



Chrome 128 Enterprise and Education release notes

For administrators who manage Chrome browser or Chrome devices for a business or school.

These release notes were published on August 14, 2024.

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

Chrome 128 release summary	2
Current Chrome version release notes	6
Chrome browser updates	6
ChromeOS updates	16
Admin console updates	22
Coming soon	23
Upcoming Chrome browser updates	23
Upcoming ChromeOS changes	38
Upcoming Admin console changes	40
Previous release notes	41
Additional resources	42
Still need help?	42

Chrome 128 release summary

Chrome browser updates	Security / Privacy	User productivity / Apps	Management
Search your history in Chrome with AI		✓	
Admin-configurable site search		✓	✓
Handling undecryptable passwords in Password Manager			✓
Inactive Tabs		✓	
New PromotionsEnabled policy replaces PromotionalTabsEnabled			✓
Revamped Chrome Safety Check on Android	✓		
Rust JSON Parser	✓		
Tab Groups on iPad		✓	
Updates for CookiePartitionKey of partitioned cookies	✓		
Deprecate CHIPS and Relaunch in WebView	✓		
Isolated Web Apps	✓		
Rename position-try-options to position-try-fallbacks	✓		
Google Calendar Card on the <i>New tab</i> page		✓	
New and updated policies in Chrome browser			✓
Removed policies in Chrome browser			✓
ChromeOS updates	Security/ Privacy	User productivity/Apps	Management

Snap groups on ChromeOS		✓	
Data processor mode: EU-wide rollout	✓		
Privacy Controls: Geolocation	✓		
ChromeOS privacy control reminders on app settings page	✓		✓
Store aggregated vitals data with one-year retention	✓		
OCR in ChromeOS Camera App		✓	
Magnifier follows Chromevox		✓	
Auto Gain Control enabled by default		✓	
APN management			✓
Pinned notifications on ChromeOS			✓
Admin console updates	Security/ Privacy	User productivity/Apps	Management
Chrome profile separation - new deployment guide	✓		
Chrome Enterprise Data Controls: Clipboard		✓	
Upcoming Chrome browser updates	Security / Privacy	User productivity / Apps	Management
Tab compare		✓	
Ad-hoc code signatures for PWA shims on macOS		✓	
Clear device data on sign out on iOS	✓		
Meter element fallback styles	✓		
Chrome will no longer support macOS 10.15	✓		✓

Deprecate Safe Browsing Extended reporting	✓		
New option in HttpsOnlyMode policy	✓		✓
Sync Tab Group		✓	
Update Google Play Services to fix issues with on-device passwords			✓
Deprecate non-standard declarative shadow DOM serialization	✓		
Deprecate the includeShadowRoots argument on DOMParser	✓		
Rename inset-area to position-area	✓		
Entrust certificate distrust	✓		
Support non-special scheme URLs	✓		
Network Service on Windows will be sandboxed			✓
Chrome Third-Party Cookie Deprecation (3PCD)	✓		
User Link capturing on PWAs		✓	✓
Private network access checks for navigation requests: warning-only mode			✓
Insecure form warnings on iOS	✓		
Chrome extension telemetry integration with Chronicle	✓		✓
Remove policy used for legacy same site behavior			✓

X25519Kyber768 key encapsulation for TLS	✓		
UI Automation accessibility framework provider on Windows		✓	
Upcoming ChromeOS changes	Security / Privacy	User productivity / Apps	Management
Update to keyboard shortcut for Select-to-speak		✓	
Chrome Enterprise Premium for file transfers on Managed Guest Sessions		✓	
Generative AI wallpapers and video conference backgrounds	✓		
ChromeOS XDR window events	✓		
Upcoming Admin console changes	Security/ Privacy	User productivity/Apps	Management
Chrome browser managed profile reporting			✓
Admin console widget for data controls			✓

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. Allow 1 to 2 weeks for translation for some languages.

Chrome Enterprise and Education release notes are published in line with the [Chrome release schedule](#), on the Early Stable date for Chrome browser.

Current Chrome version release notes

Chrome browser updates

Search your history in Chrome with AI

Starting in Chrome 128, users can search their browsing history based on page contents and not just the page title and URL. Initially, this feature is only available to users in English in the US. Admins can control this feature by using the [HistorySearchSettings](#) policy. You have the following options for your organization:

- 0 = Enable the feature for users, and send relevant data to Google to help train or improve AI models. Relevant data may include prompts, inputs, outputs, and source materials, depending on the feature. It may be reviewed by humans for the sole purpose of improving AI models.
- 1 = Enable the feature for users, but do not send data to Google to train or improve AI models.
- 2 = Fully disable feature

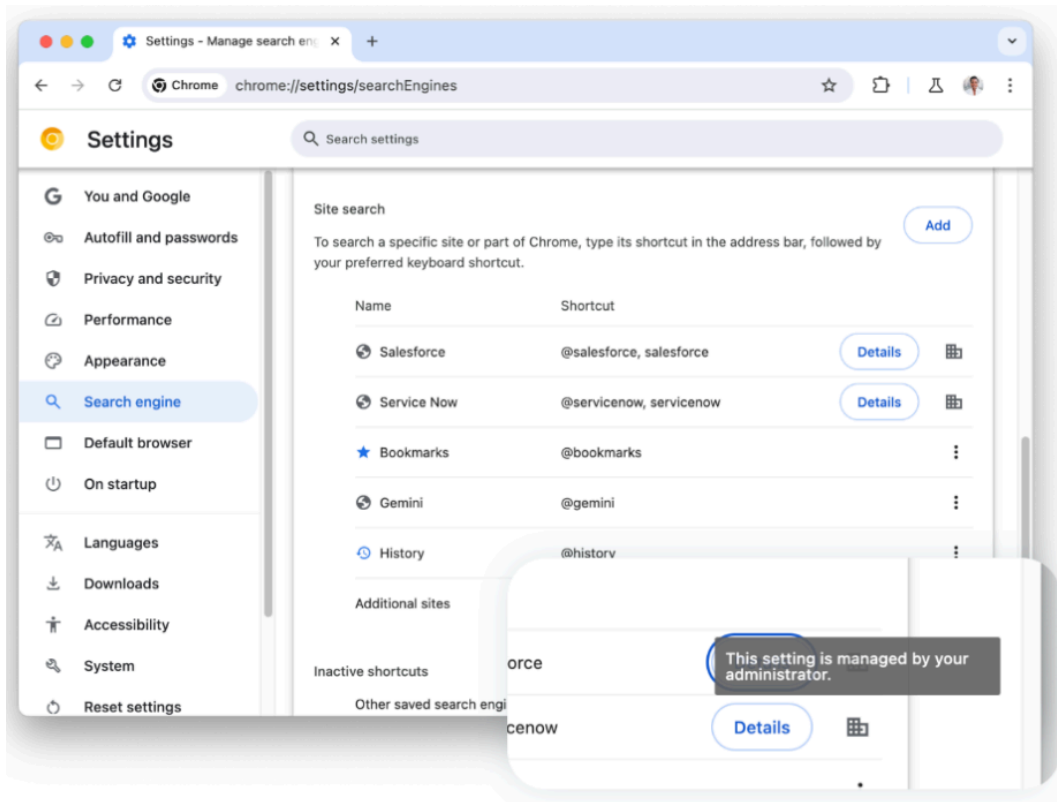
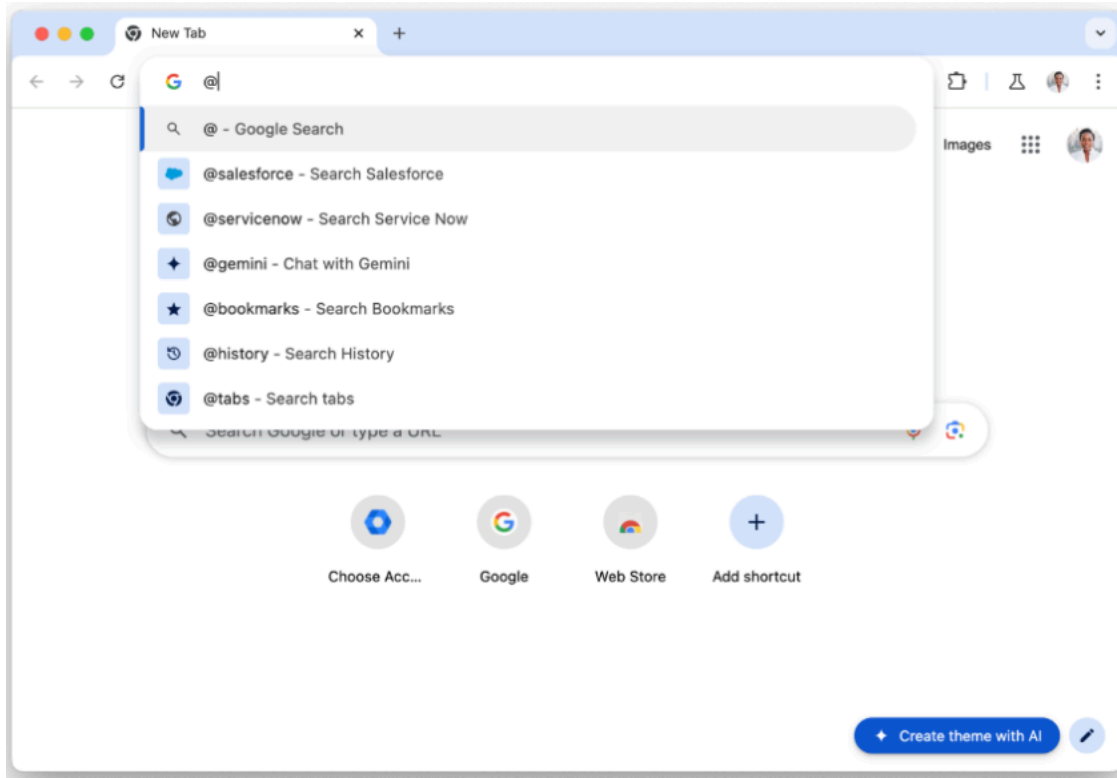
For more information, see [Search your history in Chrome with AI](#).

- **Chrome 128 on Linux, Mac, Windows**

Admin-configurable site search

Site search shortcuts are a way to use the address bar (Omnibox) as a search box for a specific site without navigating directly to the site's URL, similar to how you can use the Omnibox to perform a broad Google search of the web. You can now create site shortcuts on behalf of your managed users, to shortcut to the most critical enterprise sites. You can control this feature using the [SiteSearchSettings](#) policy.

- **Chrome 128 on ChromeOS, Linux, Mac, Windows:** Available for Chrome Browser Core customers signed up for Trusted Tester starting Chrome 128, following by gradual rollout for all Chrome Browser Enterprise customers a few weeks later



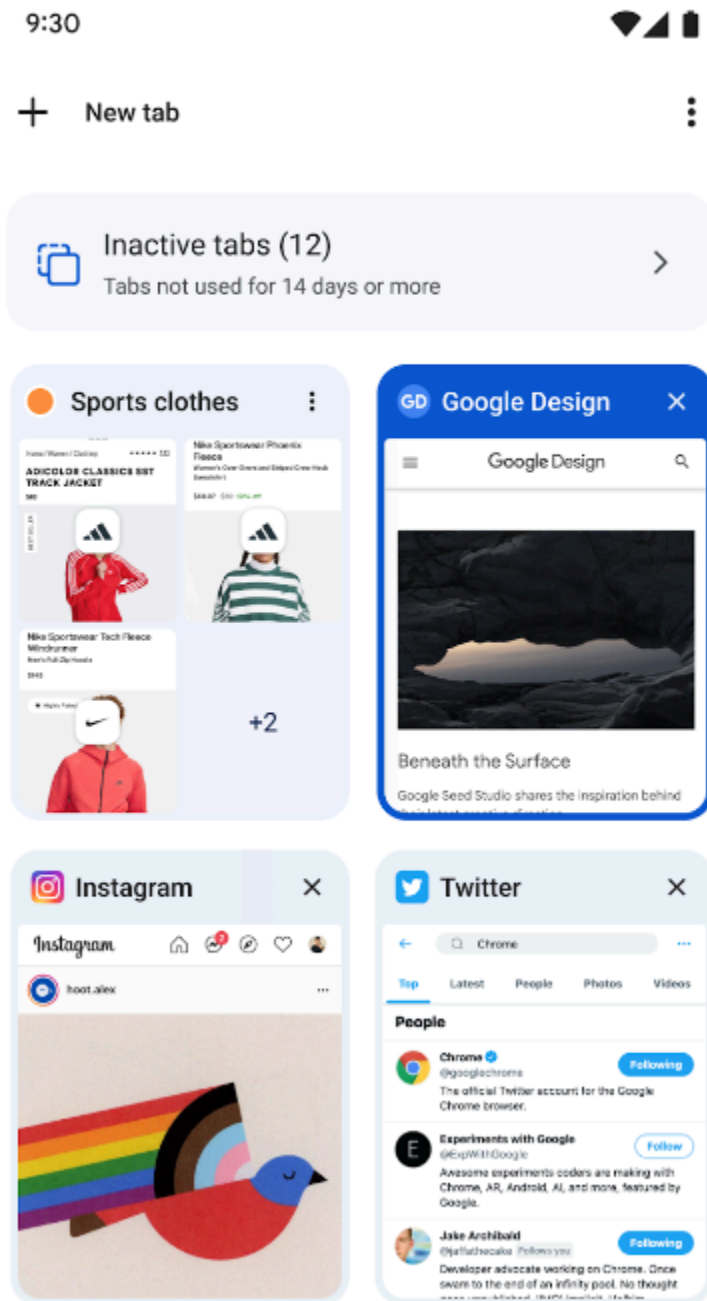
Handling undecryptable passwords in Password Manager

Users sometimes end up with undecryptable passwords on their device, for example, if they've used third party software to move to a new device. We are launching a new policy called [DeletingUndecryptablePasswordsEnabled](#) that helps handle such passwords. When enabled, this policy deletes undecryptable passwords from the user's device, unless the [UserDataDir](#) policy is specified. When [DeletingUndecryptablePasswordsEnabled](#) is off, undecryptable passwords are untouched, but this will result in broken Password Manager functionality.

- **Chrome 128 on iOS, Linux, Mac, Windows**

Inactive tabs

In Chrome 128, we now hide old tabs under a new **Inactive Tabs** section in the tab switcher on Chrome on Android. Chrome users can access the **Inactive Tabs** section to view all old tabs or close them using the new bulk tab functionality. These tabs will be deleted if inactive for over 60 days.



- Chrome 128 on Android: Rolls out to 1%

New PromotionsEnabled policy replaces PromotionalTabsEnabled

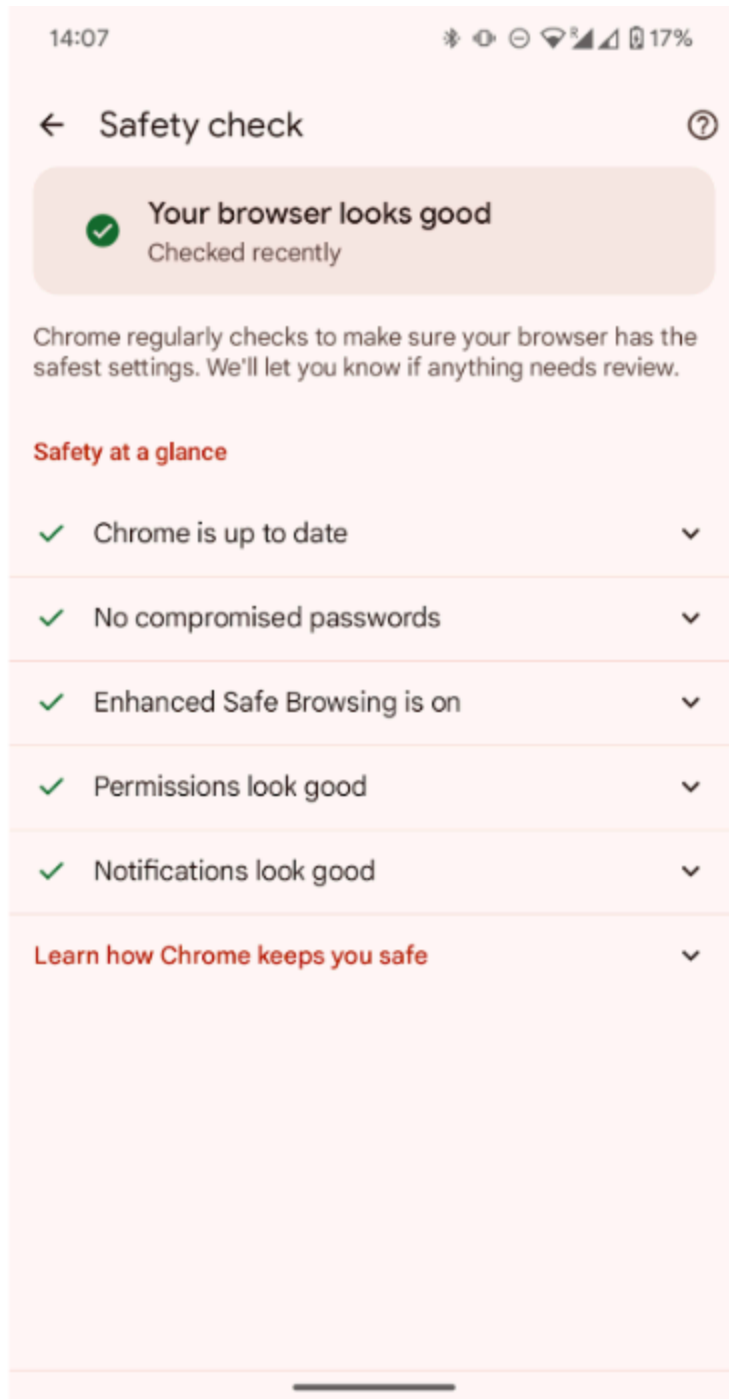
In Chrome 128, new promotional OS-level notifications are shown to users. To include a larger number of promotional features under one policy, a new policy [PromotionsEnabled](#) has been created to replace [PromotionalTabsEnabled](#), which will be deprecated in the future.

- **Chrome 128 on ChromeOS, Linux, Mac, Windows:** [PromotionsEnabled](#) will begin to roll out with Chrome 128. There is no flag.

Revamped Chrome Safety Check on Android

Chrome 128 introduces a new proactive Safety Check that regularly checks the browser for safety-related issues and informs users when there's anything that needs their attention. This launch also introduces a re-designed **Safety Check** page, `chrome://settings/safetyCheck`, with Chrome's proactive safety-related actions and information tailored to each user, designed to make it easier for users to stay safe online. For more information, see [Manage Chrome safety and security](#).

- **Chrome 128 on Android**



Rust JSON Parser

As early as Chrome 128, Chrome will parse JSON using Rust, rather than C++. This will remove the risk of memory safety vulnerabilities in the JSON parser, improving security. This change should be

transparent to users. There is a small risk of certain invalid JSON, which Chrome currently accepts, no longer being accepted, although the Rust parser remains extremely lenient.

In the event that Chrome doesn't accept the invalid JSON, this will lead to 500s or other application-level errors, not crashes. If Chrome no longer accepts some invalid JSON, the JSON should be aimed to be fixed.

- **Chrome 128**

Tab Groups on iPad

Chrome for iPad users can create and manage tab groups. This helps users stay organized, reduce clutter and manage their tasks more efficiently.

- **Chrome 128 on iOS**

Updates for CookiePartitionKey of partitioned cookies

Chrome 128 adds a cross-site ancestor bit to the keying of the partitioned cookie's CookiePartitionKey. This change unifies the partition key with the partition key values used in storage partitioning and adds protection against clickjacking attacks by preventing cross-site embedded frames from having access to the top-level-site's partitioned cookies.

If an enterprise experiences any breakage with embedded iframes, they can use the [CookiesAllowedForUrls](#) policy or use SameSite=None cookies without the Partitioned attribute and then invoke the Storage Access API (SAA) to ensure that embedded iframes have access to the same cookies as the top level domain.

- **Chrome 128 on Windows, Mac, Linux**

Deprecate CHIPS and relaunch in WebView

The WebViewClient supports a method, `shouldInterceptRequest`, which allows developers to intercept network activity and modify HTTP headers, etc. This API does not have access to the Cookie header and relies on the Android CookieManager API in order to query what cookies are

available for a particular request URL. However, partitioned cookies are double-keyed on the top-level site and the site of the URL using the cookies.

Currently, the CookieManager API provides no way for developers to query partitioned cookies correctly, and this will cause a mismatch between what the Java API returns and what frames in WebView will actually be in their Cookie header. After discussing this with the WebView team, we believe that the option that will minimize potential app breakage is to disable Cookies Having Independent Partitioned State ([CHIPS](#)) on WebView until we are able to ship support for the Cookie header to `shouldInterceptRequest`. We will release the changes to `shouldInterceptRequest` in the next target SDK version (API level 36).

Enterprise workflows that use WebView to load web content that relies on partitioned cookies will have their state cleared. WebView apps still have access to unpartitioned 3P cookies and cookies set with Partitioned after the change will revert to their legacy pre-CHIPS behavior until we relaunch the feature.

- **Chrome 128 on Android**

Isolated Web Apps

Isolated Web Apps (IWAs) are an extension of existing work on PWA installation and Web Packaging that provides stronger protections against server compromise and other tampering, which is necessary for developers of security-sensitive applications.

Rather than being hosted on live web servers and fetched over HTTPS, these IWAs are packaged into Web Bundles, signed by their developer, and distributed to end-users through one or more of the potential methods described in the Chromium project [explainer](#).

In this initial release, IWAs are only installable using a new policy, [IsolatedWebAppInstallForceList](#), on enterprise-managed ChromeOS devices.

- **Chrome 128 on ChromeOS**

Rename position-try-options to position-try-fallbacks

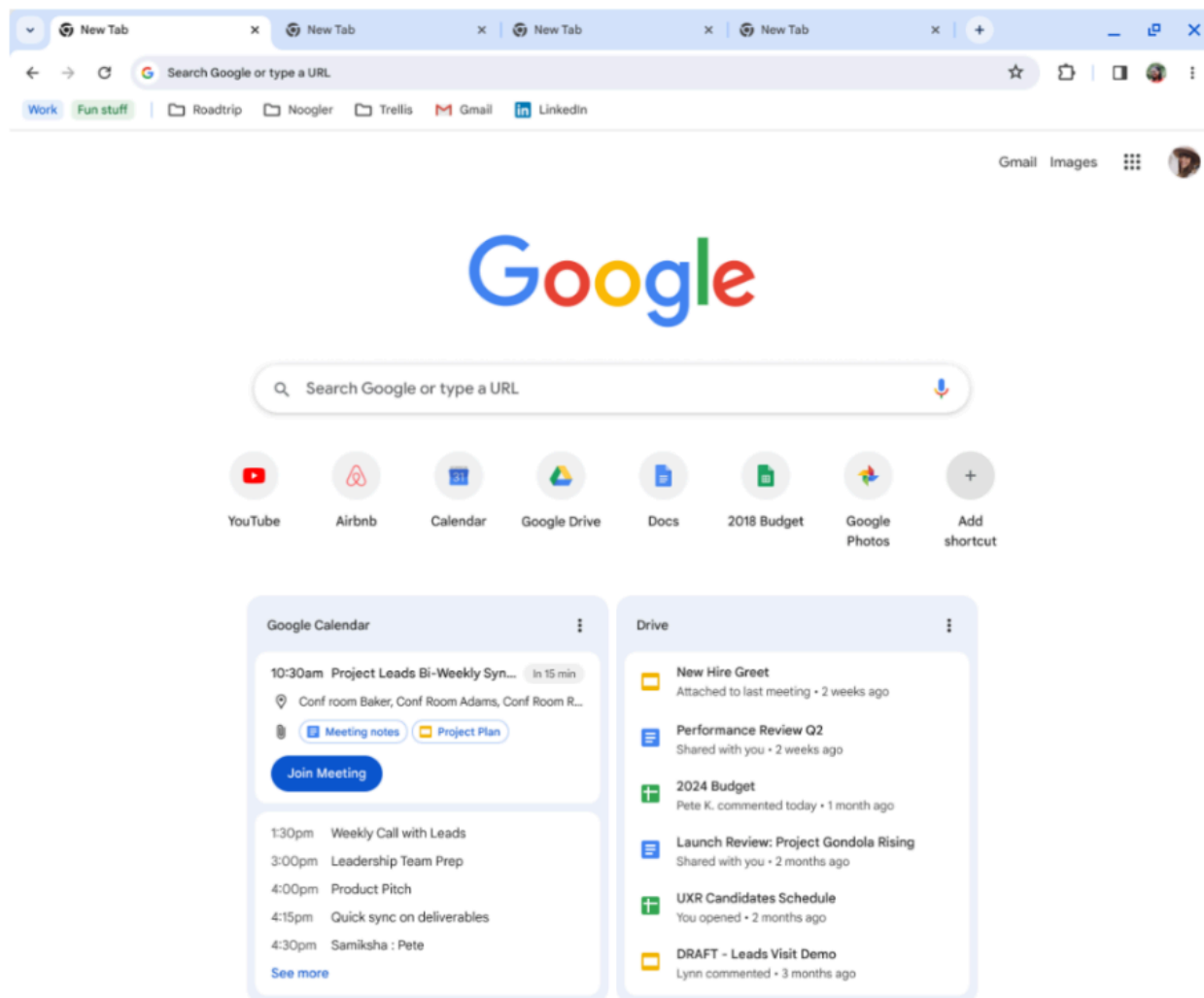
The CSS working group ([CSSWG](#)) resolved to rename this property, because fallbacks more accurately describe what this property controls. The word *options* is a bit unclear, since the styles outside of `position-try` blocks will be tested first, and if they result in a layout that fits within the containing block, none of the options will get used. So *fallbacks* is a better word to describe this behavior. For more details, see [Github](#).

- **Chrome 128 on Windows, Mac, Linux, Android**

Google Calendar Card on the New tab page

Enterprise users can now access their upcoming meetings directly from the **New tab** page with the new calendar card. This streamlined experience eliminates the need to switch tabs or waste time searching for your next meeting, allowing you to focus on what matters most. You can control cards on the **New tab** page with the [NTPCardsVisible](#) policy.

- **Chrome 128 on Linux, Mac, Windows**



New and updated policies in Chrome browser

Policy	Description
DataControlsRules	Sets a list of Data Controls rules.
PromotionsEnabled	Enable showing promotional content
SiteSearchSettings	Provides a list of sites that users can quickly search using shortcuts in the address bar.
LensOverlaySettings	Settings for the Lens Overlay feature

ExtensionDeveloperModeSettings	Control the availability of developer mode on extensions page
QRCodeGeneratorEnabled	Enable QR Code Generator
PrintingLPACSandboxEnabled	Enable Printing LPAC Sandbox
HistorySearchSettings	Settings for AI-powered History Search
ChromeForTestingAllowed	Allow Chrome for Testing
ProvisionManagedClientCertificateForUser	Enables the provisioning of client certificates for a managed user or profile
StandardizedBrowserZoomEnabled	Enable Standardized Browser Zoom Behavior
DeletingUndecryptablePasswordsEnabled	Enable deleting undecryptable passwords

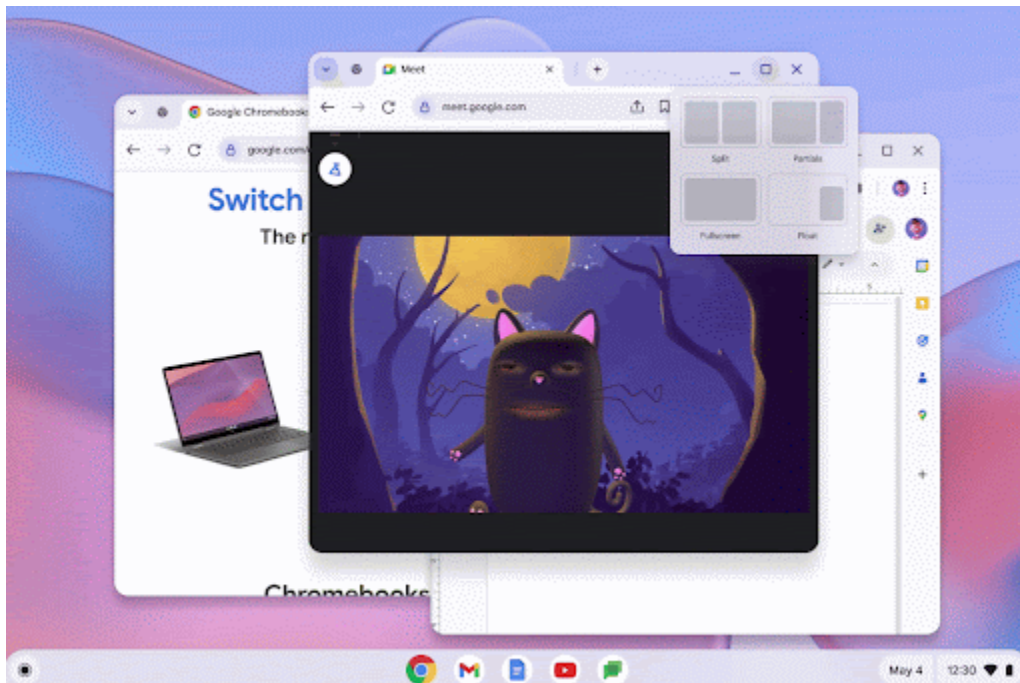
Removed policies in Chrome browser

Policy	Description
RemoteAccessHostTokenUrl	URL where remote access clients should obtain their authentication token
RemoteAccessHostTokenValidationUrl	URL for validating remote access client authentication token
EnterpriseBadgingTemporarySetting	Control the visibility of enterprise badging
RemoteAccessHostTokenValidationCertificateIssuer	Client certificate for connecting to RemoteAccessHostTokenValidationUrl
EnforceLocalAnchorConstraintsEnabled	Determines whether the built-in certificate verifier will enforce constraints encoded into trust anchors loaded from the platform trust store.
CertificateTransparencyEnforcementDisabledForLegacyCas	Disable Certificate Transparency enforcement for a list of Legacy Certificate Authorities

ChromeOS updates

Snap groups on ChromeOS

In ChromeOS 128, **Snap groups** allow you to group windows on ChromeOS. A snap group is formed when you pair two windows for a split-screen. You can bring the windows back together, resize them simultaneously, or move them both as a group.



Data processor mode: EU-wide rollout

New data processor mode features and ChromeOS terms are available to the entire EU through the Google Admin console. For more details, see [Overview of ChromeOS data processor mode](#).

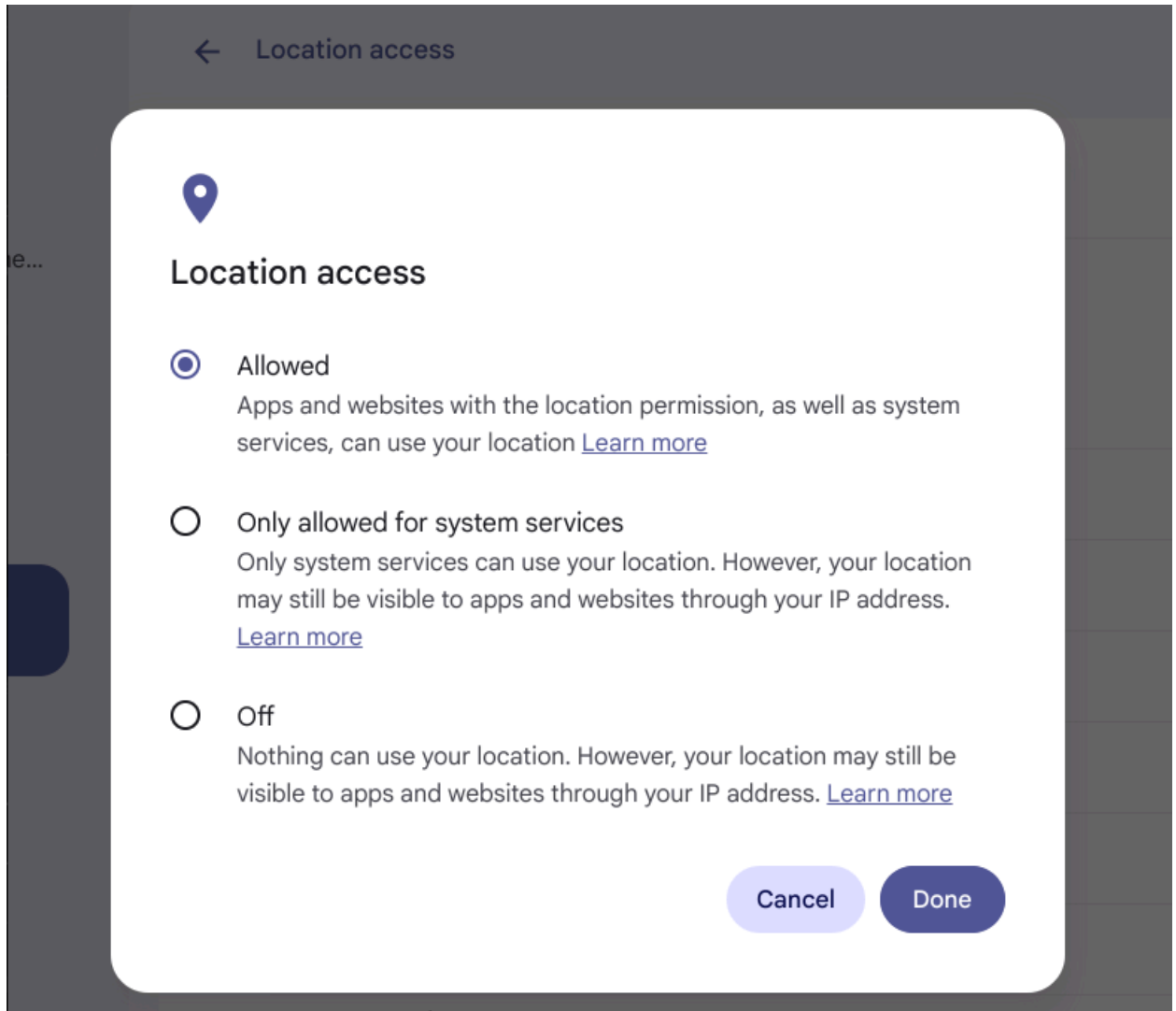
As a ChromeOS administrator, you can now activate **Data processor mode**, which covers a set of ChromeOS features and services referred to as **Essential Services**.

Privacy controls: Geolocation

Privacy on ChromeOS devices is now easier to manage by adding the ability to control geolocation access to the **Settings > Privacy and security > Privacy controls** page. Users

can now set geolocation access to **Allowed**, **Only allowed for system services**, or **Off**, depending on their preference.

We allow users to block all apps or websites, or entire systems access to geolocation regardless of previously granted permissions, and provide users easy to use controls to re-enable them whenever it would be helpful.



We've added a new policy, [GoogleLocationServicesEnabled](#). This controls the availability of geolocation on the device inside of user sessions. Unlike the now deprecated policy below, it affects the entire system, not just the Android VM (Arc).

Deprecation notice (6 months): [ArcGoogleLocationServicesEnabled](#)

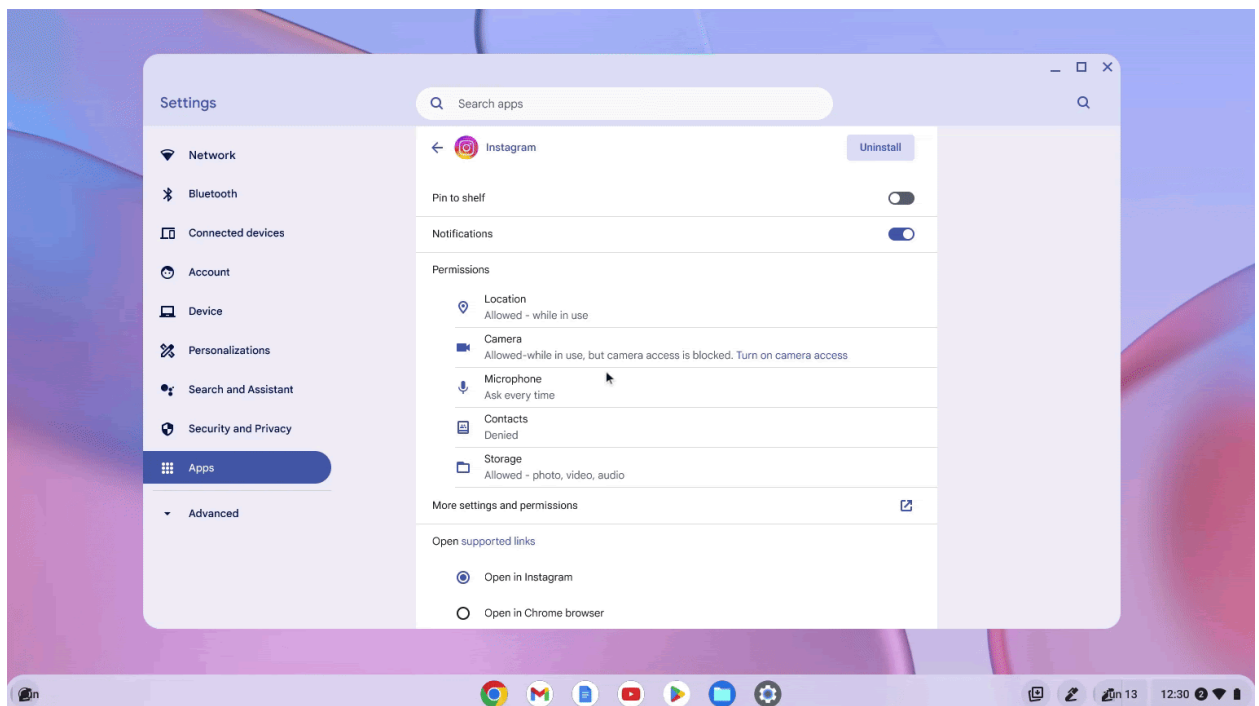
This is being deprecated in favor of the added [GoogleLocationServicesEnabled](#) policy, as it

covers the entire system and not just Android VM (Arc). Additionally, we are modifying the effect of the [DefaultGeolocationSetting](#) to no longer affect the system geolocation setting.

ChromeOS privacy control reminders on Apps settings page

To use the cameras and microphones on ChromeOS, you need to turn on both privacy controls and app permissions in two separate places.

We are making it easier for users to be aware of the states of the privacy controls and provide actionable reminders on the ChromeOS **Apps** settings page so that users have a smoother experience. To view the ChromeOS **Apps** settings page, click **Settings > Apps > Manage your Apps**, and select the desired app.

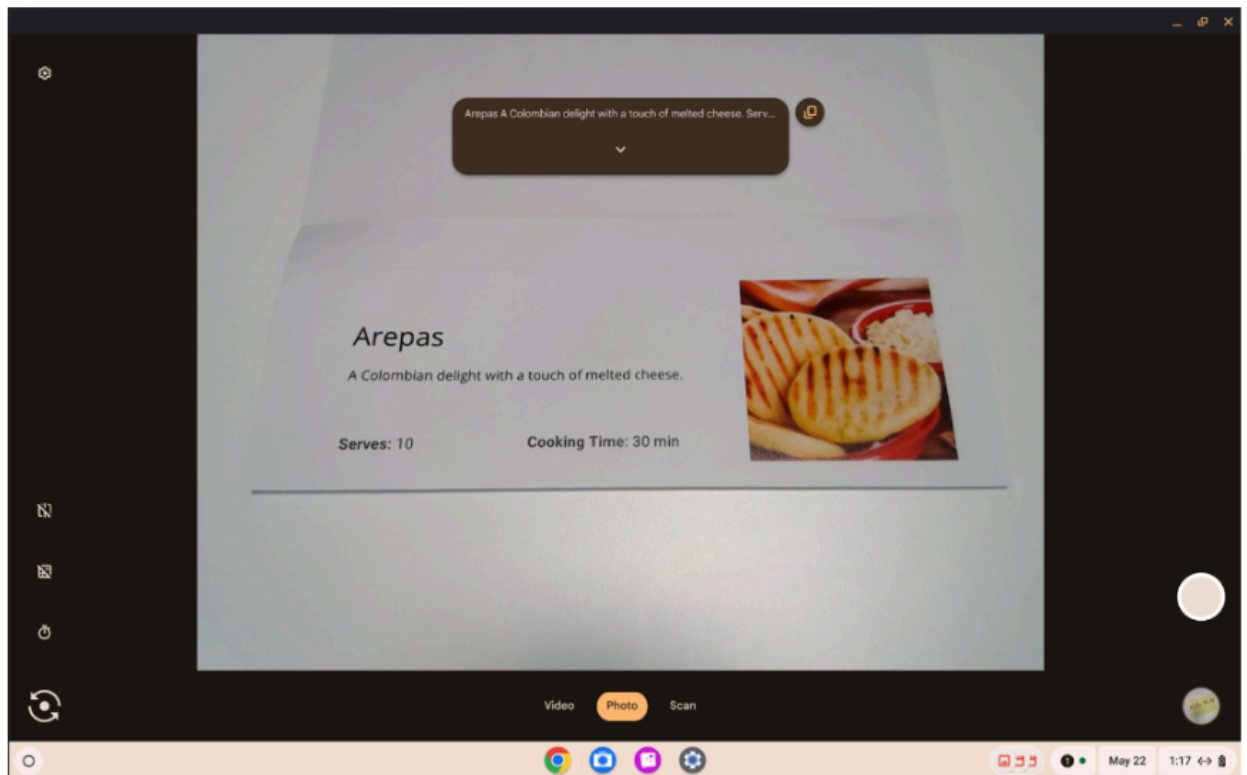


Store aggregated vitals data with one-year retention

From ChromeOS 128 onwards, we store aggregated vitals data for one-year retention to better track the progress over time. Vitals data includes Android app performance metrics, such as crash rate, and these metrics will help us improve Android app performance on ChromeOS devices.

OCR in ChromeOS Camera App

Optical Character Recognition (OCR) enables text extraction from images captured in the ChromeOS Camera App by integrating an ML-powered text extraction service. ChromeOS 128 supports 77 languages; it also supports both horizontal and vertical detection. This allows copying and searching text from images, speaking text from images by screen reader, and creating searchable PDFs from images. By default, text detection in Photo mode is disabled and can be enabled from **Settings > Text detection in preview**.

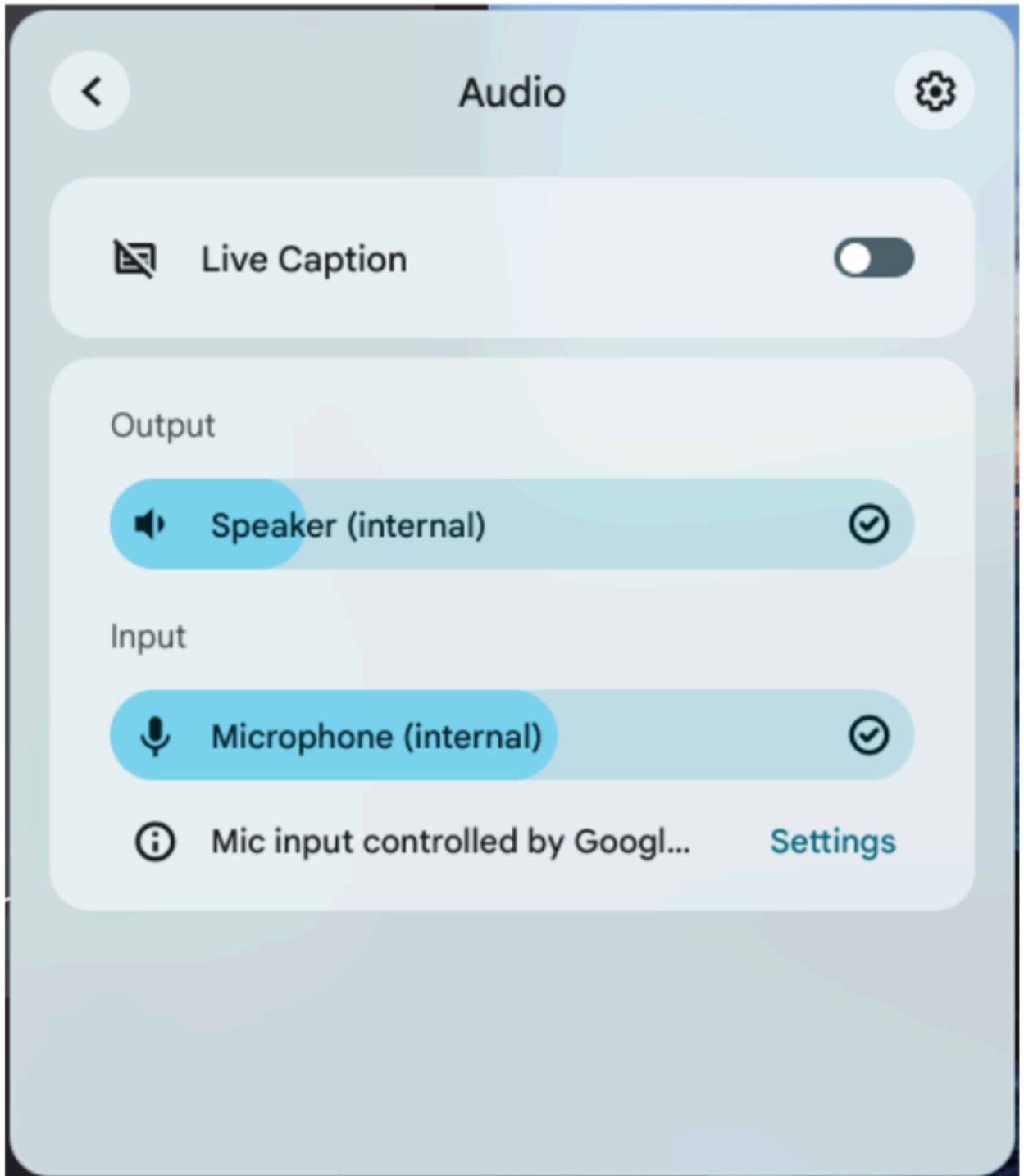


Magnifier follows ChromeVox

Magnifier following ChromeVox is designed for people who are blind or have low vision. When you read text aloud using ChromeVox, the screen magnifier now automatically follows the words, so you never lose your place. To try this out, you can enable both Magnifier and ChromeVox in your settings. Zoom in to your preferred zoom level using **Ctrl + Alt + Brightness up** and **Ctrl + Alt + Brightness down**. A setting is available under the Magnifier settings to adjust this behavior.

Auto Gain Control enabled by default

Auto Gain Control (AGC) allows apps, such as video calling apps, to automatically optimize microphone volume for best audio quality. When auto gain control is enabled and in-use, a message appears in the quick settings panel to inform the user that the microphone gain slider is being overridden. AGC is enabled by default in ChromeOS 128. If you want to manually control the microphone volume even for apps that support AGC, you can go to **Settings > Device > Audio** and deselect **Allow apps to automatically adjust mic volume**.



APN management

For Chrome OS cellular-enabled devices, we have made it easier to view, manage, and add Access Point Names (APNs). We've also improved registration failure handling and

messaging.

Pinned notifications on ChromeOS

ChromeOS notifications help to visually separate pinned notifications from other notifications. ChromeOS 128 significantly differentiates the visual look of pinned notifications from typical notifications to reflect their significant difference - we notify the user of an ongoing process rather than an instantaneous event.

Admin console updates

Chrome profile separation - new deployment guide

In Chrome 127, we launched 3 new policies to help you control profile separation in your organization: [ProfileSeparationSettings](#), [ProfileSeparationDataMigrationSettings](#) and [ProfileSeparationDomainExceptionList](#).

In addition to these policies, we also now have a [detailed deployment guide](#).

- **Chrome 128 on Windows, Mac, Linux**

Chrome Enterprise Data Controls: Clipboard


Data Controls are lightweight rules in the Admin console that set a Chrome policy to control security-sensitive user actions like file attachments, downloads, copy and paste actions, and printing. Chrome blocks or warns the user when these actions happen by applying those rules locally.

Chrome 128 releases the clipboard protection parts of Data Controls, that is, copy and paste actions. Other protections are planned in future releases.

You can control this feature with the [DataControlsRules](#) policy.

- **Chrome 128 on ChromeOS, Linux, Mac, Windows**

Copying from this site is not allowed

 Your administrator has blocked this action

Ok

Pasting this content to this site is not allowed

 Your administrator has blocked this action

OK

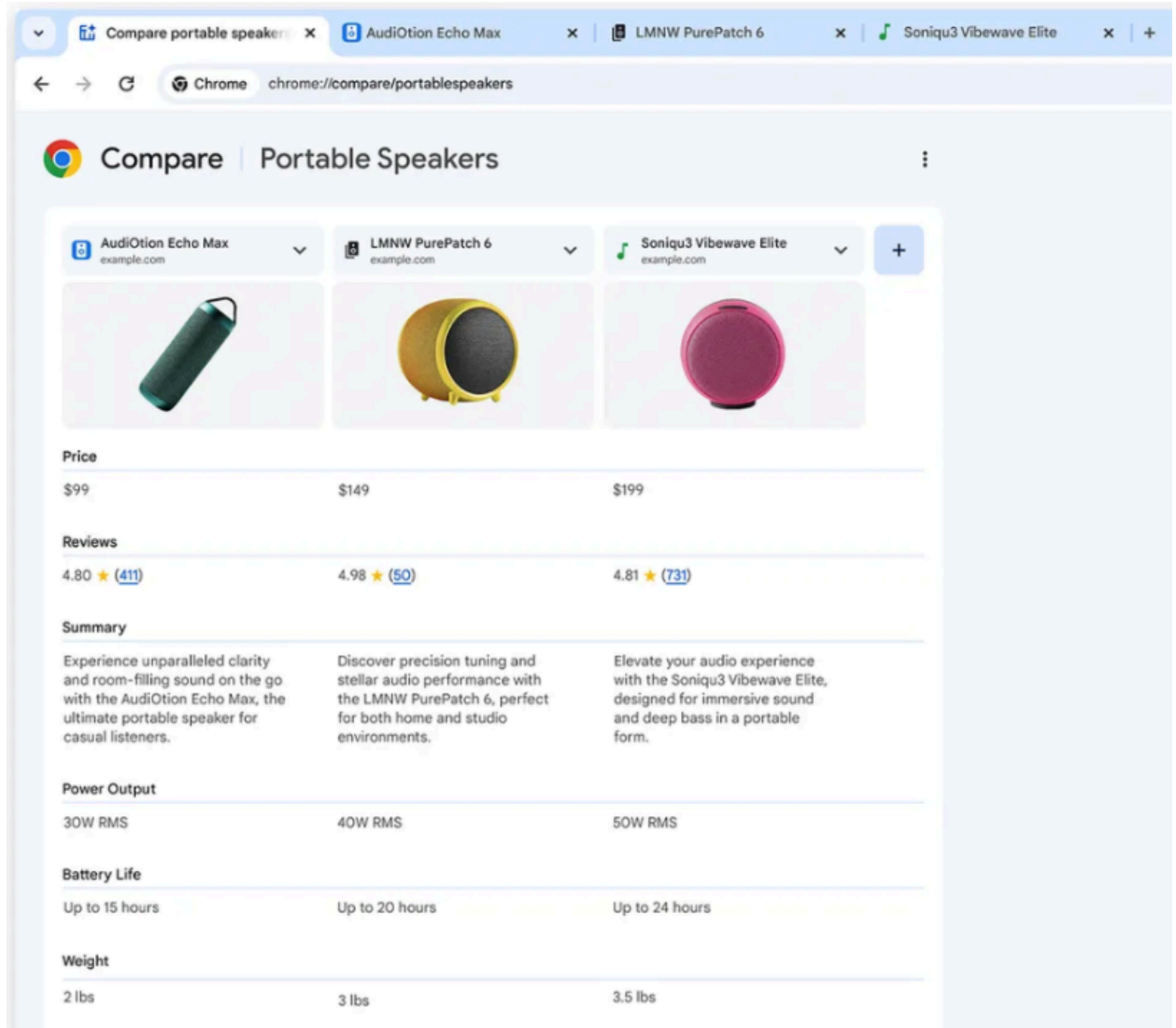
Coming soon

Upcoming Chrome browser updates

Tab compare

Starting in Chrome 129 (US-only), we will introduce **Tab compare**, a new feature that presents an AI-generated overview of products from across multiple tabs, all in one place. This feature will be controlled through the TabCompareSettings policy.

- **Chrome 129 on Linux, Mac, Windows**



Ad-hoc code signatures for PWA shims on macOS

Code signatures for application shims that are created when installing a Progressive Web App (PWA) on macOS are changing to use ad-hoc code signatures, which are created when the application is installed. The code signature is used by macOS as part of the application's identity. These ad-hoc signatures will result in each PWA shim having a unique identity to macOS; currently every PWA looks like the same application to macOS.

This will address problems when attempting to include multiple PWAs in the macOS **Open at Login** preference pane, and will permit future improvements for handling user notifications within PWAs on macOS.

- **Chrome 129 on Mac**

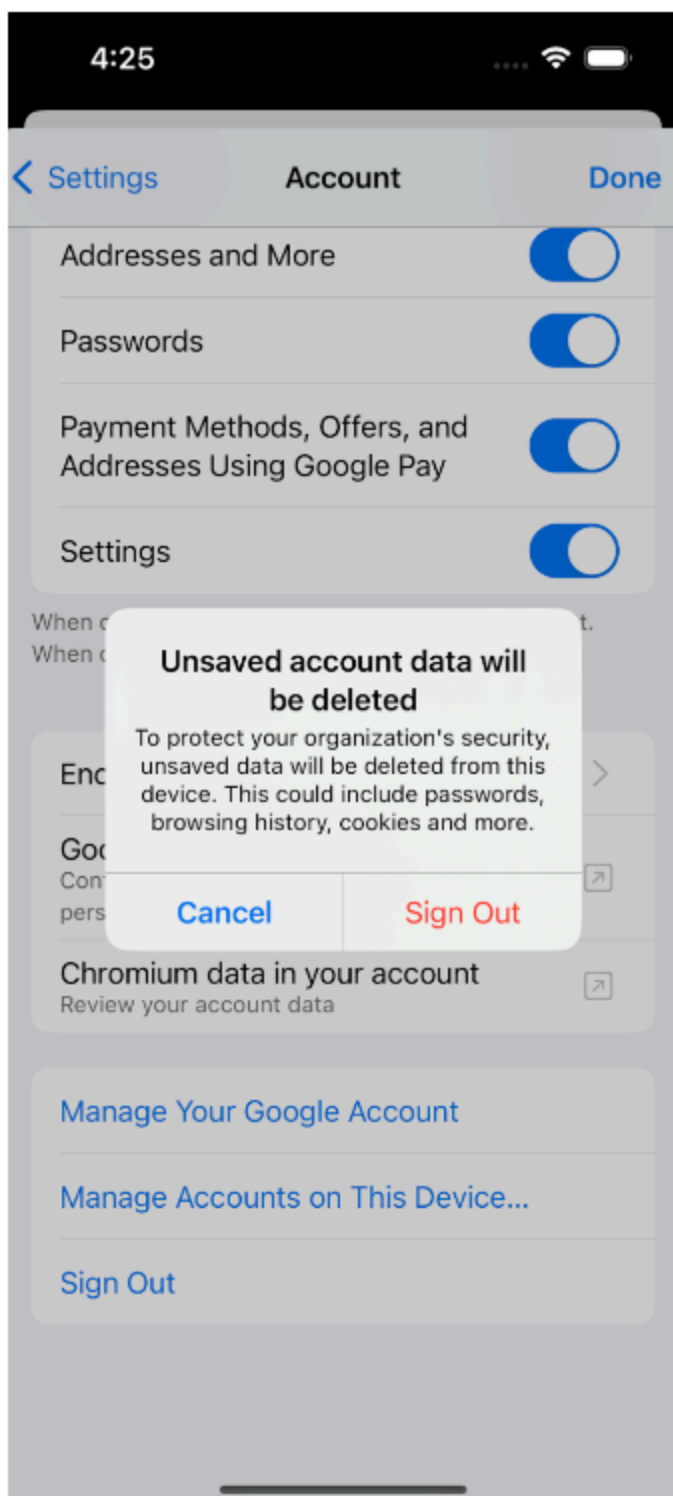
Clear device data on sign out on iOS

Starting in Chrome 129, signing out from a managed account in an unmanaged browser will delete browsing data that is saved on the device. Managed users will be presented a confirmation dialog on sign-out explaining that the data will be cleared. Data will be cleared only from the time of sign-in, otherwise all data will be cleared; time of sign-in is only known if the user signed in on Chrome 122 or later.

The data that will be deleted includes:

- browsing history
- cookies and site data
- passwords
- site settings
- autofill
- cached images and files

- **Chrome 129 on iOS**



Fallback styles for <meter> elements

As early as Chrome 129, [HTML5 <meter> elements](#) with ``appearance: none`` will have a reasonable fallback style that matches Safari and Firefox instead of just disappearing from the page. In addition, developers will be able to custom style the <meter> elements.

A temporary policy **MeterAppearanceNoneFallbackStyle** will be available until Chrome 133 to control this feature.

- **Chrome 129 on Windows, Mac, Linux, Android**

Chrome will no longer support macOS 10.15

Chrome will no longer support macOS 10.15, which is already outside of its support window with Apple. Users have to update their operating systems in order to continue running Chrome browser. Running on a supported operating system is essential to maintaining security. If run on macOS 10.15, Chrome continues to show an infobar that reminds users that Chrome 129 will no longer support macOS 10.15.

- **Chrome 129 on Mac:** Chrome no longer supports macOS 10.15

Deprecate Safe Browsing Extended reporting

Safe Browsing Extended reporting is a feature that enhances the security of all users by collecting telemetry information from participating users that is used for Google Safe Browsing protections. The data collected includes URLs of visited web pages, limited system information, and some page content. However, this feature is now superseded by **Enhanced protection** mode. We suggest users switch to **Enhanced protection** to continue providing security for all users in addition to enabling the strongest security available in Chrome. For more information, see [Safe Browsing protection levels](#).

Safe Browsing

Enhanced protection

- ☒ Real-time, proactive protection against dangerous sites, downloads, and extensions that's based on your browsing data getting sent to Google



When on

- II. Warns you about dangerous sites, even ones Google didn't know about before, by analyzing more data from sites than standard protection. You can choose to skip Chrome warnings.
- ⬇ In-depth scans for suspicious downloads.
- 🛡 When you're signed in, protects you across Google services.
- 🌐 Improves security for you and everyone on the web.
- 🔑 Warns you if you use a password that has been compromised in a data breach.

Things to consider

- 📡 Sends the URLs of sites you visit and a small sample of page content, downloads, extension activity, and system information to Google Safe Browsing to check if they're harmful.
- 🔗 When you're signed in, this data is linked to your Google Account to protect you across Google services, for example increasing protection in Gmail after a security incident.
- ✅ Doesn't noticeably slow down your browser or device.

Learn more about [how Chrome keeps your data private](#)

Standard protection

Protects against sites, downloads, and extensions that are known to be dangerous.

- ☐ When you visit a site, Chrome sends an obfuscated portion of the URL to Google through a privacy server that hides your IP address. If a site does something suspicious, full URLs and bits of page content are also sent.



Help improve security on the web for everyone

Sends URLs of some pages you visit, limited system information, and some page content to Google, to help discover new threats and protect everyone on the web.



Warn you if a password was compromised in a data breach

When you use a password, Chrome warns you if it has been published online. When doing this, your passwords and usernames are encrypted, so they can't be read by anyone, including Google.



No protection (not recommended)

- ☐ Does not protect you against dangerous websites, downloads, and extensions. Your Safe Browsing settings in other Google products won't be affected.



Advanced

- **Chrome 129 on Android, iOS, ChromeOS, Linux, Mac, Windows:** Deprecation of Safe Browsing Extended Reporting

New option in `HttpsOnlyMode` policy

Ask Before HTTP (ABH), formerly named HTTPS Only/First Modes, is a setting that tells Chrome to ask for user consent before sending insecure HTTP content over the wire. The [HttpsOnlyMode](#) policy allows force-enabling, or force-disabling, ABH.

In Chrome 129, we are adding a new middle-ground variant of ABH called *balanced mode*. This variant aims to reduce user inconvenience by working like (strict) ABH most of the time, but not asking when Chrome knows that an HTTPS connection isn't possible, such as when connecting to a single-label hostname like `internal/`.

We are adding a *force_balanced_enabled* policy option to allow force-enabling this new variant. Setting *force_balanced_enabled* on browsers before Chrome 129 will result in the default behavior, which places no enterprise restrictions on the ABH setting.

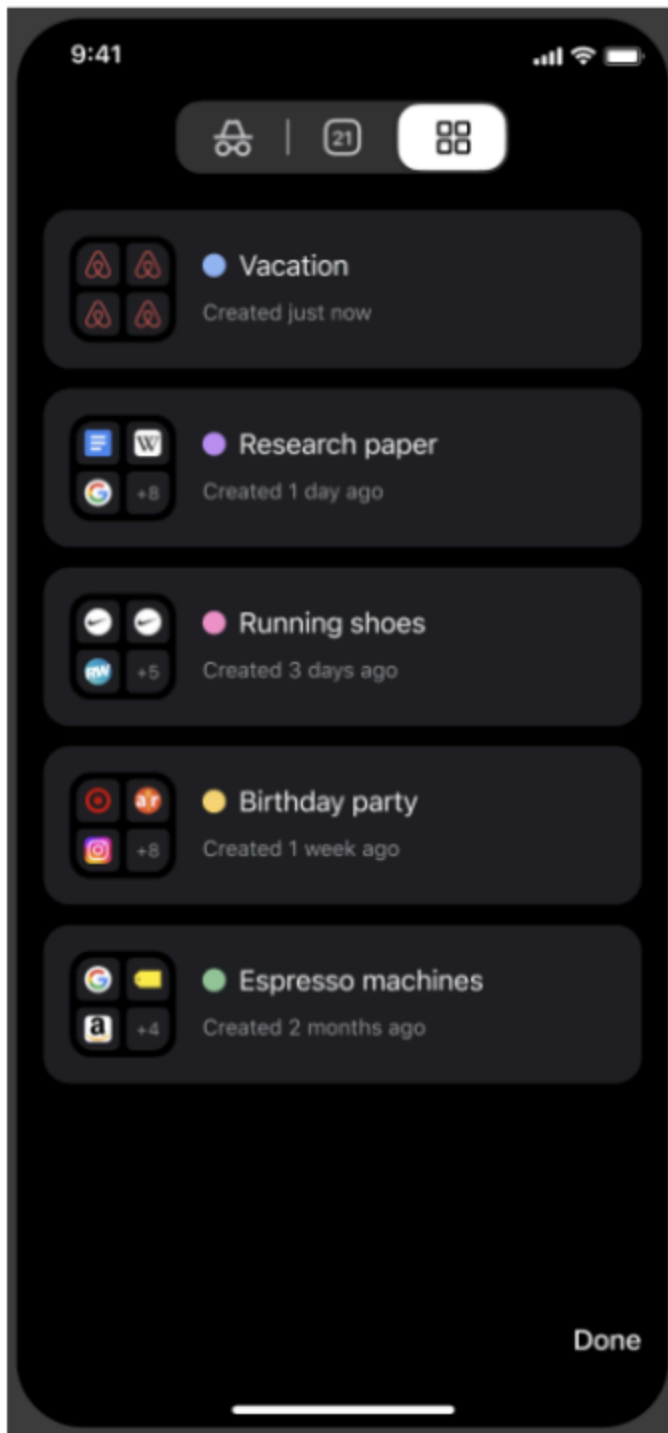
To avoid unexpected impact, if you have previously set *force_enabled*, we recommend not setting *force_balanced_enabled* until your entire fleet has upgraded to Chrome 129 or higher. If you are not migrating from *force_enabled* to *force_balanced_enabled*, you will be unaffected by this change.

- **Chrome 129 on Android, ChromeOS, LaCrOS, Linux, Mac, Windows, Fuchsia**

Sync Tab Group

The tab groups on iOS will now be saved. Closing a tab group will no longer delete it. For users syncing their tabs across devices, the groups will also sync.

- **Chrome 129 on iOS**



Update Google Play Services to fix issues with on-device passwords

Users with old versions of Google Play Services will experience reduced functionality with their on-device passwords, and Password Manager might soon stop working for them

altogether. These users will need to update Play Services, or will be guided through other troubleshooting methods depending on their state. This is part of an ongoing migration that only affects Android users of Password Manager.

- **Chrome 129 on Android**

Deprecate of non-standard declarative shadow DOM serialization

The prototype implementation, which was shipped in 2020 and then updated in 2023, contained a method called ``getInnerHTML()`` that could be used to serialize DOM trees containing shadow roots. That part of the prototype was not standardized with the rest of the declarative shadow DOM, and has only recently reached spec consensus (for details, see [Github](#)). As part of that consensus, the shape of the `getInnerHTML` API changed.

This feature represents the deprecation of the previously shipped ``getInnerHTML()`` method. The replacement is called ``getHTML()``, which shipped in Chrome 125. For details, see this [ChromeStatus feature description](#).

- **Chrome 129 on Windows, Mac, Linux, Android**

Deprecate the `includeShadowRoots` argument on `DOMParser`

The `includeShadowRoots` argument was a never-standardized argument to the `DOMParser.parseFromString()` function, which was there to allow imperative parsing of HTML content that contains declarative shadow DOM. This was shipped in [Chrome 90](#) as part of the initial shipment of declarative shadow DOM. Since the standards discussion rematerialized in 2023, the shape of DSD APIs changed, including this feature for imperative parsing. To read more, see details of the [context on the related standards](#), and information is also available on the related deprecations of [shadow DOM serialization](#) and [shadow root attribute](#).

Now that a standardized version of this API, in the form of [setHTMLUnsafe\(\)](#) and [parseHTMLUnsafe\(\)](#) shipped in Chrome 124, the non-standard `includeShadowRoots`

argument needs to be deprecated and removed. All usage should shift accordingly:

Instead of:

```
(new  
DOMParser()).parseFromString(html, 'text/html', {includeShadowRoots:  
true});
```

This can be used instead:

```
document.parseHTMLUnsafe(html);
```

- **Chrome 129 on Linux, Mac, Windows, Android**

Rename inset-area to position-area

The CSS working group ([CSSWG](#)) resolved to rename this property from `inset-area` to `position-area`. See the CSSWG discussion in [Github](#).

Chrome has decided to release an interoperable solution, by supporting both property names. We will ship the new property name, `position-area`, as a synonym for `inset-area` first. Then after a suitable amount of time, we will remove `inset-area`. The latter removal will be done under a separate Intent.

- **Chrome 129 on Windows, Mac, Linux, Android**

Entrust certificate distrust

In response to sustained compliance failures, Chrome 127 changes how publicly-trusted TLS server authentication, that is, websites or certificates issued by Entrust, are trusted by default. This applies to Chrome 127 and later on Windows, macOS, ChromeOS, Android, and Linux; iOS policies do not allow use of the Chrome Root Store in Chrome for iOS.

Specifically, TLS certificates validating to the Entrust root CA certificates included in the Chrome Root Store and issued:

- after October 31, 2024, will no longer be trusted by default.
- on or before October 31, 2024, will be unaffected by this change.

If a Chrome user or an enterprise explicitly trusts any of the affected Entrust certificates on a platform and version of Chrome relying on the Chrome Root Store, for example, when explicit trust is conveyed through a Windows Group Policy Object, the Signed Certificate Timestamp (SCT) constraints described above will be overridden and certificates will function as they do today.

For additional information and testing resources, see [Sustaining Digital Certificate Security - Entrust Certificate Distrust](#).

To learn more about the Chrome Root Store, see this [FAQ](#).

- Chrome 127 on Android, ChromeOS, Linux, Mac, Windows: All versions of Chrome 127 and higher that rely on the Chrome Root Store will honor the blocking action, but the blocking action will only begin for certificates issued after October 31, 2024.
- **Chrome 130 on ChromeOS, Linux, Mac, Windows:** The blocking action will begin for certificates issued after October 31, 2024. This will also affect Chrome 127, 128 and 129.

Support non-special scheme URLs

Chrome 130 will support non-special scheme URLs correctly. Previously, Chromium's URL parser doesn't support non-special URLs. The parser parses non-special URLs as if they had an "opaque path", which is not aligned with the URL Standard. Now, Chromium's URL parser parses non-special URLs correctly, following the URL Standard. For more details, see [Support Non-Special Scheme URLs](#).

- **Chrome 130 on Windows, Mac, Linux, Android**

Network Service on Windows will be sandboxed

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. You can use the [Chromium bug tracker](#) to report any issues you encounter.

- **Chrome 130 on Windows:** Network Service sandboxed on Windows

Chrome Third-Party Cookie Deprecation (3PCD)

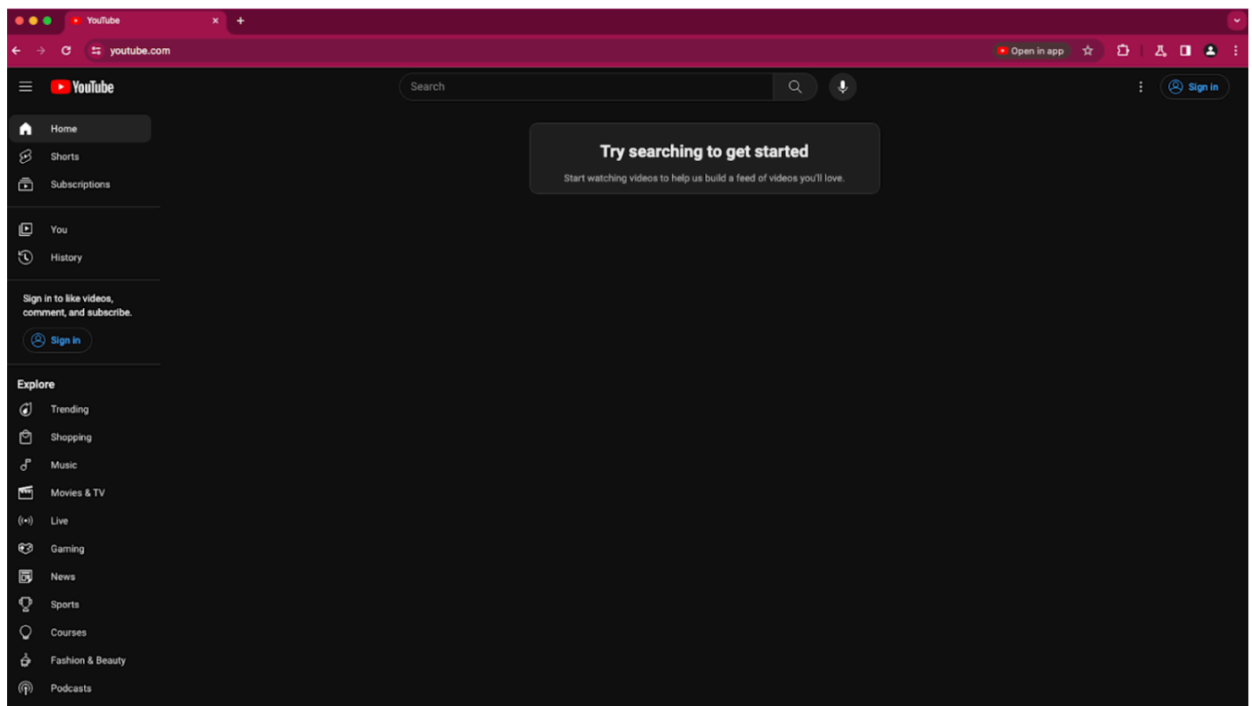
On July 22nd, we announced a new path forward for Privacy Sandbox on the web. Instead of deprecating third-party cookies, we would introduce a new experience in Chrome that lets people make an informed choice that applies across their web browsing, and they'd be able to adjust that choice at any time. We're discussing this new path with regulators, and will engage with the industry as we roll this out.

For more details, see this [Privacy Sandbox update](#).

User Link capturing on PWAs

Web links automatically direct users to installed web apps. To better align with users' expectations around installed web apps, Chrome makes it easier to move between the browser and installed web apps. When the user clicks a link that could be handled by an installed web app, Chrome adds a chip in the address bar to suggest switching over to the app. When the user clicks the chip, this either launches the app directly, or opens a grid of apps that can support that link. For some users, clicking a link always automatically opens the app.

- **Chrome 121 on Linux, Mac, Windows:** When some users click a link, it always opens in an installed PWA, while some users see the link open in a new tab with a chip in the address bar, clicking on which will launch the app. A flag is available to control this feature: `chrome://flags/#enable-user-link-capturing-pwa`.
- **Chrome 130 on Linux, Mac, Windows:** Launch to 100% of Stable with either a default on (always launch apps on link clicks) or a default off (always open in a tab, only launch if the user clicks on chip on address bar).



Private network access checks for navigation requests: warning-only mode

Before a website A navigates to another site B in the user's private network, this feature does the following:

1. Checks whether the request has been initiated from a secure context.
2. Sends a preflight request, and checks whether B responds with a header that allows private network access.

There are already features for subresources and workers, but this one is for navigation requests specifically. These checks protect the user's private network.

Since this feature is the *warning-only* mode, we do not fail the requests if any of the checks fail. Instead, a warning will be shown in the DevTools console, to help developers prepare for the coming enforcement.

- **Chrome 130 on Windows, Mac, Linux, Android**

Insecure form warnings on iOS

Chrome 125 started to block form submissions from secure pages to insecure pages on iOS. When Chrome detects an insecure form submission, it now displays a warning asking the user to confirm the submission. The goal is to prevent leaking of form data over plain text without user's explicit approval. A policy [InsecureFormsWarningsEnabled](#) is available to control this feature, and will be removed in Chrome 130.

- Chrome 125 on iOS: Feature rolls out
- **Chrome 130 on iOS:** InsecureFormsWarningsEnabled policy will be removed

Chrome extension telemetry integration with Chronicle

As early as Chrome 131, we will begin to collect relevant extension telemetry data from within Chrome, for managed profiles and devices, and send it to [Chronicle](#). Chronicle will analyze the data to provide instant analysis and context on risky activity.

- **Chrome 131 on ChromeOS, LaCrOS, Linux, Mac, Windows**

Remove enterprise policy used for legacy same site behavior

In Chrome 79, we introduced the [LegacySameSiteCookieBehaviorEnabledForDomainList](#) policy to revert the SameSite behavior of cookies to legacy behavior on the specified domains. The [LegacySameSiteCookieBehaviorEnabledForDomainList](#) policy's lifetime has been extended and will be removed on the milestone listed below.

- **Chrome 132 on Android, ChromeOS, Linux, Mac, Windows:** Remove [LegacySameSiteCookieBehaviorEnabledForDomainList](#) policy

X25519Kyber768 key encapsulation for TLS

Starting in Chrome 124, Chrome enables by default on all desktop platforms a new post-quantum secure TLS key encapsulation mechanism X25519Kyber768, based on a NIST

standard (ML-KEM). This protects network traffic from Chrome with servers that also support ML-KEM from decryption by a future quantum computer. This is exposed as a new TLS cipher suite. TLS automatically negotiates supported ciphers, so this change should be transparent to server operators. This cipher will be used for both TLS 1.3 and QUIC connections.

However, some TLS middleboxes might be unprepared for the size of a Kyber (ML-KEM) key encapsulation, or a new TLS ClientHello cipher code point, leading to dropped or hanging connections. This can be resolved by updating your middlebox, or disabling the key encapsulation mechanism via the temporary [PostQuantumKeyAgreementEnabled](#) enterprise policy, which will be available through the end of 2024. However, long term, post-quantum secure ciphers will be required in TLS and the enterprise policy will be removed.

Post-quantum cryptography is required for CSNA 2.0.

For more detail, see this [Chromium blog](#) post.

- Chrome 124 on Windows, Mac, Linux
- **Chrome 135 on Android**

UI Automation accessibility framework provider on Windows

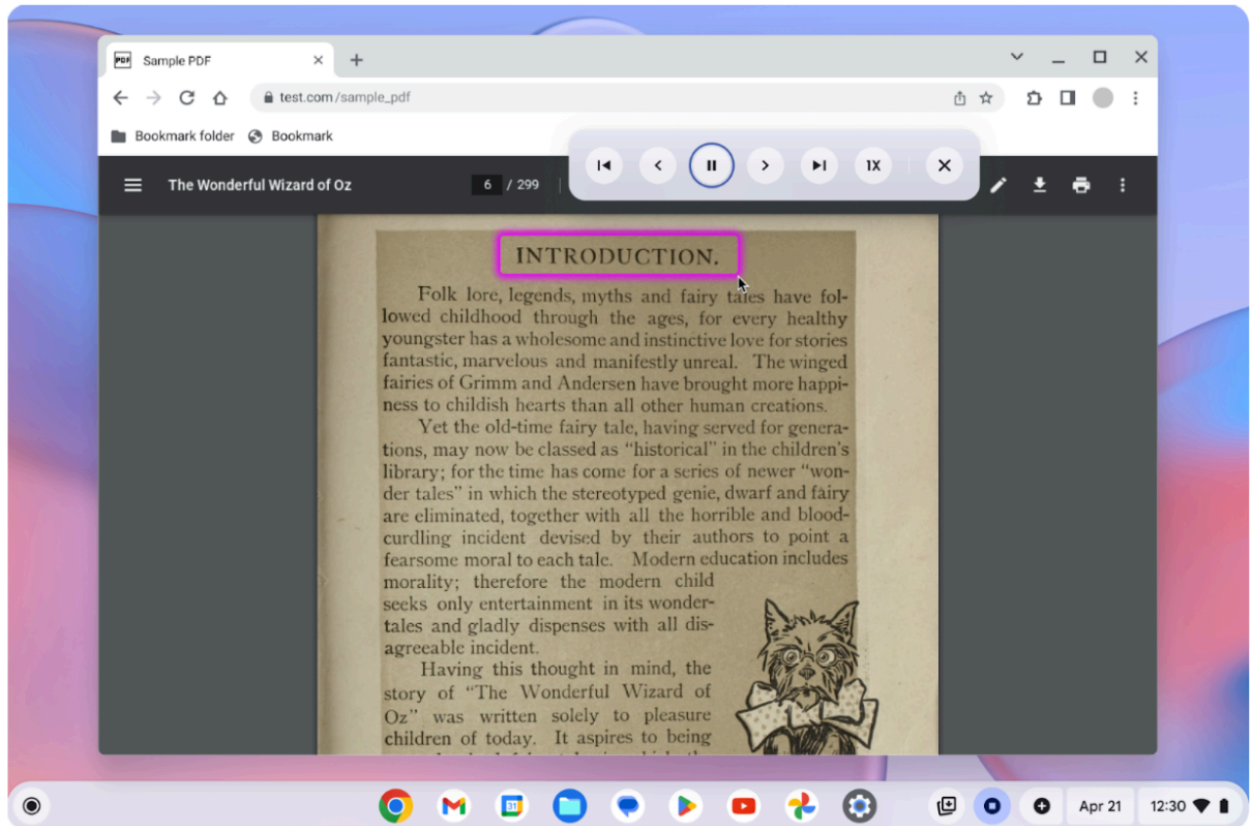
Starting in Chrome 126, Chrome will start directly supporting accessibility client software that uses Microsoft Windows's UI Automation accessibility framework. Prior to this change, such software interoperated with Chrome by way of a compatibility shim in Microsoft Windows. This change is being made to improve the accessible user experience for many users. It provides complete support for Narrator, Magnifier, and Voice Access; and will improve third-party apps that use Windows's UI Automation accessibility framework. Users of Chrome will find reduced memory usage and processing overhead when used with accessibility tools. It will also ease development of software using assistive technologies. Administrators might use the [UiAutomationProviderEnabled](#) enterprise policy, available from Chrome 125, to either force-enable the new provider (so that all users receive the new functionality), or disable the new provider. This policy will be supported through Chrome 136, and will be removed in Chrome 137. This one-year period is intended to give enterprises sufficient time to work with third-party vendors so that they may fix any incompatibilities resulting from the switch from Microsoft's compatibility shim to Chrome's UI Automation provider.

- Chrome 125 on Windows: The [UiAutomationProviderEnabled](#) policy is introduced so that administrators can enable Chrome's UI Automation accessibility framework provider and validate that third-party accessibility tools continue to work.
- Chrome 126 on Windows: The Chrome variations framework will be used to begin enabling Chrome's UI Automation accessibility framework provider for users. It will be progressively enabled to the full stable population, with pauses as needed to address compatibility issues that can be resolved in Chrome. Enterprise administrators may continue to use the [UiAutomationProviderEnabled](#) policy to either opt-in early to the new behavior, or to temporarily opt-out through Chrome 136.
- **Chrome 137 on Windows:** The [UiAutomationProviderEnabled](#) policy will be removed from Chrome. All clients will use the browser's UI Automation accessibility framework provider.

Upcoming ChromeOS changes

Update to keyboard shortcut for Select-to-speak

On Chromebooks, the Select-to-speak keyboard shortcut (Search + s) now works when it is first pressed. As early as ChromeOS 129, you will no longer need to enable it first in **Settings > Accessibility > Text-to-Speech > Select-to-speak**. A dialog appears confirming that you want to turn on Select-to-speak the first time you press the keyboard shortcut.



Chrome Enterprise Premium for file transfers on Managed Guest Sessions

As early as ChromeOS 129, organizations will be able to extend Chrome Enterprise Premium's powerful scanning and content and context-based protection to local files on ChromeOS on Managed Guest Sessions.

For example, a misplaced file containing Social Security numbers is instantly blocked when a user attempts to copy it to an external drive, safeguarding this confidential information.

ChromeOS XDR Window Events

In ChromeOS 130, window focus events will be available as part of Extended Threat Detection and Response (XDR) on ChromeOS. You will be able to bring windows into focus activities of devices in your managed fleet by simply updating XDR events in the Admin console!

Generative AI wallpapers and video conference backgrounds

As early as ChromeOS 130, we plan to introduce high-resolution, generative AI wallpapers on ChromeOS. With this feature, you can unleash your creativity and turn your Chromebook into a canvas of personal expression. Choose from a diverse collection of templates and, in just a few clicks, infuse your Chromebook with your unique personality, mood, or interest.

Two new policies will be available to control these features; **GenAIVcBackgroundSettings** and **GenAIWallpaperSettings**.

Upcoming Admin console changes

Chrome browser managed profile reporting

Chrome Enterprise Core will introduce new Chrome browser managed profile reporting in the Admin console. This feature will provide a new Managed profile listing and detail pages. On these pages, IT administrators will be able to find reporting information on managed profiles such as profile details, browser versions, policies applied, and more.

- **Chrome 130 on Android, Linux, Mac, Windows**

Admin console widget for data controls

A new settings widget in the Admin console allows users to configure data controls policies for specific URLs.

- **Chrome 128 on ChromeOS, Linux, Mac, Windows**

Default change for GenAI policies

Starting with 130, we will change the default setting for GenAI policies from switched off to allowed, without improving AI models. This doesn't impact age restrictions on access to any relevant GenAI features. The existing policies that will have the updated default setting are:

- [CreateThemesSettings](#)
- [DevToolsGenAiSettings](#)
- [HelpMeWriteSettings](#)
- [HistorySearchSettings](#)
- [TabOrganizerSettings](#)

Previous release notes

Chrome version & targeted Stable channel release date	PDF
Chrome 127: July 17, 2024	PDF
Chrome 126: June 5, 2024	PDF
Chrome 125: May 8, 2024	PDF
Chrome 124: April 10, 2024	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](#)

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.