



# Chrome 113 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 April 26, 2023.*

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

[Chrome 113 release summary](#)

[Current Chrome version release notes](#)

[Chrome browser updates](#)

[ChromeOS updates](#)

[Admin console updates](#)

[Coming soon](#)

[Upcoming Chrome browser changes](#)

[Upcoming ChromeOS changes](#)

[Previous release notes](#)

[Additional resources](#)

[Still need help?](#)

## Chrome 113 release summary

<b>Chrome browser updates</b>	<b>Security/ Privacy</b>	<b>User productivity /Apps</b>	<b>Management</b>
Deprecation Trial for Unpartitioned third-party Storage, Service Workers, and Communication APIs	✓		
First-Party Sets user controls	✓		
Collect additional data for off-store extensions in telemetry reports	✓		
Launching FastCheckout for Checkout experiences		✓	
Updated Password Management Experience on iOS in Chrome 113		✓	
Image-set css changes	✓		
Restructure of the three-dot menu in Desktop		✓	
Policy troubleshooting page available on Android			✓
Chrome Desktop <i>New tab</i> page: Journeys card		✓	
Discover Feed on iOS and Android		✓	
Adopt Android media picker		✓	
Partial translate		✓	
New and updated policies in Chrome browser			✓
Removed policies in Chrome browser			✓
<b>ChromeOS updates</b>	<b>Security/ Privacy</b>	<b>User productivity /Apps</b>	<b>Management</b>
Screensaver preview		✓	
Report USB firmware version			✓
Allow policy-provided custom trust anchors at the lock screen	✓		

Files app inline sync status	✓		
ChromeOS administrator instant reboot	✓		✓
Removal of permissive Chrome Apps webview behaviors	✓		
<b>Admin console updates</b>	<b>Security/ Privacy</b>	<b>User productivity /Apps</b>	<b>Management sandboxe</b>
Risk Assessment card		✓	✓
New policies in the Admin console			✓
<b>Upcoming Chrome browser changes</b>	<b>Security/ Privacy</b>	<b>User productivity /Apps</b>	<b>Management</b>
Chrome Root Store updates and removal of the ChromeRootStoreEnabled policy	✓		
Support for Private State Tokens	✓		
New inactive tabs section in the Chrome app on iPhone and iPad		✓	
Lock profile cookie files on disk	✓		
Changes to Google Password Manager in Chrome 114		✓	
Updates to Bookmarks on Desktop		✓	
Password management: save and retrieve notes		✓	
Unpacking Nested Archives in Download Protection	✓		
Separate storage of settings synced to account in Chrome 114	✓		
Chrome policy: disable extensions unpublished from Chrome Web Store (CWS)			✓
Network Service on Windows will be sandboxed	✓		
Enable access to WebUSB API from extension service workers in Chrome 113		✓	

Skip unload events	✓		
Release cycle changes			✓
Read mode		✓	
Changes to phishing protection on Android as early as Chrome 113	✓		✓
Chrome 117 will no longer support macOS 10.13 and macOS 10.14	✓		✓
Extensions must be updated to leverage Manifest V3		✓	✓
<b>Upcoming ChromeOS changes</b>	<b>Security/ Privacy</b>	<b>User productivity /Apps</b>	<b>Management</b>
Cursive pre-installed for Enterprise and Education accounts		✓	
Passpoint: Seamless, secure connection to Wi-Fi networks	✓	✓	
Mandatory extensions for Incognito navigation	✓		
App Streaming on Chrome OS		✓	

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

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

Beginning gradually in Chrome 113, storage, service workers, and communication APIs are [partitioned in third-party contexts](#). In addition to being isolated by the same-origin policy, the affected APIs used in third-party contexts are also 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. During the trial, sites can 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 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](#).

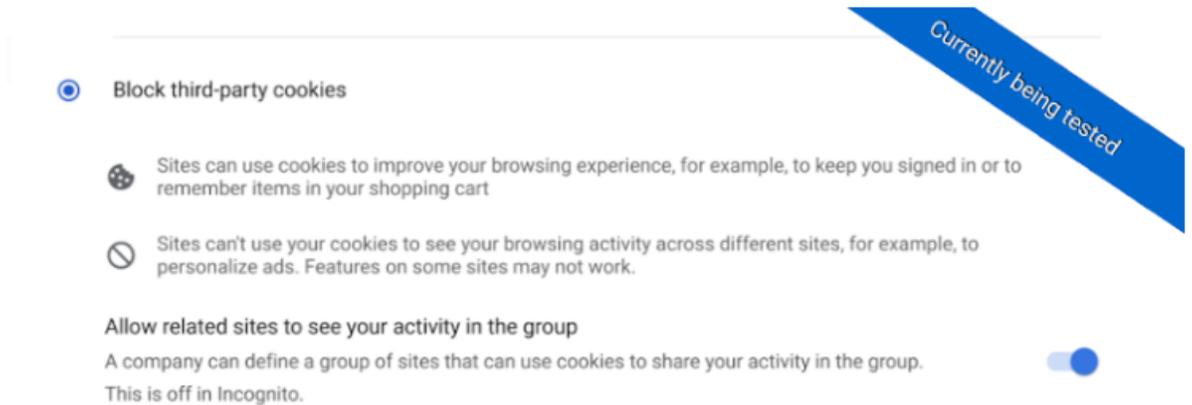
Chrome 113 also add the [DefaultThirdPartyStoragePartitioningSetting](#) enterprise policy, which unpartitions APIs in all third-party contexts, as well as [ThirdPartyStoragePartitioningBlockedForOrigins](#), which unpartitions APIs for third-party contexts when the first-party context's origin matches the list. Both will be supported for at least 12 milestones. You can read more in this [blog post](#).

### **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 introduces user controls for these First-Party Sets. Two enterprise policies are available to manage First-Party Sets: [FirstPartySetsEnabled](#) to enable or disable First-Party Sets, and [FirstPartySetsOverrides](#) to apply your own sets.

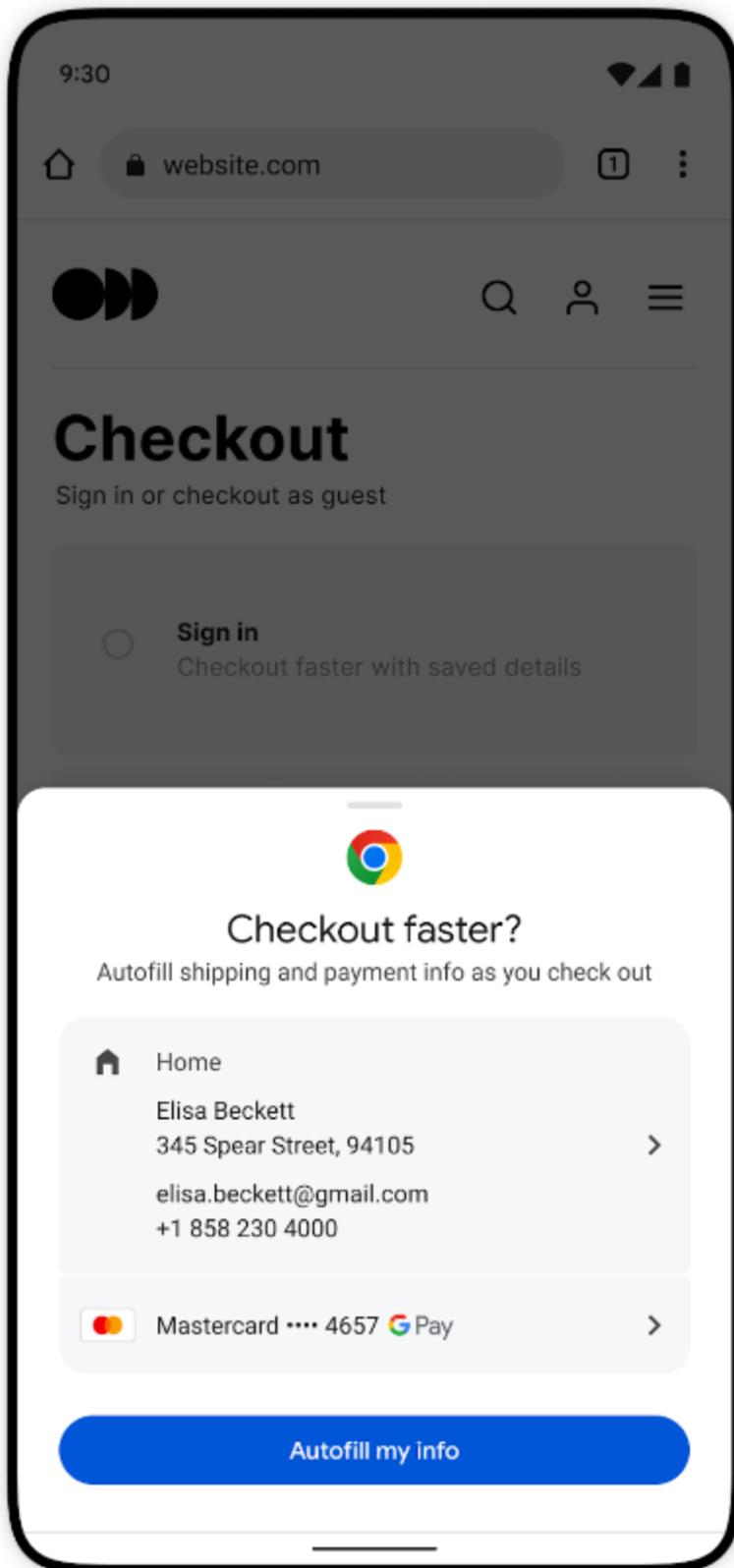


### Collect additional data for off-store extensions in telemetry reports

When Enhanced Safe Browsing is enabled, Chrome 113 starts collecting additional telemetry on off-store extensions, such as file hashes and the `manifest.json` file. Google servers analyze the data collected 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 see updated Autofill options targeting checkout pages on some shopping websites. It can be disabled by either disabling policy [AutofillAddressEnabled](#) or [AutofillCreditCardEnabled](#).



## 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 can now use and save passwords in their Google Account. Relevant enterprise policies such as [BrowserSignin](#), [SyncDisabled](#), [SyncTypesListDisabled](#) and [PasswordManagerEnabled](#) continue to work as before and can be used to configure whether users can use and save passwords in their Google Account.

## Image-set css changes

Chrome 113 implements standard syntax support for image-set and now treats the previously supported `-webkit-` vendor prefix syntax as a parse time alias for the standard. This means that values set with the vendor prefix serialize as standard.

Example:

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

Serializes 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 is the same for both the prefixed and standard syntax ([Chrome Status](#)).

## **Restructure of the three-dot menu in Desktop**

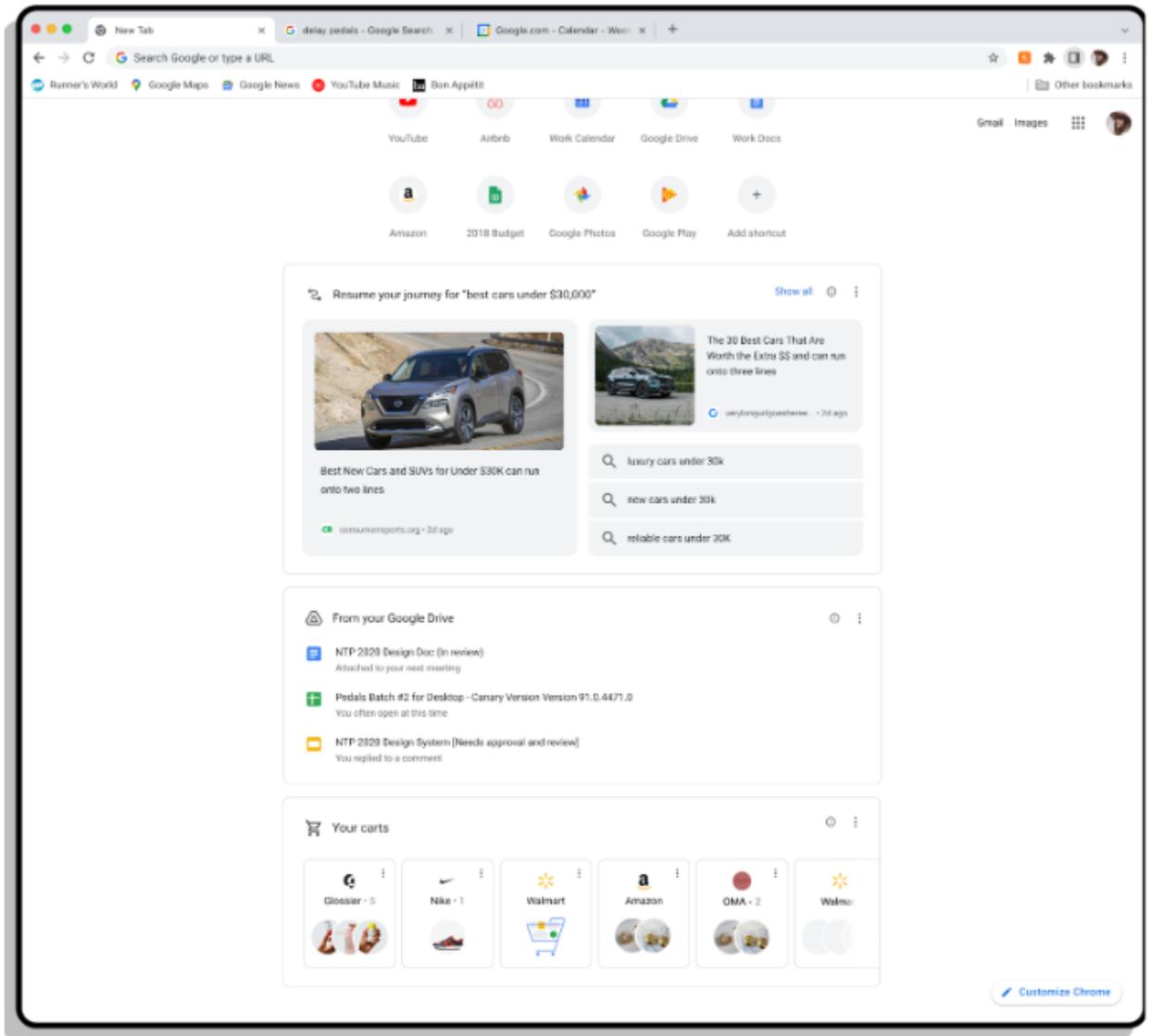
We want to help our users to discover how to customize Chrome to perfectly fit their needs by moving Extensions and the Chrome Web Store to the 1st level of the three-dot menu.

## **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 becomes available in Chrome 113.

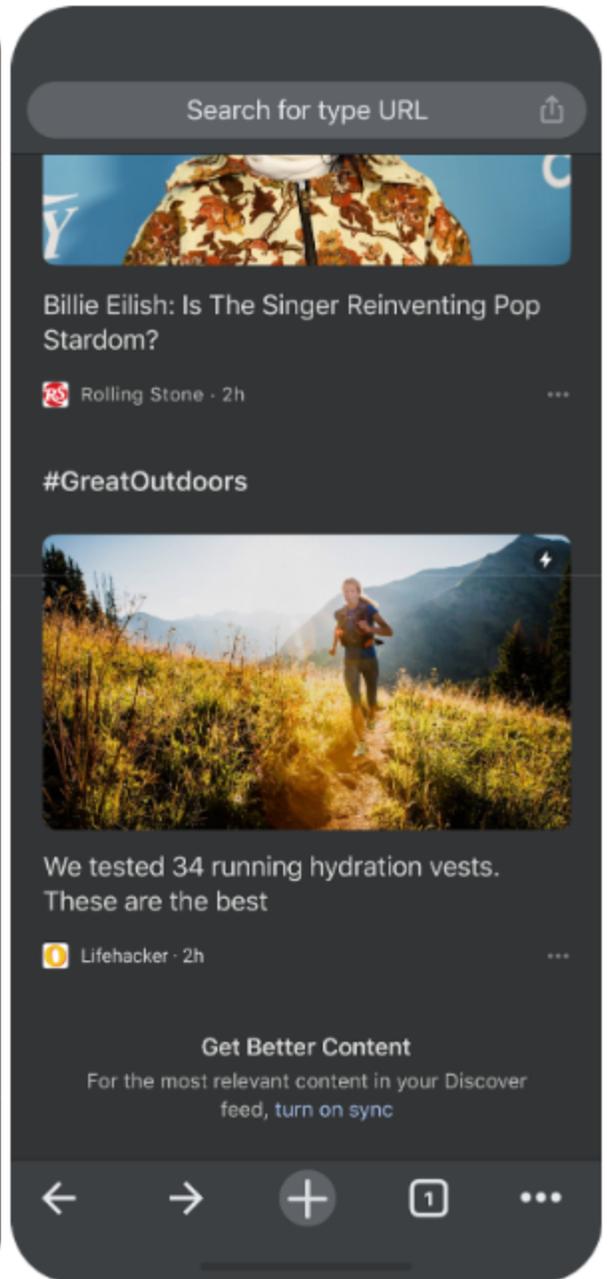
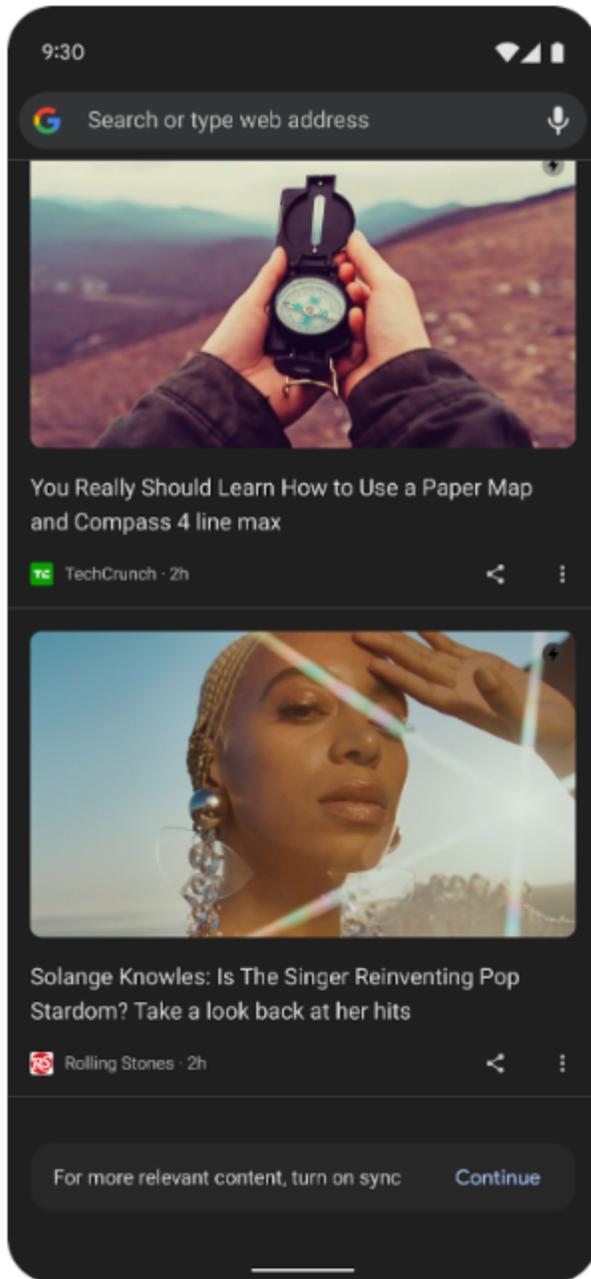
## **Chrome Desktop *New tab* page: Journeys card**

Chrome assists with complex, multi-session task completion through Journeys resumption and next step suggestions on the **New tab** page. You can control the visibility of cards on the **New tab** page using the [NTPCardsVisible](#) policy.

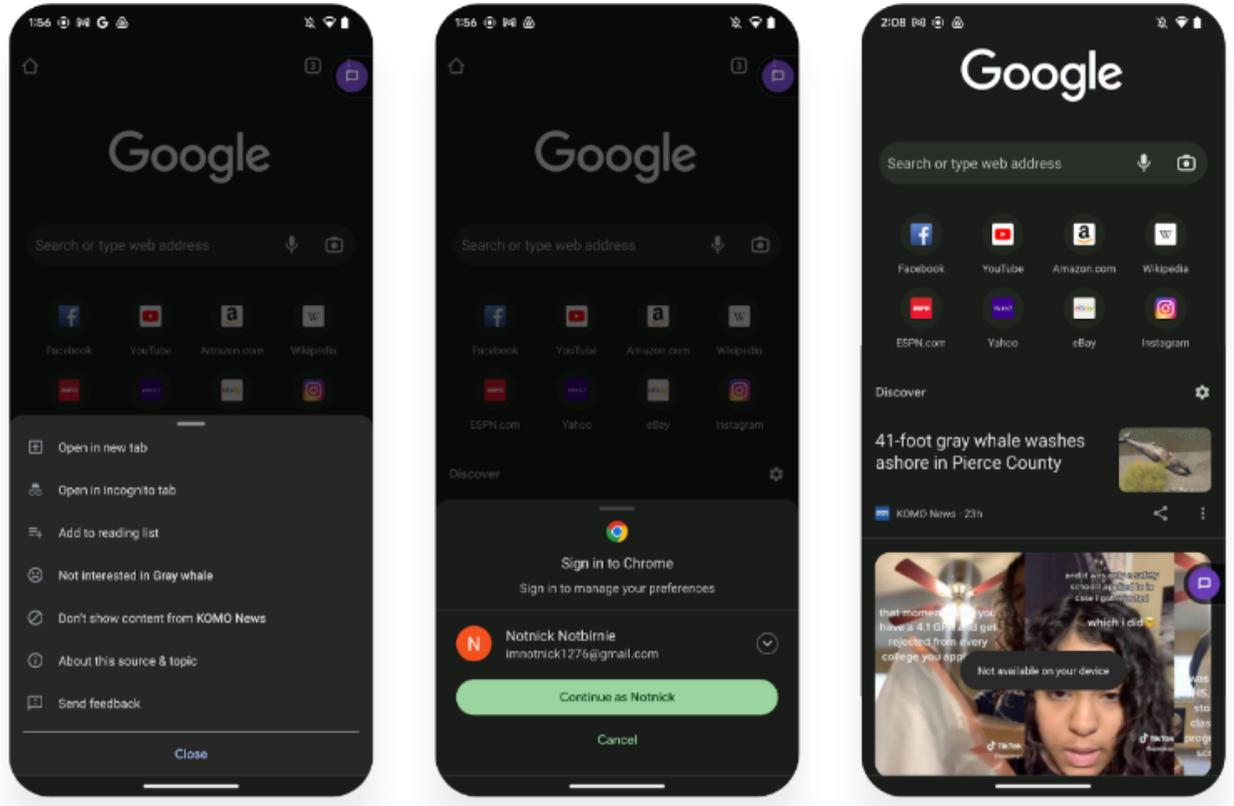


## Discover Feed on iOS and Android

In Chrome 113, Chrome might prompt some users to see more personalized content in their Discover Feed.



The Discover Feed also allows non-signed-in users to control the types of content they see, using updated personalization options. For example, they may choose to hide content from a certain source.



When users who are not signed in want to make a change to their feed content, Chrome prompts them to sign in or sync. As an admin, you still control user sign-in and sync with the [BrowserSignin](#), [SyncDisabled](#), and [SyncTypesListDisabled](#) policies. So, if an enterprise policy prevents sign-in or sync, users see *Not available on your device*.

### Adopt Android media picker

Chrome browser replaces its custom media picker for the new unified Android media picker, when uploading photos and videos to the web. The two are functionally equivalent, but there are slight differences in how they look.

14:16

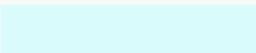


This app can only access the photos you select

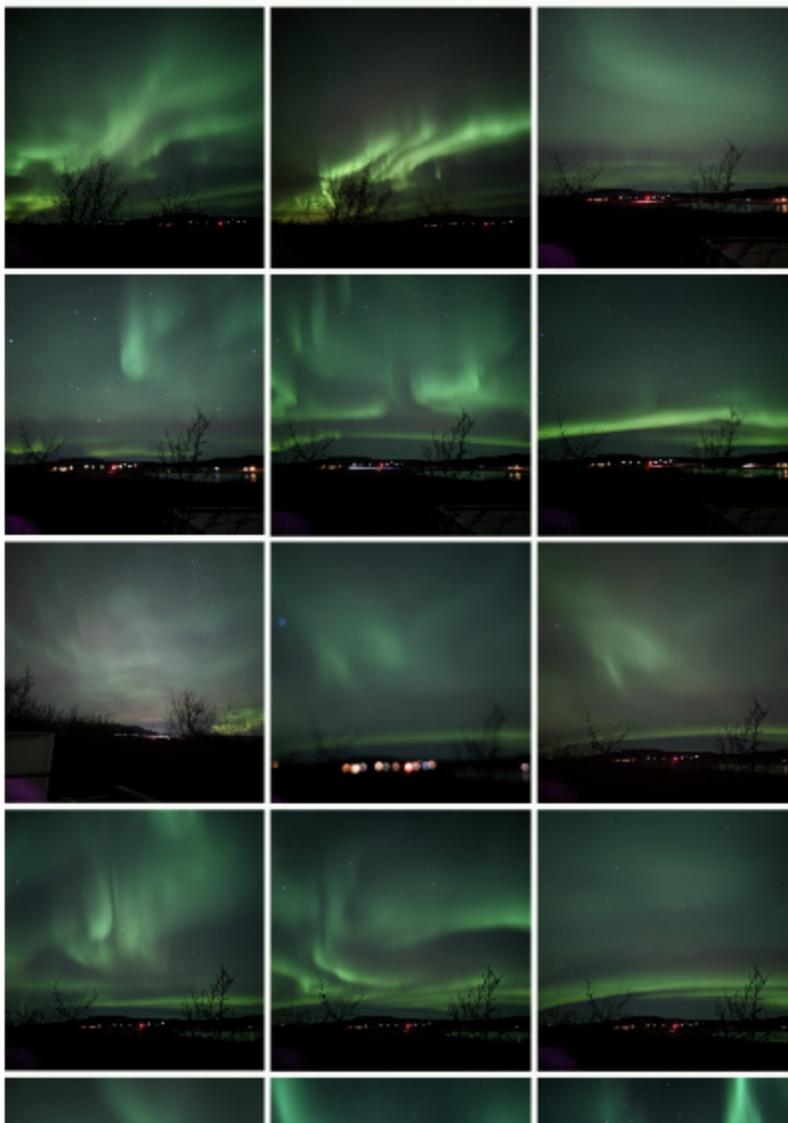


Photos

Albums

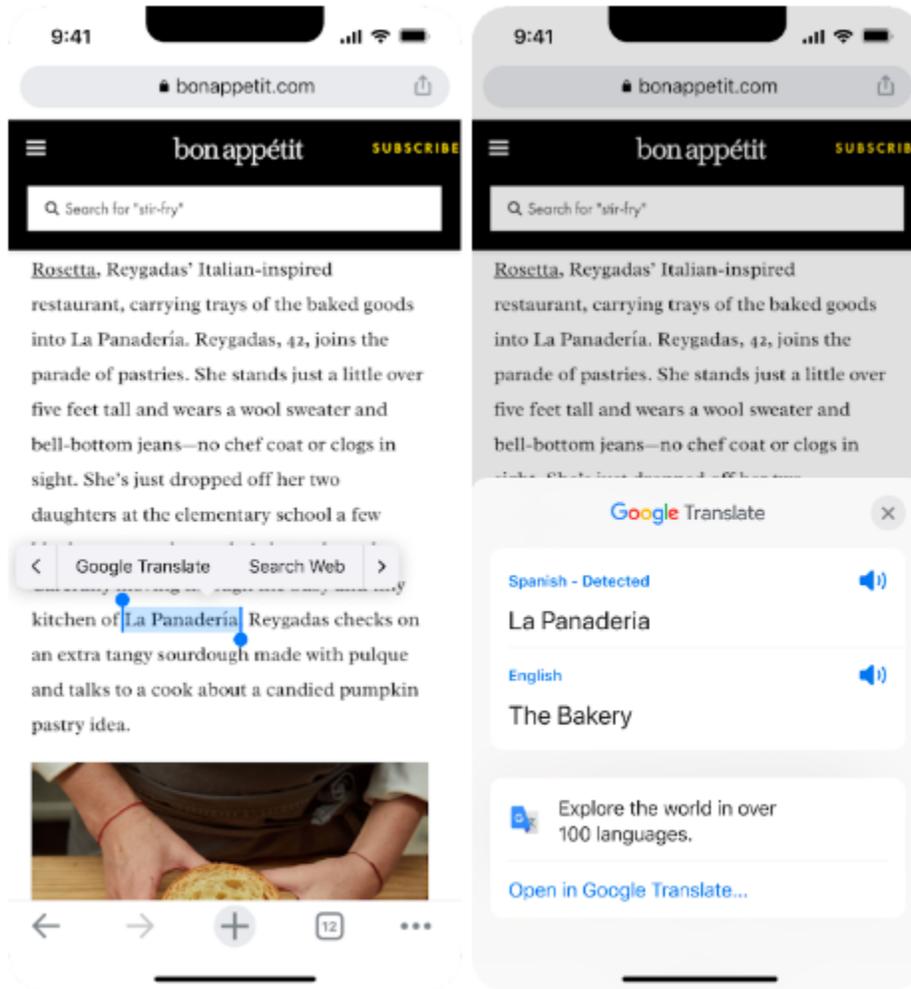


Sat, Nov 26, 2022



## Partial translate

You can now translate part of a web page using the **Edit** menu on Chrome on iOS. You can control this translate functionality with the [TranslateEnabled](#) policy. This only controls Google Translate and won't have any effect on Apple Translate.



## New and updated policies in Chrome browser

Policy	Description
<a href="#">WebRtcTextLogCollectionAllowed</a>	Allow WebRTC text logs collection from Google Services
<a href="#">FirstPartySetsOverrides</a>	Override First-Party Sets
<a href="#">FirstPartySetsEnabled</a>	Enable First-Party Sets.
<a href="#">DefaultThirdPartyStoragePartitioningSetting</a>	Default third-party storage partitioning setting
<a href="#">ThirdPartyStoragePartitioningBlockedForOrigins</a>	Block third-party storage partitioning for these origins
<a href="#">LensCameraAssistedSearchEnabled</a>	Allow Google Lens camera assisted search (now available on iOS)
<a href="#">ScreenCaptureWithoutGestureAllowedForOrigins</a>	Allow screen capture without prior user gesture
<a href="#">ChromeAppsWebViewPermissiveBehaviorAllowed</a>	Restore permissive Chrome Apps webview behavior
<a href="#">FileOrDirectoryPickerWithoutGestureAllowedForOrigins</a>	Allow file or directory picker APIs to be called without prior user gesture

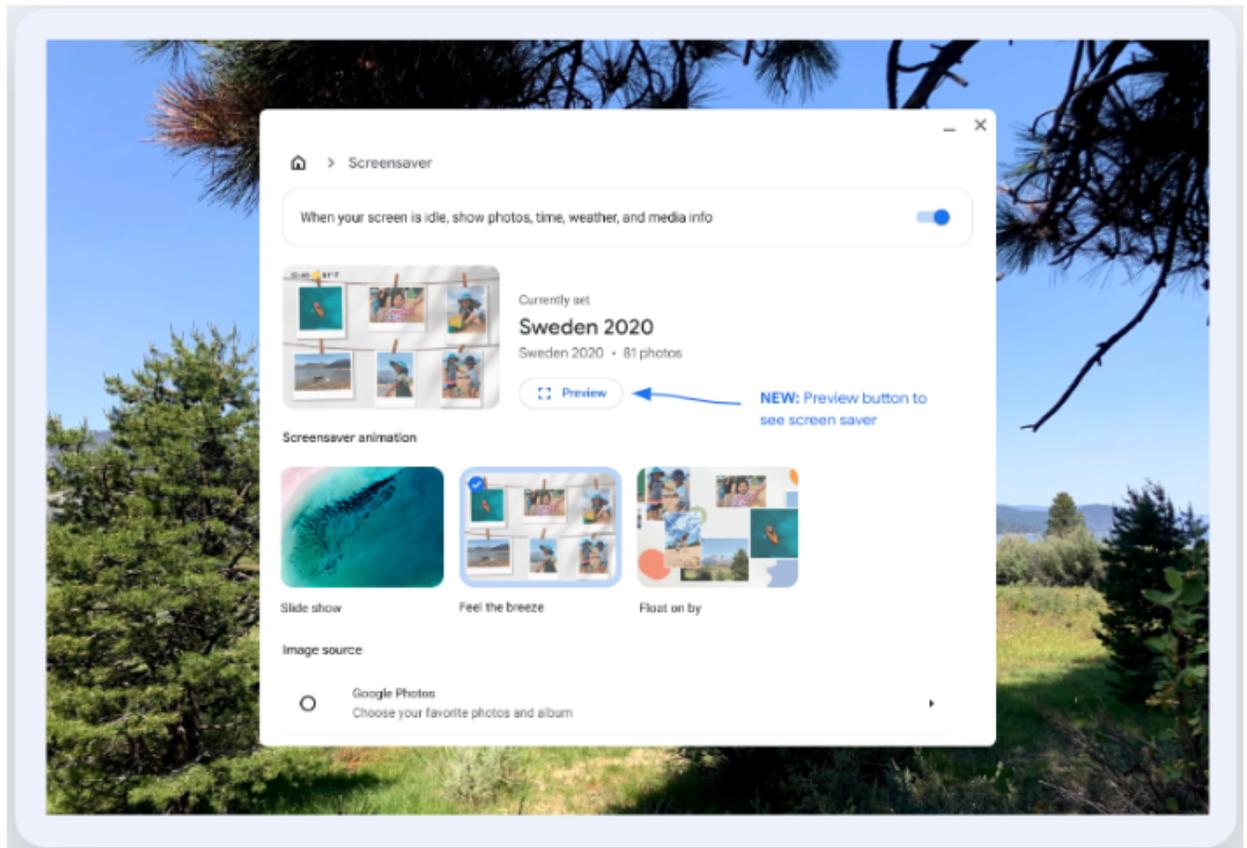
## Removed policies in Chrome browser

Policy	Description
ChromeRootStoreEnabled	Determines whether the Chrome Root Store and built-in certificate verifier will be used to verify server certificates (removed on Windows and Mac)
WebSQLNonSecureContextEnabled	Force WebSQL in non-secure contexts to be enabled
PrefixedStorageInfoEnabled	Re-enable the deprecated window.webkitStorageInfo API

# ChromeOS updates

## Screensaver preview

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



## Report USB firmware version

Whenever a USB device is plugged or unplugged from a managed ChromeOS device, the USB firmware version is reported alongside existing USB events and telemetry. You can control this using the [ReportDevicePeripherals](#) policy, which controls reporting of existing USB events and telemetry.

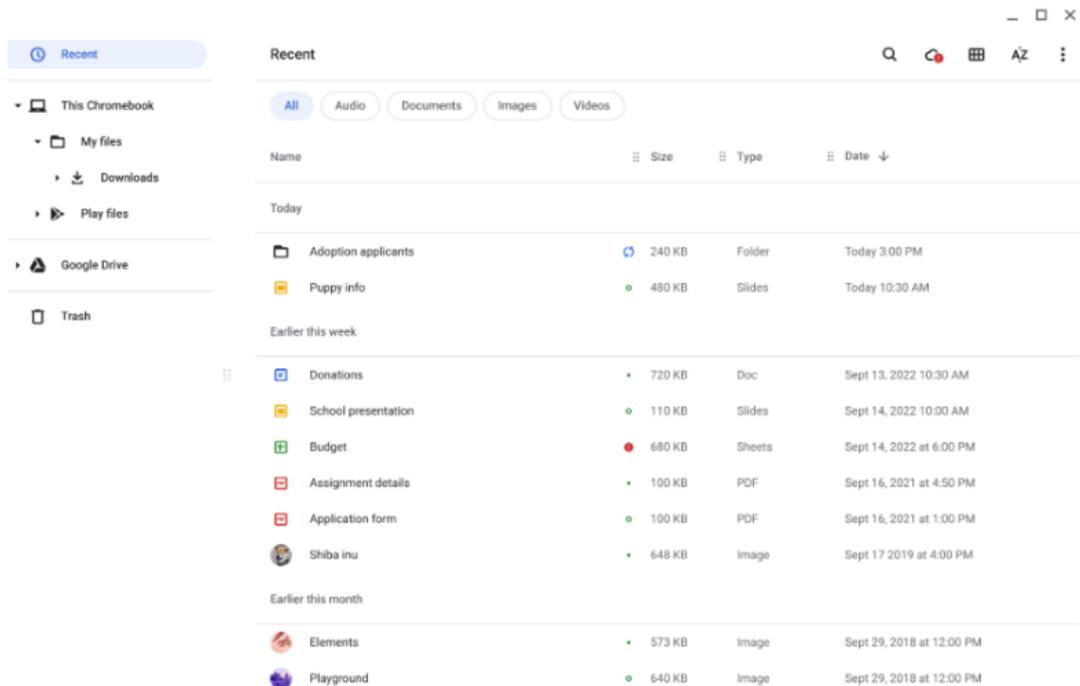
## Allow policy-provided custom trust anchors at the lock screen

Enterprise and EDU deployments might have proxies that intercept, decrypt and inspect user traffic. This requires the client device to have a CA certificate configured to allow it to trust the proxy server certificate for all web hosts, which is usually issued on the fly. For ChromeOS, enterprise deployments configure such trusted CA certificates through enterprise policy.

These custom policy-provided CA certificates are currently only honored for user traffic and inside the user session, but not at the lock screen. This is an issue for customers who have to do re-authentication at the lock screen, which is enforced by policy, since the proxy set in the user session is enforced at the lock screen but the CA certificate is not accessible.

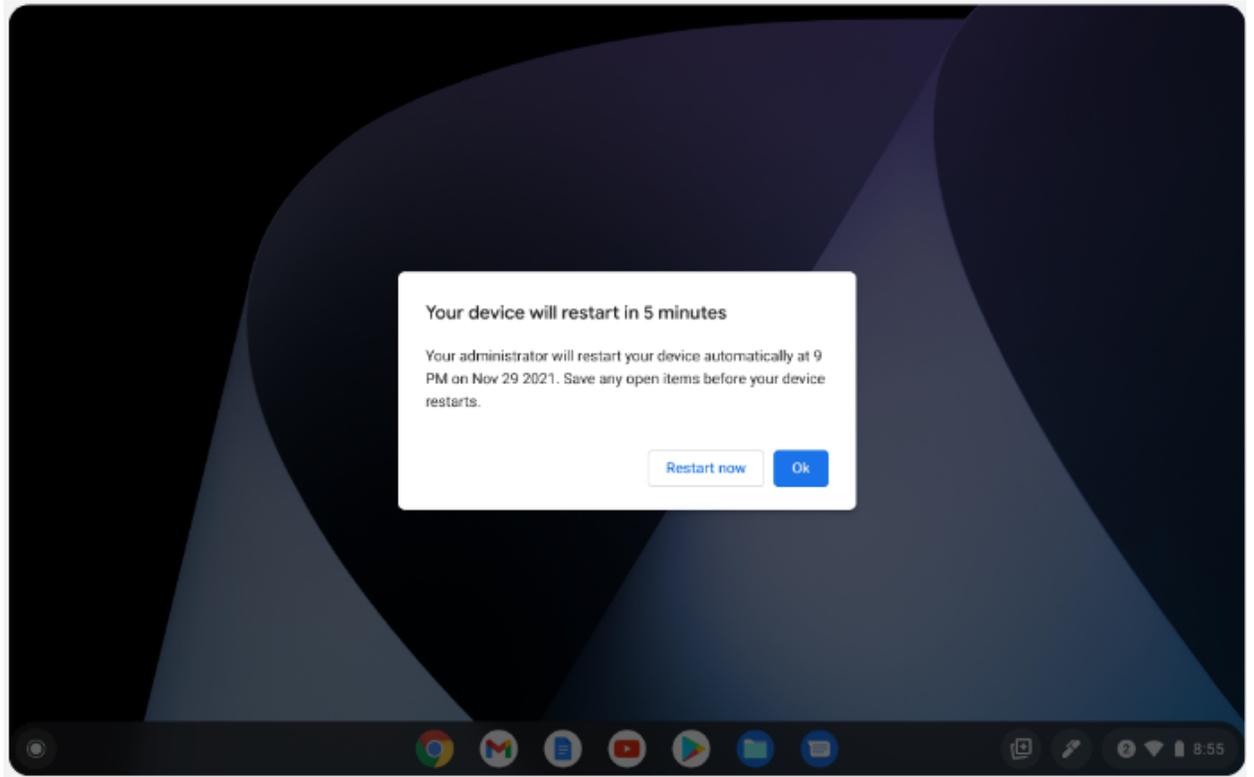
## Files app inline sync status

This feature moves the existing syncing notification and visual signal to a more granular inline sync status. The status appears adjacent to files in Google Drive that are actively syncing. The status also displays for folders within a hierarchy that have syncing descendants.



## ChromeOS administrator instant reboot

With Chrome OS 113, we give admins the option to trigger ChromeOS reboots via the Admin console to facilitate support flows and apply policies instantly when required.



## Removal of permissive Chrome Apps webview behaviors

In Chrome 113, Chrome Apps [webview](#) usage have the following restrictions:

1. SSL errors within webview 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 causes the window reference returned by the `window.open` call in the originating webview to be invalidated.

A temporary enterprise policy [ChromeAppsWebViewPermissiveBehaviorAllowed](#) is available to give enterprises time to address possible breakage related to these changes. To test

whether this change is the cause of any breakage, without needing to set the enterprise policy, 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`.

## Admin console updates

### Risk Assessment card

In the **Extension details** page, we have created a new **Risk assessment** card to show third-party risk scores for public extensions. [Learn more](#).

Risk assessment			
The risk assessment scores are provided by the 3rd parties below. Google makes no guarantee about the data provided by 3rd party companies. Google does not host this data. <a href="#">Learn more</a>			
Version	Installs	CRXcavator	Spin.AI
2.1 (latest)	1	● <a href="#">402</a>	● <a href="#">76</a> / 100
1.5	3	● <a href="#">428</a>	● <a href="#">82</a> / 100

### New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
<a href="#">ChromeAppsWebViewPermissiveBehaviorAllowed</a>	User, Managed Guest Session	Chrome (Linux, Mac, Windows) ChromeOS	Additional app settings
<a href="#">DefaultThirdPartyStoragePartitioningSetting</a>	User, Managed Guest Session	Chrome (Android) Chrome (Linux, Mac, Windows) ChromeOS	Content
<a href="#">ThirdPartyStoragePartitioningBlockedForOrigins</a>	User, Managed Guest Session GS	Chrome (Android) Chrome (Linux, Mac, Windows) ChromeOS	Content

# 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

### Chrome Root Store updates and removal of the ChromeRootStoreEnabled policy

As early as Chrome 114, 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 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.

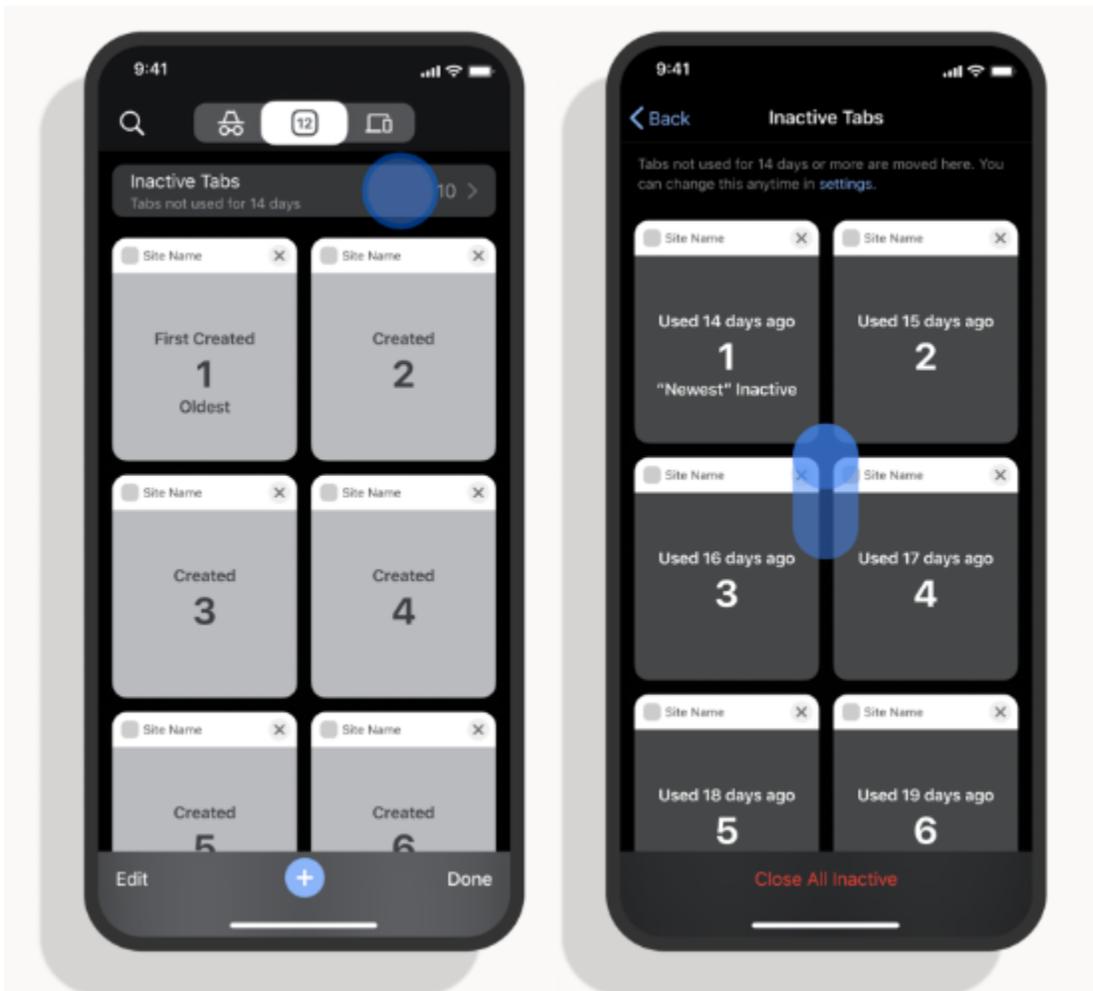
### Support for Private State Tokens

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**. For more information, see this [developer blog post](#).

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

In Chrome 114, 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. Alternatively, users can bring back an inactive tab by clicking on it.



## **Lock profile cookie files on disk**

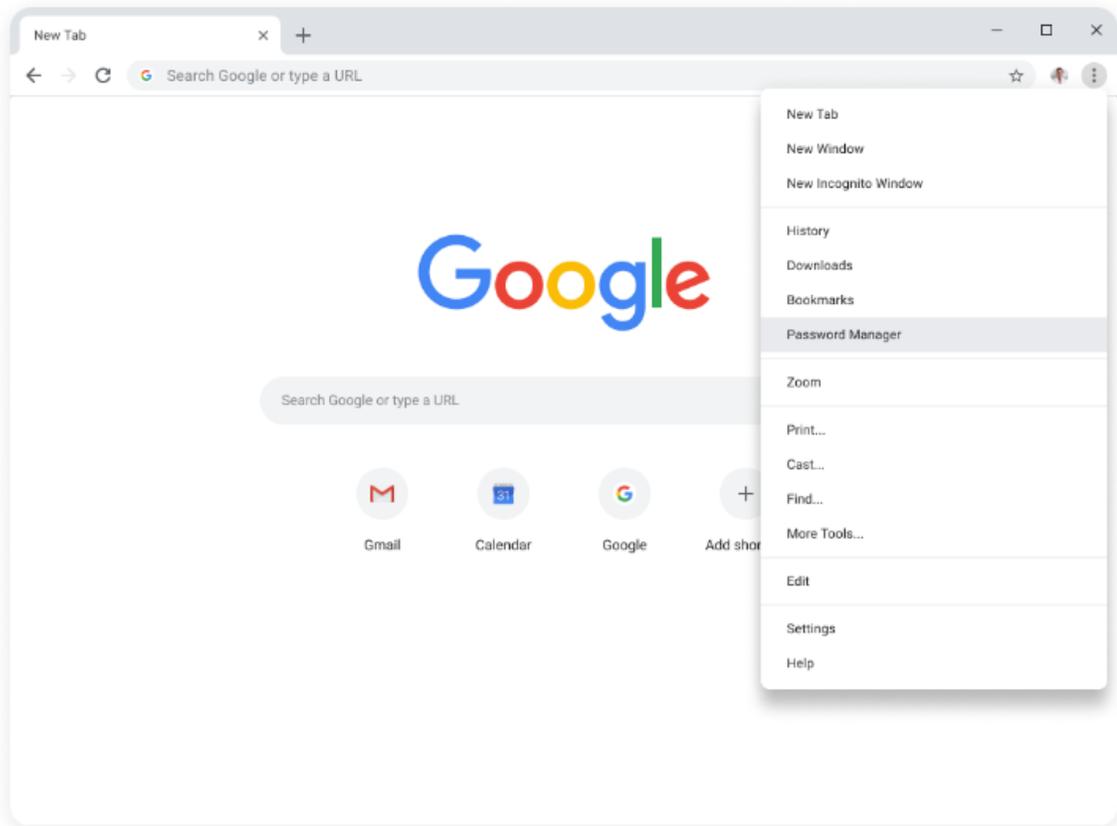
To help protect Chrome users against malware attempting to steal cookie information, Chrome 114 on Windows holds an exclusive lock on the profile cookie files on disk. You can test this behavior to ensure this doesn't interfere with any sanctioned software on your systems by running Chrome with the

``-enable-features=LockProfileCookieDatabase`` command line flag on Dev and Beta channel of Chrome 114.

## **Changes to Google Password Manager in Chrome 114**

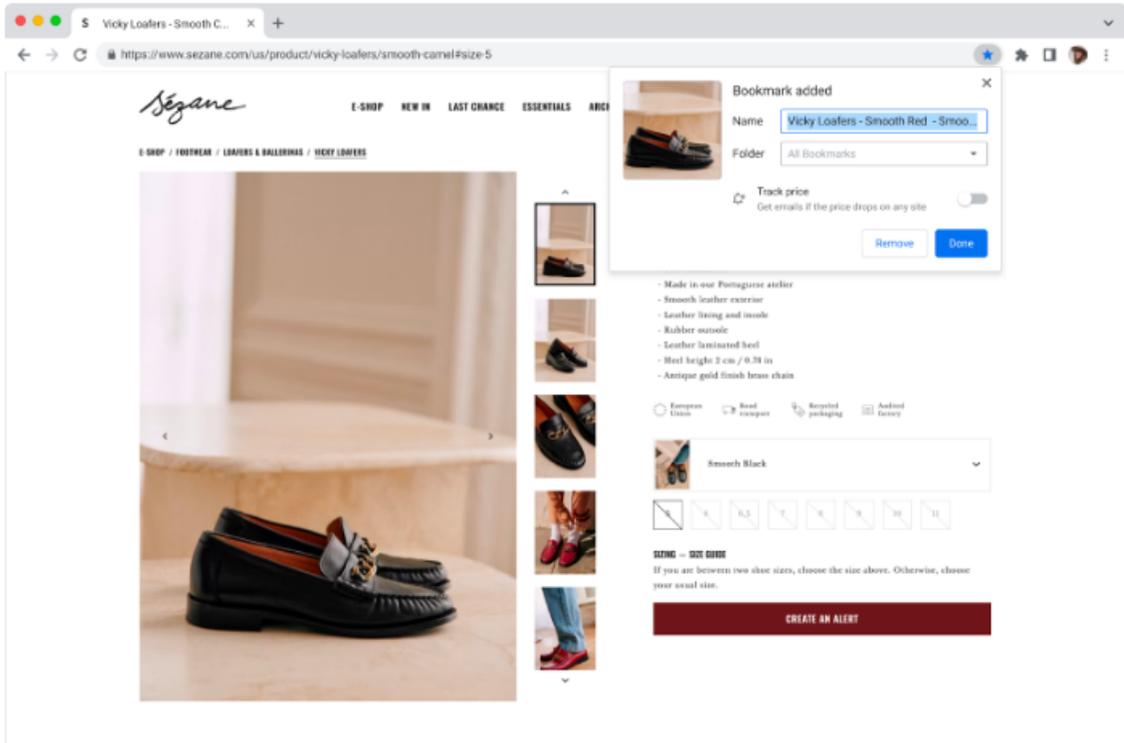
In Chrome 114 the password manager will be rebranded as **Google Password Manager**.

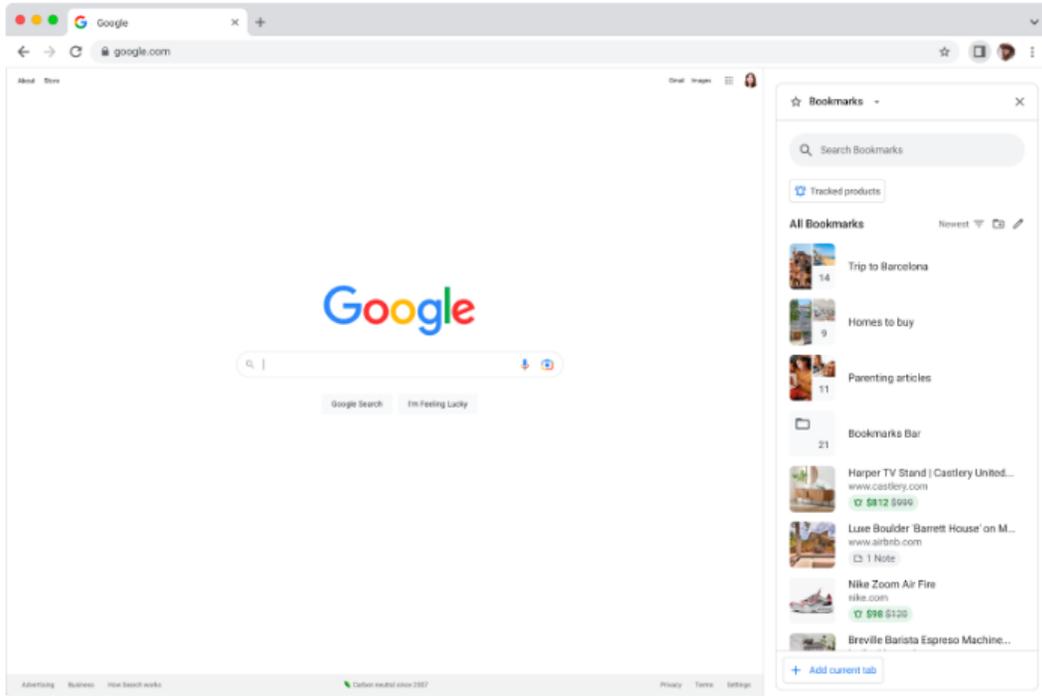
**Google Password Manager** will offer more functionality and be easier to access. You will be able to access the new look password manager via the three dot menu (previously located in **Settings>Autofill**). The upgraded **Google Password Manager** groups similar passwords together, has an improved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



## Updates to Bookmarks on Desktop

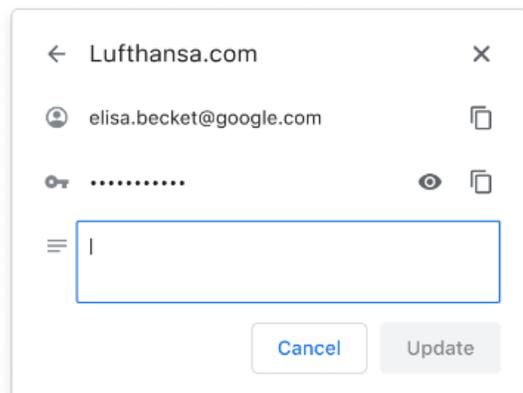
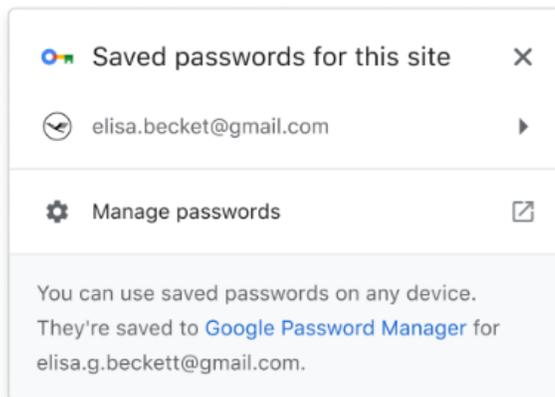
In Chrome 114, some users will see an updated experience of the Bookmarks side panel content and entry point to be inclusive of bookmark powers, as well as other features such as filtering, sorting, and editing.





### Password management: save and retrieve notes

Chrome 114 revamps the password management native bubble 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, username, password, unmask the password and edit the stored note.



## Unpacking Nested Archives in Download Protection

Starting in Chrome 114, users with Safe Browsing enabled will begin recursively unpacking downloads of archives. This extends the long-standing protections Chrome offers against malware and unwanted software to combat techniques being abused by distributors of cookie theft malware. The [SafeBrowsingProtectionLevel](#) policy can be used to enable or disable Safe Browsing, including this feature.

## Separate storage of settings synced to account in Chrome 114

For Chrome users on iOS and Android who have Sync enabled, settings synced to their Google account will be kept separate from the local Chrome settings, which were set when Sync was turned-off. This will allow 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 can be enabled via

```
chrome://flags#enable-preferences-account-storage.
```

There are two existing policies to disable Sync functionality, which will 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.

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

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

## Network Service on Windows will be sandboxed

As early as Chrome 115, 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.

### **Enable access to WebUSB API from extension service workers in Chrome 115**

As early as Chrome 115, 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.

### **Skip unload events**

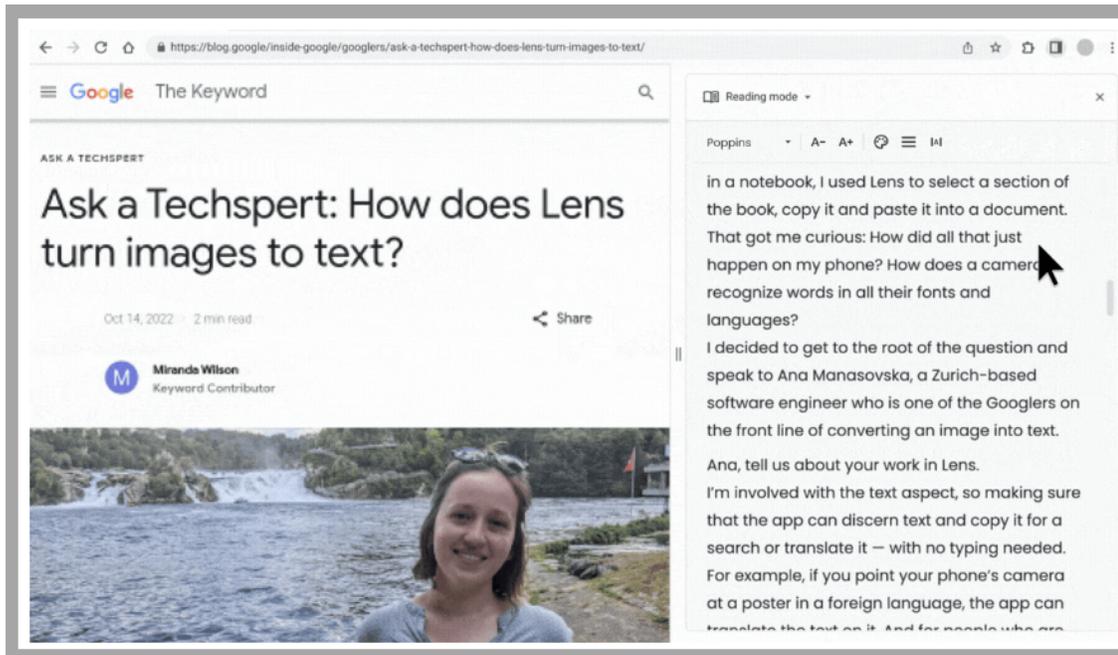
The presence of unload event listeners is a primary blocker for [back/forward cache](#) on Chromium based browsers and for Firefox on desktop platforms. On the other hand, for mobile platforms, almost all browsers prioritize the [bfcache](#) by not firing unload events in most cases. To improve the situation, 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.

### **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.

## Read mode

As more content is read online, we're adding a new feature to help boost the 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.



## Changes to phishing protection on Android as early as Chrome 115

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.

### **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.

### **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](#).

## 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*.

### **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 will allow administrator to configure a list of extensions which users need to explicitly allow to run in Incognito, to use Incognito mode for navigation.

### **App Streaming on Chrome OS**

In Chrome OS 114, 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 Chrome OS desktop. This is part of a [Google-wide ambient computing](#) effort.

## Previous release notes

Chrome version & targeted Stable channel release date	PDF
<a href="#">Chrome 112: Mar 29, 2023</a>	<a href="#">PDF</a>
<a href="#">Chrome 111: Mar 01, 2023</a>	<a href="#">PDF</a>
<a href="#">Chrome 110: Feb 01, 2023</a>	<a href="#">PDF</a>
<a href="#">Chrome 109: Jan 10, 2023</a>	<a href="#">PDF</a>
<a href="#">Archived release notes</a>	

## 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](#)

*Google and related marks and logos are trademarks of Google LLC. All other company and product names are trademarks of the companies with which they are associated.*