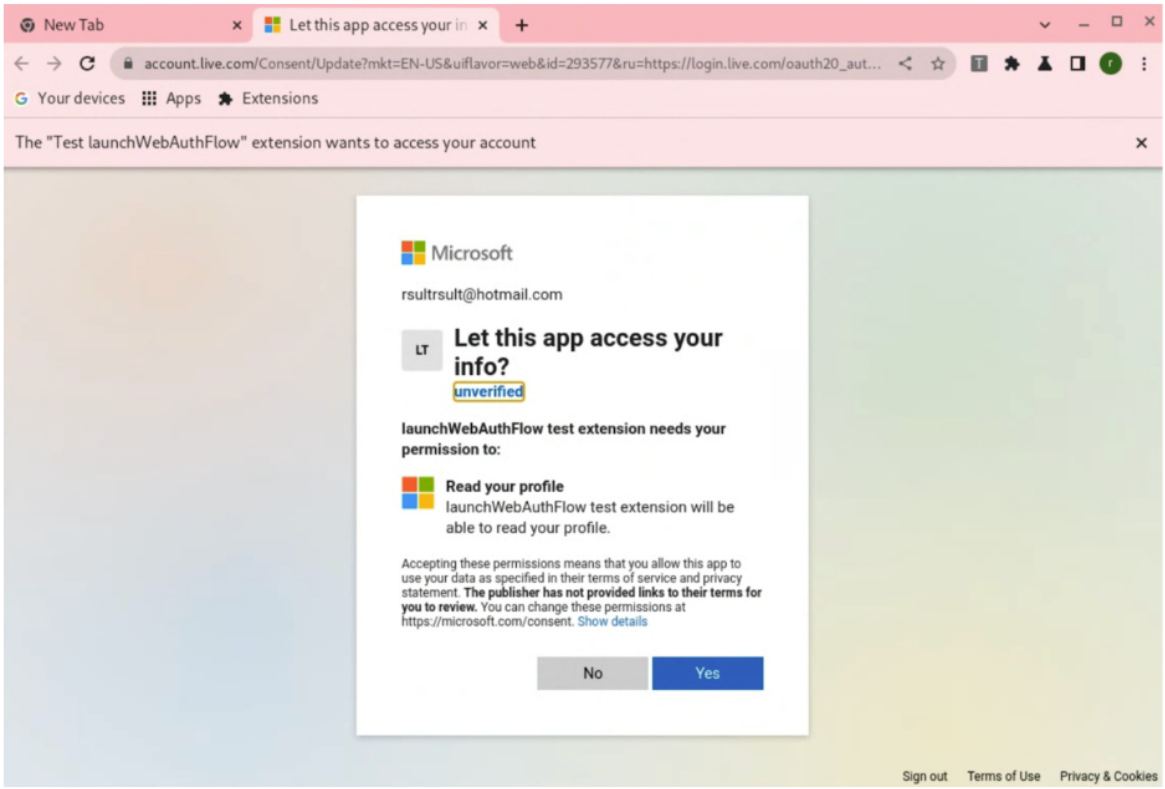
To improve privacy, Android WebView begins phasing out the X-Requested-With HTTP request header. Sites that currently rely on this header can sign up for the Deprecation Origin Trial, which will allow them to continue to receive the header. The deprecation trial is planned to run for at least one year, but will continue until replacement APIs have been launched to address the current use cases for the header. Apps can also enable the header for individual

destination origins by using a newly introduced AndroidX API. Using this API will continue to provide the header to sites past the end of the deprecation trial.

Web auth flow to use browser tab instead of App window

In Chrome 112, the authorization page for web auth flow in Chrome extensions now displays either in a new tab or a popup window. This change concerns two API methods: launchWebAuthFlow and getAuthToken. It resolves several existing UX problems:

- the authorization page now displays a URL which protects against phishing attacks.
- sign-in state is now shared with all browser tabs; no need to sign-in into extension separately.
- sign-in state is persisted on Chrome restart.
- fixed accessibility issues of App window.



Chrome for Testing

In Chrome 112, Puppeteer, Chrome's browser automation library, uses the **Chrome for Testing** binary instead of a Chromium binary. In case you have the Chromium binary allowlisted, you can allowlist the **Chrome for Testing** binary too.

Chrome for Testing is a dedicated Chrome flavor for the automated testing use case. It's not an end-user facing product, but rather a tool to be used by automation engineers through other projects such as Puppeteer. **Chrome for Testing** is a completely separate binary from *regular* Chrome.

Price tracking on iOS

Chrome 112 on iOS enables users to track the prices of products across the web, and receive notifications when the price drops. An enterprise policy, ShoppingListEnabled, is available to control this shopping feature.

New and updated policies in Chrome browser

Policy	Description
ChromeVariations	Determine the availability of variations (now available on Android).
HttpAllowlist	Disable HTTPS upgrades for some hostnames, potentially decreasing user security.
HttpsUpgradesEnabled	Enable automatic HTTPS upgrades.
EnforceLocalAnchorConstraintsEnabled	Determines whether the built-in certificate verifier will enforce constraints encoded into trust anchors loaded from the platform trust store.
ExtensionExtendedBackgroundLifetimeForPortConnectionsToUrls	Configure a list of origins that grant extended background lifetime to the connecting extensions.
ShoppingListEnabled	Allow the shopping list feature to be enabled (now available on iOS).

CredentialProviderPromoEnabled	Allows users to be shown the Credential Provider Extension promo.

ChromeOS updates

Screencast supports multi-language transcription in recordings

ChromeOS 112 dramatically expands **Screencast** recording capabilities by including a wide range of languages by integrating with Google's **S3** transcription API.

The **Screencast** app for ChromeOS lets users record transcribed screencasts on their Chromebook. In previous versions, this feature was available in EN-US only, which meant that only English speaking users in the US could record screencasts. Soon, it will be possible to record and transcribe screencasts in a wide range of languages including Spanish, Japanese, French, Italian, and German.

Fast Pair saved devices

ChromeOS 112 adds a subpage to Fast Pair settings for saved devices, where users can view their device associations, remove any that may be unwanted, and configure whether they want Fast Pair-paired devices to automatically save to their account. This experience mirrors the management capabilities already available for Fast Pair on Android today, and was explicitly requested as a fast-follow improvement by the ChromeOS Privacy team.

Introducing the Rupee symbol on US-English keyboards in India

ChromeOS 112 adds the Rupee symbol ₹ to both the virtual keyboard and the physical keyboard, where AltGr+4 is the rupee symbol (hold right-alt + 4).

The compact virtual keyboard just moves some currency keys around so that you can access the Rupee symbol in the **more symbols** menu. For accessibility, the virtual keyboard has the AltGr layer toggle available, which lets you type AltGr+4 and get the rupee symbol.

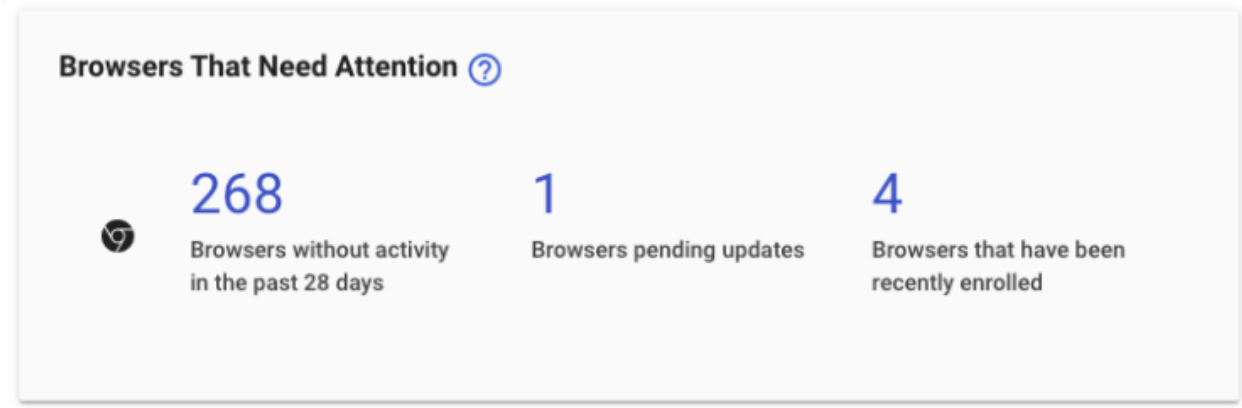
Screen Capture show clicks and keyboard shortcuts

You can now enhance demos made with **Screen Capture** by enabling users to show clicks and keyboard shortcuts on screen.

Admin console updates

New Chrome browser insights

In Chrome 112, a new **Browsers that need attention** insights card allows IT admins to quickly identify browsers that have a pending Chrome update, browsers that are inactive and browsers that have recently enrolled.



New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
PrivacySandboxSiteEnabledAdsEnabled	User & Browser Settings	Chrome (Linux, Mac, Windows) ChromeOS, Android	Security > Privacy Sandbox>Control whether privacy sandbox prompts.
PrivacySandboxPromptEnabled	User & Browser Settings	Chrome (Linux, Mac, Windows) ChromeOS, Android	Security > Controls whether the Privacy Sandbox Site-suggested ads setting can be disabled for your users.
PrivacySandboxAdTopicsEnabled	User & Browser Settings	Chrome (Linux, Mac, Windows) ChromeOS, Android	Security >Controls whether your users see the Privacy Sandbox prompt.
PrivacySandboxAdMeasurementEnabled	User & Browser Settings	Chrome (Linux, Mac, Windows) ChromeOS, Android	Security >Controls whether the Privacy Sandbox Ad measurement setting can be disabled for your users.

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

Changes to phishing protection on Android as early as Chrome 113

When a user authenticates to Android with their Google password, for example, during account setup, Chrome will be notified so the password can begin receiving phishing protection when surfing the Web with Chrome. In previous versions of Chrome on Android, users needed to explicitly provide their password within a Chrome tab, for example, sign in to Gmail, to receive phishing protection for their Google password.

You can disable warnings regarding password reuse by setting PasswordProtectionWarningTrigger to 0.

Deprecation Trial for Unpartitioned third-party Storage, Service Workers, and Communication APIs

Beginning gradually in Chrome 113, storage, service workers, and communication APIs will be partitioned in third-party contexts. In addition to being isolated by the same-origin policy, the affected APIs used in third-party contexts would also be separated by the site of the top-level context. Sites that haven't had time to implement support for third-party storage partitioning can take part in a deprecation trial to temporarily **unpartition** (continue isolation by same-origin policy but remove isolation by top-level site) and restore prior behavior of storage, service workers, and communication APIs in content embedded on their site.

The following APIs will remain unpartitioned in third-party contexts should you enroll the top-level site in the **DisableThirdPartyStoragePartitioning** deprecation trial: Storage APIs (such as localStorage, sessionStorage, IndexedDB, Quota, and so on), Communication APIs (such as BroadcastChannel, SharedWorkers, and WebLocks), and ServiceWorker API.

Chrome 113 will also add the **DefaultThirdPartyStoragePartitioningSetting** enterprise policy, which will unpartition APIs in all third-party contexts, as well as **ThirdPartyStoragePartitioningBlockedForOrigins**, which will unpartition APIs for third-party contexts when the first-party context's origin matches the list. Both will be supported for at least 12 milestones. You can read more in the 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 will be 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.

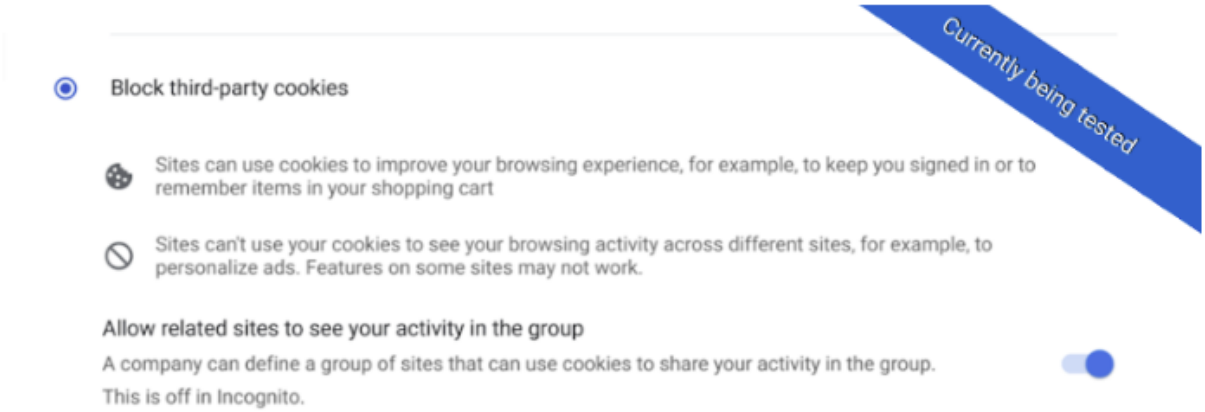
First-Party Sets user controls

First-Party Sets is an upcoming framework for developers to declare relationships between domains, such that the browser can make decisions regarding access based on the third

party's relationship to the first party. A set may enjoy first party benefits, including continued access to their cookies when the top-level domain is in the same set.

First-Party Sets are part of Chrome's roadmap for a more privacy-focused web.

Chrome 113 will introduce user controls for these First-Party Sets. Two enterprise policies will be made available to manage First-Party sets: one to disable First-Party Sets and one to provide your own sets.



Removal of permissive Chrome Apps webview behaviors

In Chrome 113, Chrome Apps webview usage will have the following restrictions:

1. SSL errors within webview will show an error page that does not provide the user the option to unsafely proceed.
2. The use of the webview NewWindow event to attach to a webview element in another App window will cause the window reference returned by the `window.open` call in the originating webview to be invalidated.

In Chrome 112, you'll be able to test out this new behavior by navigating to `chrome://flags` and enabling the `chrome://flags/#enable-webview-tag-mparch-behavior`.

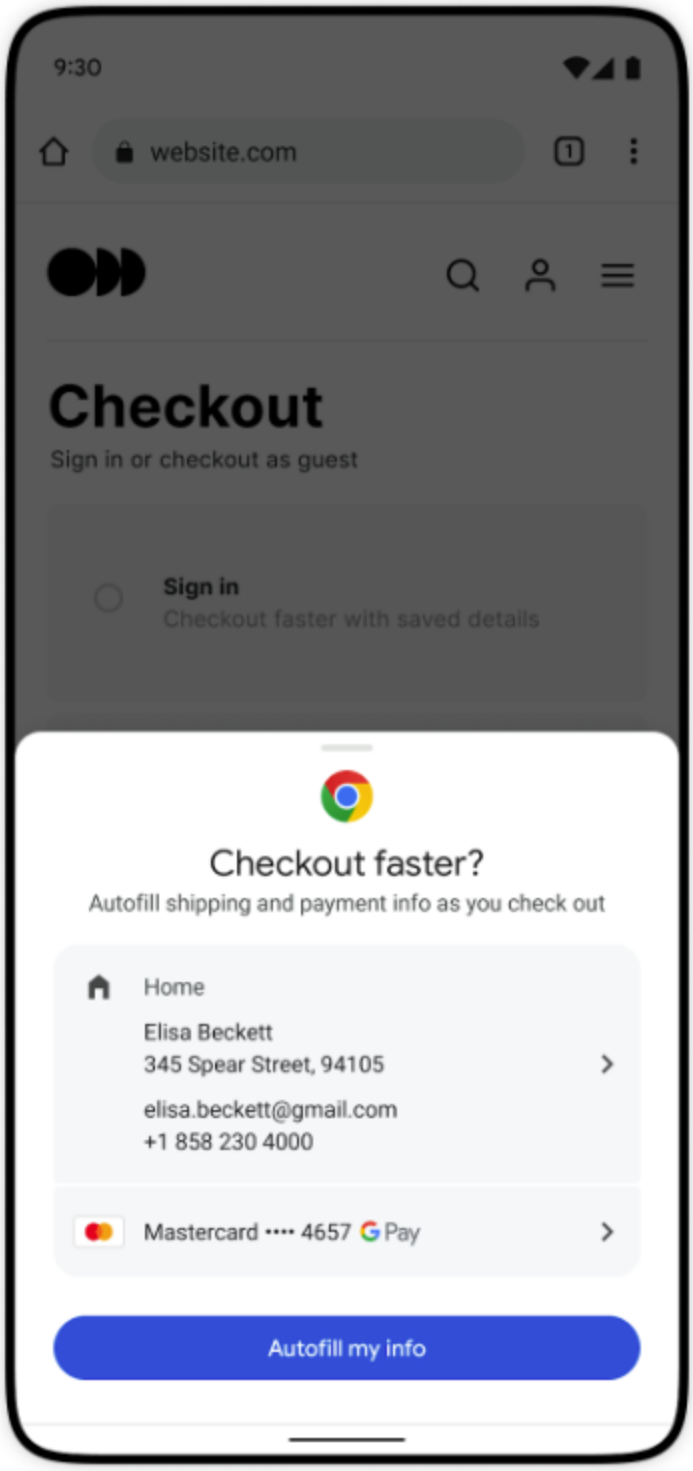
A temporary enterprise policy **ChromeAppsWebViewPermissiveBehaviorAllowed** will be available to give enterprises time to address possible breakage related to these changes.

Collect additional data for off-store extensions in telemetry reports

When Enhanced Safe Browsing is enabled, Chrome 113 will start collecting additional telemetry on off-store extensions, such as file hashes and the `manifest.json` file. The data collected are analyzed on Google servers to detect malicious off-store extensions (including self-hosted extensions) and improve protection for all Chrome extension users. This functionality along with the entire extension telemetry feature can be turned off by setting SafeBrowsingProtectionLevel to any value other than 2; this disables Enhanced Safe Browsing. Enterprise admins can use the SafeBrowsingProtectionLevel policy if they have any concerns about exposing this data.

Launching FastCheckout for Checkout experiences

In Chrome 113, some users will see an updated Autofill UI targeting checkout pages on shopping websites. It can be disabled by either disabling policy AutofillAddressEnabled or AutofillCreditCardEnabled.


9:30
website.com
Checkout
Sign in or checkout as guest
Sign in
Checkout faster with saved details
Checkout faster?
Autofill shipping and payment info as you check out
Home
Elisa Beckett
345 Spear Street, 94105
elisa.beckett@gmail.com
+1 858 230 4000
Mastercard •••• 4657 G Pay
Autofill my info

Updated Password Management Experience on iOS in Chrome 113

On Chrome on iOS, some users who are signed-in to Chrome but don't have Chrome sync enabled will be able to use and save passwords in their Google Account. Relevant enterprise policies such as BrowserSignin, SyncDisabled, SyncTypesListDisabled and PasswordManagerEnabled will continue to work as before and can be used to configure whether users can use and save passwords in their Google Account.

New inactive tabs section in the Chrome app on iPhone and iPad

In Chrome 113, old tabs will be hidden under a new Inactive Tabs section in the Tab grid view. Chrome users will be able to access the inactive tabs section to view all old tabs or close them using the new bulk tab functionality.

Image-set css changes

Chrome 113 implements standard syntax support for image-set and will treat the previously supported `-webkit-` vendor prefix syntax as a parse time alias for the standard. As a result of this, values set with the vendor prefix will serialize as standard.

Example:

```
-webkit-image-set(url(example.png) 1x)
```

Will serialize to:

`image-set(url(""example.png"") 1x)` for specified value (as returned via `getPropertyValue() like: testDiv.style.getPropertyValue(""background-image"");`)

and to

`image-set(url(""example.png"") 1dppx)` for computed value (as returned via `getComputedStyle() like window.getComputedStyle(testDiv)[""background-image""]`).

If needed, the new behavior can be turned off via the `CSSImageSet` runtime flag. The rendering and image-selection behavior will be the same for both the prefixed and standard syntax (Chrome Status).

Support for Private State Tokens

Starting in Chrome 113, the Private State Tokens API will be 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 will be controlled using a new setting in Chrome settings called **Auto-verify**.

Enable access to WebUSB API from extension service workers in Chrome 114

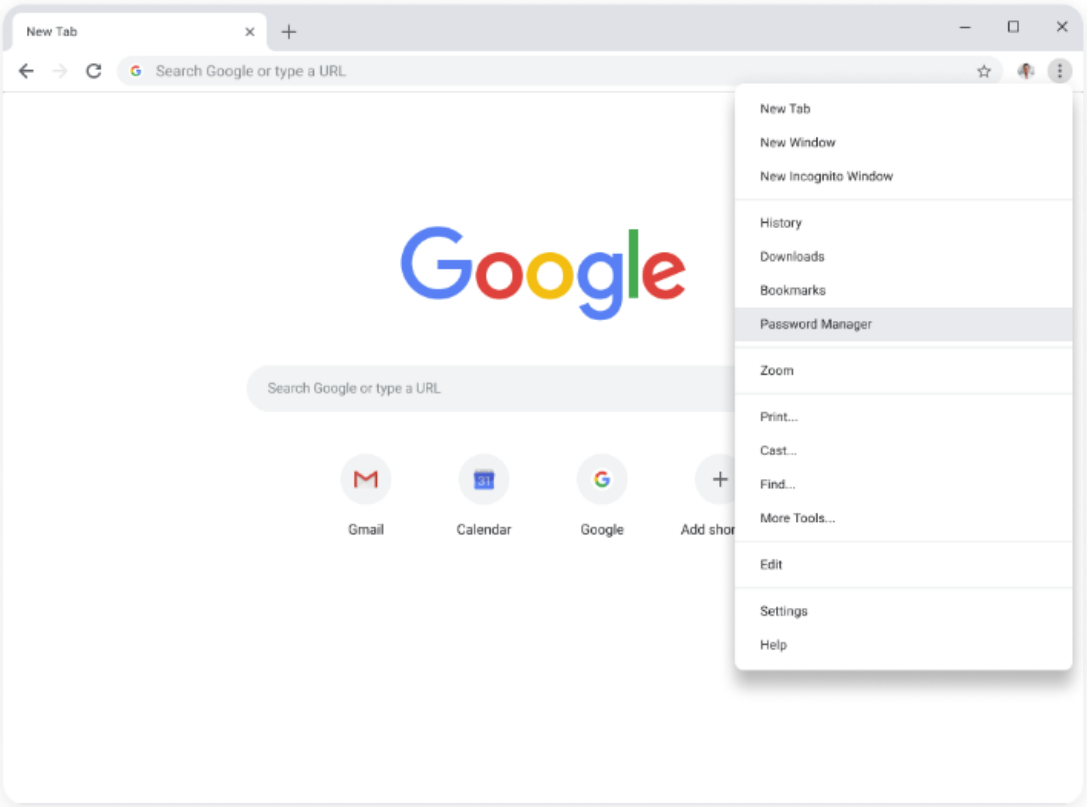
As early as Chrome 114, we will enable access to WebUSB API from extension service workers as a migration path for Manifest V2 extensions that currently access the API from a background page.

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

Changes to Google Password Manager in Chrome 114

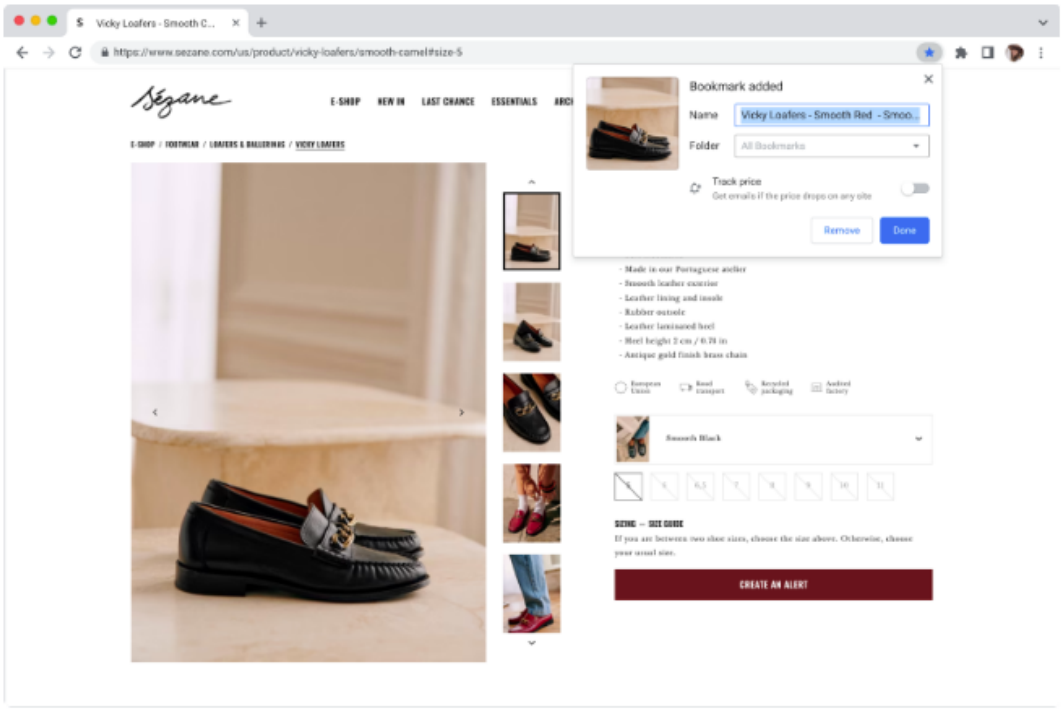
In Chrome 114 the password manager will be re-branded as **Google Password Manager**.

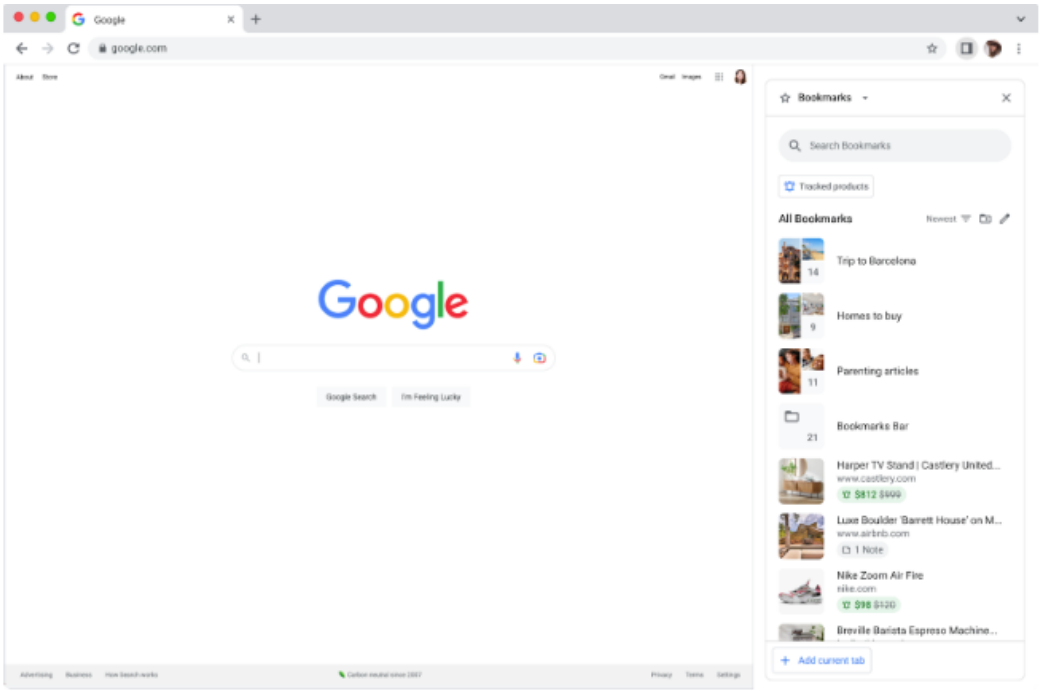
Google Password Manager will offer more functionality and will be easier to access. You will be able to access the new look password manager via the three dot menu (previously located in **Settings>Autofill**) The upgraded **Google Password Manager** groups similar passwords together, has an improved checkup flow and users will be able to add the password manager to their desktop, for easy access.



Updates to Bookmarks on Desktop

In Chrome 114, some users will see an updated experience of the Bookmarks side panel content and entry point to be inclusive of bookmark powers, as well as other features such as search, sorting, and editing.


Vicky Loafers - Smooth C...
https://www.sezane.com/us/product/vicky-loafers/smooth-camel#size-5
Sézane
E-SHOP
NEW IN
LAST CHANCE
ESSENTIALS
E-SHOP / FOOTWEAR / LOAFERS & BALLERINAS / VICKY LOAFERS
Bookmark added
Name
Vicky Loafers - Smooth Red - Smoo...
Folder
All Bookmarks
Track price
Get emails if the price drops on any site
Remove
Done
- Made in our Portuguese atelier
- Smooth leather exterior
- Leather lining and insole
- Rubber outsole
- Leather laminated heel
- Heel height 2 cm / 0.79 in
- Antique gold finish brass chain
Smooth Black
SIZING — SIZE GUIDE
If you are between two shoe sizes, choose the size above. Otherwise, choose your usual size.
CREATE AN ALERT


Google
google.com
Google
Google Search
I'm Feeling Lucky
Bookmarks
Search Bookmarks
Tracked products
All Bookmarks
Newest
Trip to Barcelona
Homes to buy
Parenting articles
Bookmarks Bar
Harper TV Stand | Castlery United...
www.castlery.com
$812 $999
Luxe Boulder 'Barrett House' on M...
www.airbnb.com
1 Note
Nike Zoom Air Fire
nike.com
$98 $120
Breville Barista Espresso Machine...
Add current tab

Network Service on Windows will be sandboxed

As early as Chrome 114, to improve security and reliability, the network service, already running in its own process, will be sandboxed on Windows. As part of this, third-party code that is currently able to tamper with the network service may be prevented from doing so. This might cause interoperability issues with software that injects code into Chrome's process space, such as Data Loss Prevention software. The NetworkServiceSandboxEnabled policy allows you to disable the sandbox if incompatibilities are discovered. You can test the sandbox in your environment using these instructions and report any issues you encounter.

Chrome 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.

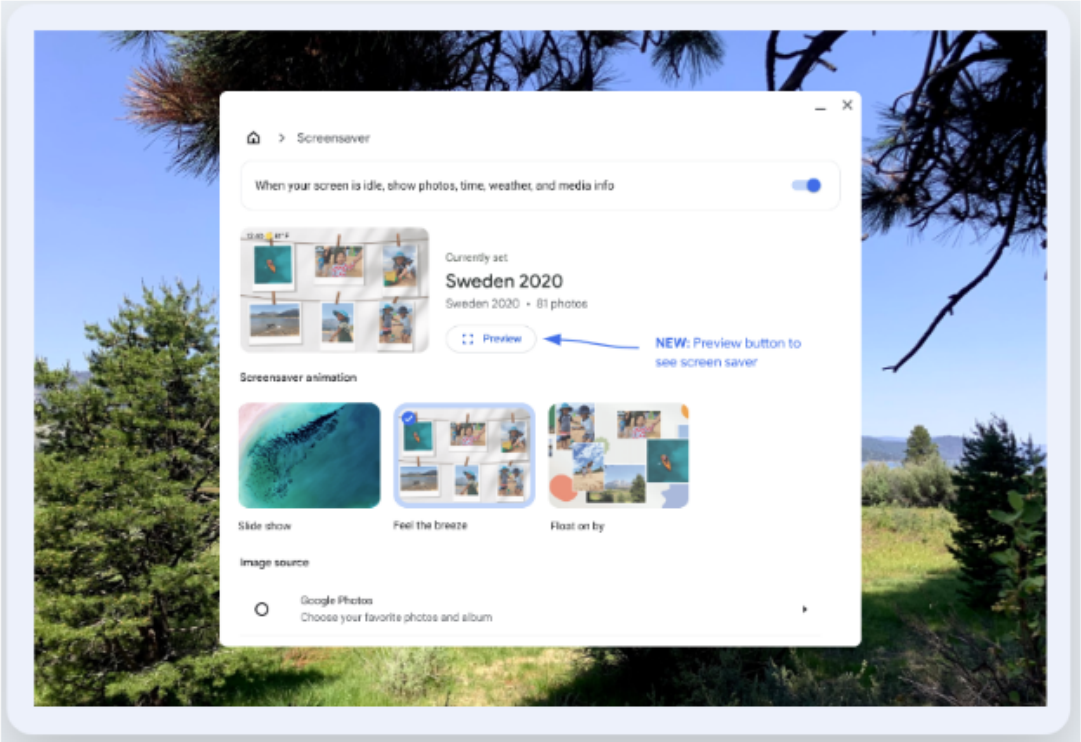
Upcoming ChromeOS changes

Cursive pre-installed for Enterprise and Education accounts

In ChromeOS 113, Cursive, a stylus-first notes app, will be 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*.

Screensaver preview

In ChromeOS 113, a new option will allow users to preview screensaver settings before applying. A preview will prove useful especially when using Google Photos with animations.



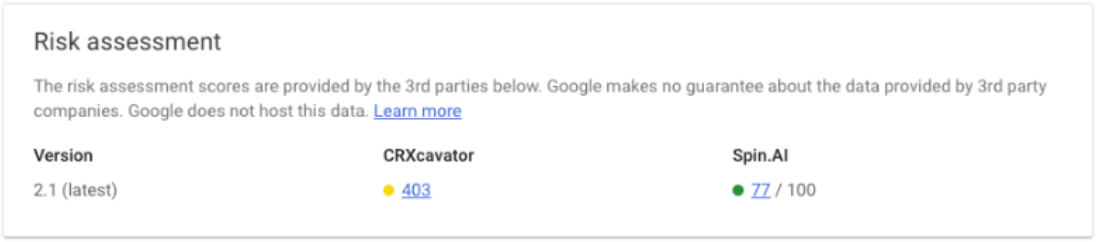
Passpoint: Seamless, secure connection to Wi-Fi networks

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.

Upcoming Admin console changes

Risk Assessment card

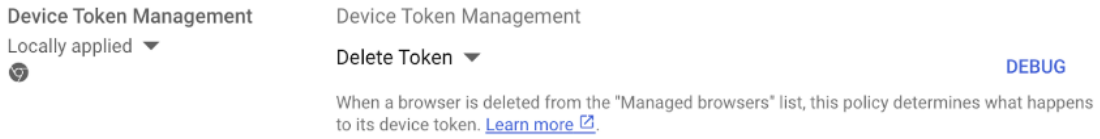
We are creating a new card in the **Extension details** page, which will show third-party risk scores for public extensions.



Device Token Management policy for device token deletion

As early as Chrome 113, a new policy will allow Chrome Browser Cloud Management administrators to delete the device token on the end-point devices when deleting a browser from the managed browsers list in the Admin console.

When the new *Delete token* value is selected and a browser is deleted from the Managed browser list, the browser will automatically re-enroll in Chrome Browser Cloud Management the next time it is online, if the enrollment token was not deleted on the device and the enrollment token is still active. The default value will remain to invalidate the device token.



Previous release notes

Chrome version & targeted Stable channel release date	PDF
Chrome 111: Mar 01, 2023	PDF
Chrome 110: Feb 01, 2023	PDF
Chrome 109: Jan 10, 2023	PDF
Chrome 108: Nov 29, 2022	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