



Chrome 129 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 September 11, 2024.

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

Chrome 129 release summary	2
Current Chrome version release notes	5
Chrome browser updates	5
ChromeOS updates	16
Admin console updates	19
Coming soon	20
Upcoming Chrome browser updates	20
Upcoming ChromeOS changes	27
Upcoming Admin console changes	27
Additional resources	30
Still need help?	30

Chrome 129 release summary

Chrome browser updates	Security / Privacy	User productivity / Apps	Management
Tab compare		✓	
Chrome no longer support macOS 10.15	✓		✓
Ad-hoc code signatures for PWA shims on macOS		✓	
Certificate Manager on Windows and macOS	✓		
Chrome Security Insights	✓		✓
Deprecate Safe Browsing Extended reporting	✓		
Inactive tabs on Android		✓	
New option in HttpsOnlyMode policy	✓		✓
Screenshot protections	✓		
Sync tab group		✓	
Google Play Services fixes issues with on-device passwords			✓
Deprecation of non-standard declarative shadow DOM serialization	✓		
Deprecate the includeShadowRoots argument on DOMParser	✓		
Rename inset-area to position-area	✓		
Clear local device data on sign out on iOS	✓		

Toolbar customization		✓	
Google Password Manager Passkey usage on ChromeOS		✓	
New and updated policies in Chrome browser			✓
ChromeOS updates	Security/Privacy	User productivity/Apps	Management
Chrome Enterprise Premium for file transfers on Managed Guest Sessions	✓		
Educators Appreciation wallpaper		✓	
Display brightness controls		✓	
Peripheral Welcome experience		✓	
Managed accounts no longer sync'd as secondary accounts on Android	✓		✓
Live Translate		✓	
Keyboard brightness controls		✓	
Keyboard shortcut for Select-to-Speak		✓	
PIN as an authentication factor	✓		
Automatic reload of sign-in screen	✓		
CSE Workspace file types now supported in Google Drive			✓
Battery Icon updates		✓	
Admin console updates	Security/Privacy	User productivity/Apps	Management
Extension Risk Score on the Apps and Extensions Usage report			✓
Upcoming Chrome browser updates	Security / Privacy	User productivity / Apps	Management

Entrust certificate distrust	✓		
Fallback styles for <meter> element	✓		
Compression dictionary transport with Shared Brotli and Shared Zstandard	✓		
Keyboard-focusable scroll containers		✓	
Support non-special scheme URLs	✓		
Simplified sign-in and sync experience		✓	
Chrome extension telemetry integration with SecOps	✓		✓
User Link capturing on PWAs		✓	✓
Chrome Third-Party Cookie Deprecation (3PCD)	✓		
Insecure form warnings on iOS	✓		
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
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			✓
Default change for GenAI policies		✓	
Support for user-level settings on the Custom Configurations page			✓

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.

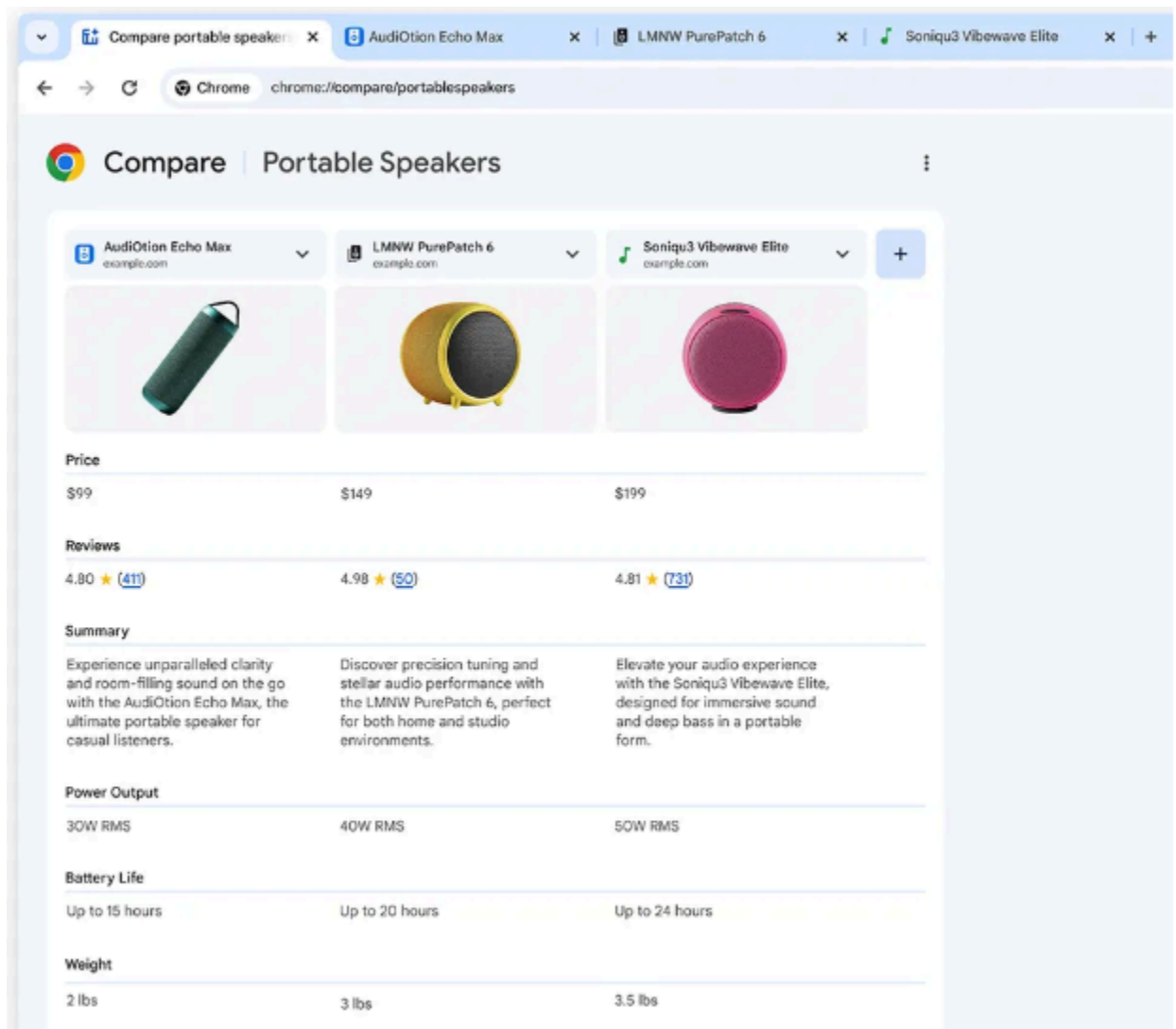
Current Chrome version release notes

Chrome browser updates

Tab compare

Starting in Chrome 129 (US-only), we introduce **Tab compare**, a new feature that presents an AI-generated overview of products from across multiple tabs, all in one place. This feature is controlled through the [TabCompareSettings](#) policy. Learn more in our [Help Center Article](#).

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



Chrome no longer supports macOS 10.15

Chrome 129 no longer supports 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 no longer supports macOS 10.15.

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

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

- **Chrome 129 on macOS**

Certificate Manager on Windows and macOS

As early as Chrome 129, there is a new certificate management settings screen accessible from security settings on Windows and macOS. This replaces the link to Windows cert manager and macOS keychain, respectively, although these operating system surfaces are still accessible from the certificate management settings page.

The certificate manager displays certificates that are trusted or distrusted by Chrome, including the contents of the Chrome Root Store, and any certificates that have been imported from the underlying operating system. Users can access the page directly by navigating to `chrome://certificate-manager`.

A future release will introduce user and enterprise management of certificates added directly to Chrome.

- **Chrome 129 on macOS, Windows**

Chrome Security Insights

You can now enable Chrome Security Insights, which allows you to monitor insider risk and data loss enhanced monitoring for Chrome activity if you have Chrome Enterprise Core and Workspace Enterprise Standard or Workspace Enterprise Plus with assigned licenses. For more information, see [Monitoring for insider risk and data loss](#).

- Chrome 125 on ChromeOS, Linux, macOS, Windows: Feature enabled for Chrome Enterprise Core
- **Chrome 129 on ChromeOS, Linux, macOS, Windows:** Feature enabled for EDU customers (except K-12)









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	Things to consider
<p> 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.</p> <p> In-depth scans for suspicious downloads.</p> <p> When you're signed in, protects you across Google services.</p> <p> Improves security for you and everyone on the web.</p> <p> Warns you if you use a password that has been compromised in a data breach.</p>	<p> 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.</p> <p> 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.</p> <p> Doesn't noticeably slow down your browser or device.</p> <p>Learn more about how Chrome keeps your data private</p>

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, macOS, Windows:** Deprecation of Safe Browsing Extended Reporting — Excluding real-time Client Safe Browsing Report Request

- Chrome 131 on Android, iOS, ChromeOS, Linux, macOS, Windows: Deprecating [SafeBrowsingExtendedReportingEnabled](#) for real-time Client Safe Browsing Report Request

Inactive tabs on Android

In Chrome 129, old tabs will be hidden 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 after being in this section for over 60 days.

- **Chrome 129 on Android:** Feature rolls out to 1%

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, macOS, Windows, Fuchsia**

Screenshot protections

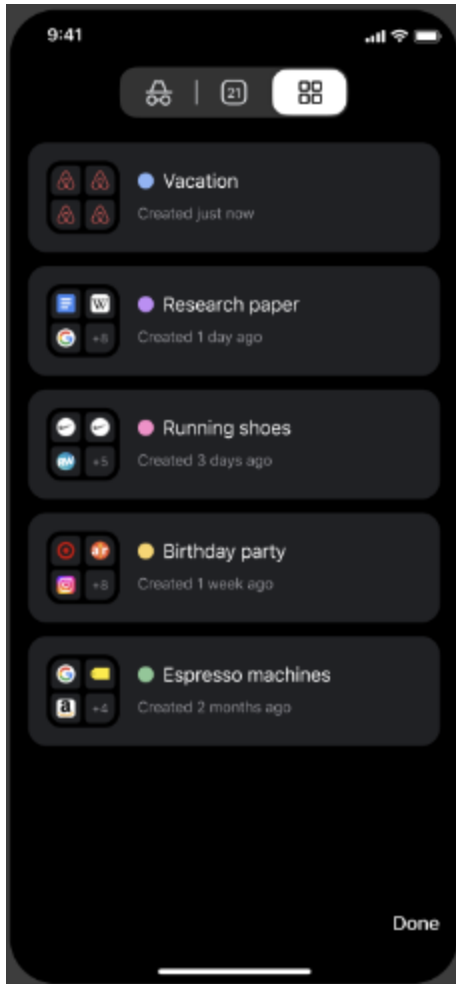
Screenshot protections allow Admins to prevent users from taking screenshots or screen sharing specific web pages considered to contain sensitive data. This feature is available to [Chrome Enterprise Premium](#) users only. This feature can be controlled via the same [EnterpriseRealTimeUrlCheckMode](#) Chrome Enterprise policy that enables all real-time URL lookups.

- **Chrome 129 on ChromeOS, Linux, macOS, Windows**

Sync tab group

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

- **Chrome 129 on iOS**



Google Play Services fixes issues with on-device passwords

Users with old versions of Google Play Services (<24w02) experience reduced functionality with their on-device passwords, and Password Manager might soon stop working for them altogether. These users need to update Play Services, otherwise they 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 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, macOS, Windows, Android**

Deprecation 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, macOS, Linux, Android**

Rename inset-area to position-area

The CSS working group ([CSSWG](#)) resolved to rename this property from ``inset-area`` to ``position-area``. For more details, see the CSSWG discussion in [Github](#). Chrome will support both the old and new property names for a few milestones, to help developers migrate to the new position-area name. We are shipping the new property name, ``position-area``, as a synonym for ``inset-area`` in Chrome 129 along with the deprecation DevTrial for ``inset-area``.

The ``inset-area`` property is currently planned for removal in Chrome 131.

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

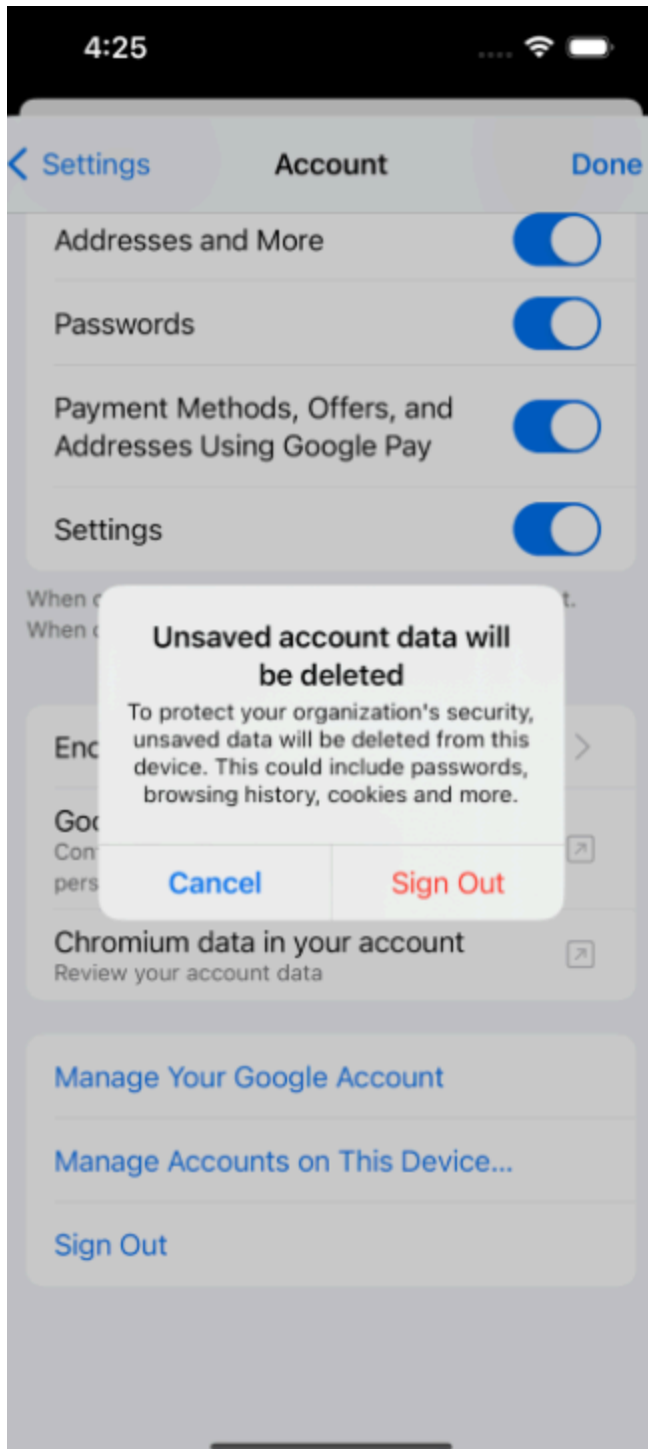
Clear device data on sign out on iOS

Starting in Chrome 129, signing out from a managed account in an unmanaged browser deletes local browsing data that is saved on the device. Managed users are presented a confirmation dialog on sign-out explaining that unsaved 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 is deleted includes:

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

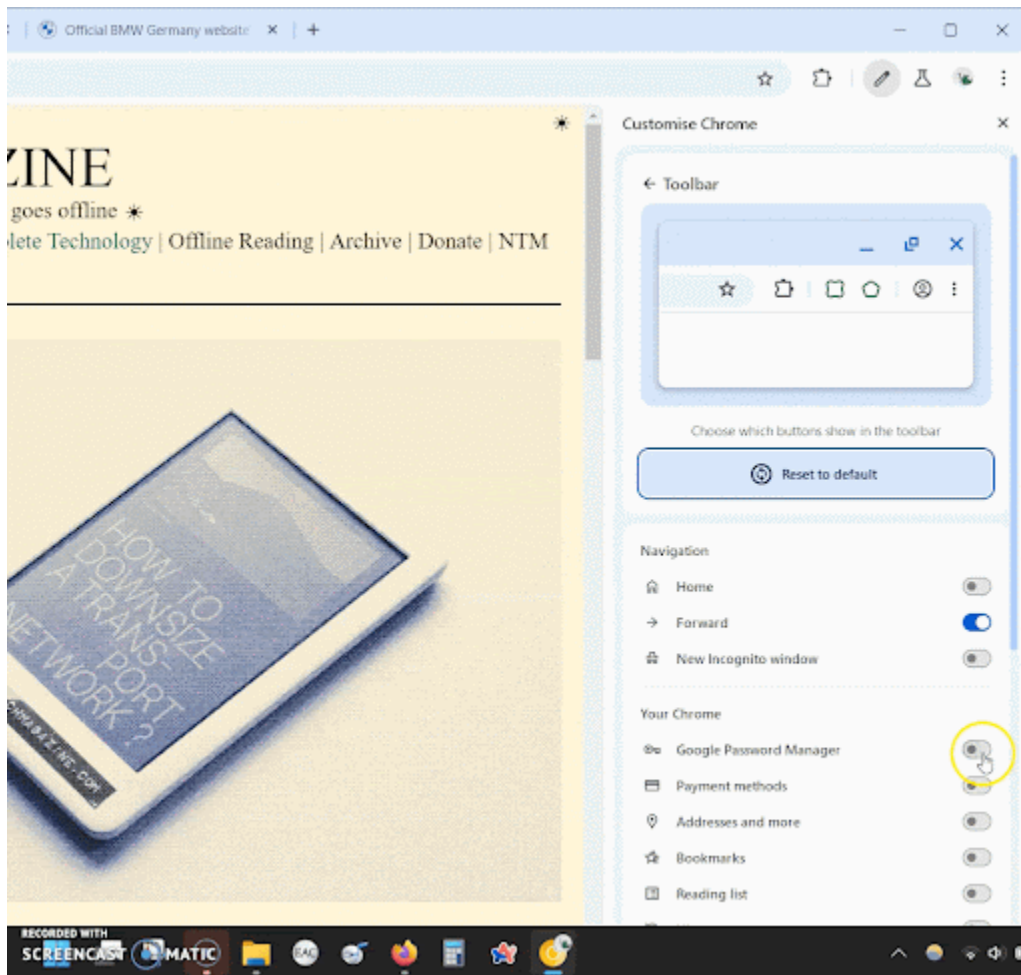
- **Chrome 129 on iOS**



Toolbar customization

We are introducing a toolbar customization feature in Chrome 129, which allows desktop browser users to pin and unpin icons to their toolbar via a new side panel.

- **Chrome 129 on ChromeOS, Linux, macOS, Windows:** Rolls out gradually



Google Password Manager Passkey usage on ChromeOS

Passkeys improve user security but until today have been slightly more difficult to use across devices. Now, users can save passkeys to Google Password Manager and use them across devices and platforms. This feature is already available on Windows, macOS, Linux and Android. It is now available on ChromeOS.

- Chrome 127 on Windows, Android and macOS
- **Chrome 129 on Windows, Android, macOS and ChromeOS**

New and updated policies in Chrome browser

Policy	Description
TabCompareSettings	Tab Compare settings
AdHocCodeSigningForPWAsEnabled	Ad-hoc code signing for Progressive Web App shims

ChromeOS updates

Chrome Enterprise Premium for file transfers on Managed Guest Sessions

In ChromeOS 129, organizations can 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.

Educators Appreciation wallpaper

In ChromeOS 129, we have added a new wallpaper collection to celebrate and share our gratitude and support to educators around the world.

Display brightness controls

Chromebook users can now easily adjust display brightness and control the ambient light sensor directly from the Settings app. This new feature lets you set your screen brightness to the perfect level and turn the ambient light sensor on or off as needed in the Settings app.

These updates make it simpler to use your device and help manage battery life.

Peripheral Welcome experience

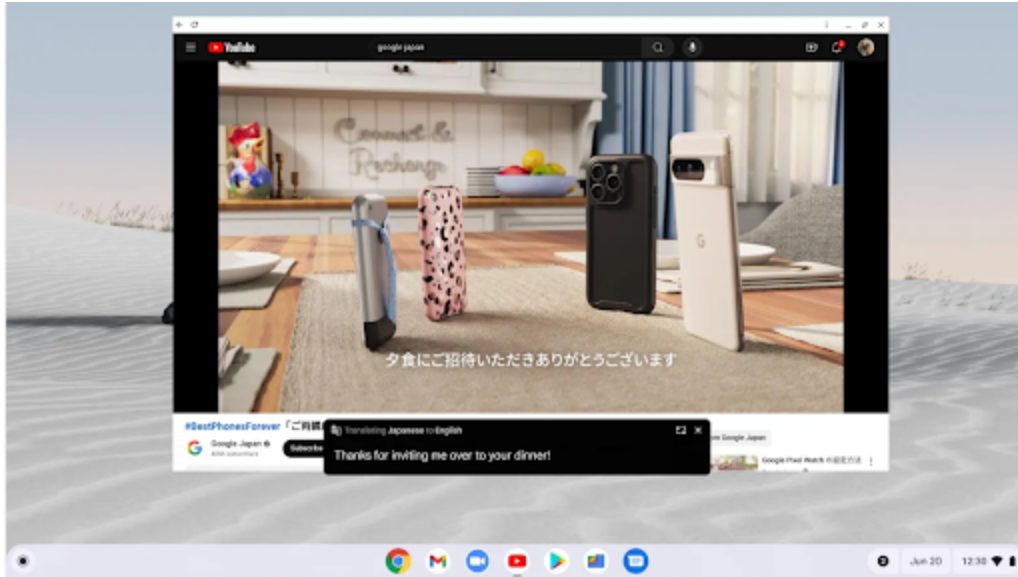
Knowing that a peripheral has been successfully connected, configuring it, and finding its companion app are critical steps in the peripheral user journey. This release aims to deliver a high-quality Welcome Experience by letting users know their peripheral is successfully connected and inviting them to configure it and make the most of it.

Managed accounts no longer synced as secondary accounts on Android

Starting from ChromeOS version 129, we enhance the data security for Android on ChromeOS. Enterprise accounts that are added as secondary accounts in-session will no longer automatically be added to the Android on ChromeOS environment. This change does not affect consumer accounts, education accounts, or accounts that were previously added.

Live Translate

[Chromebook Plus devices](#) are getting **Live Translate** which will allow a user to translate captionable content from Live Captions into a language of their choice. If an English speaking user is having a conversation with a person with whom they don't share the same language, so long as Live Captions is supported for the language of the person they're speaking with, it can be translated into English. This also works for videos as well and can be used on YouTube to Live Translate a video to English.

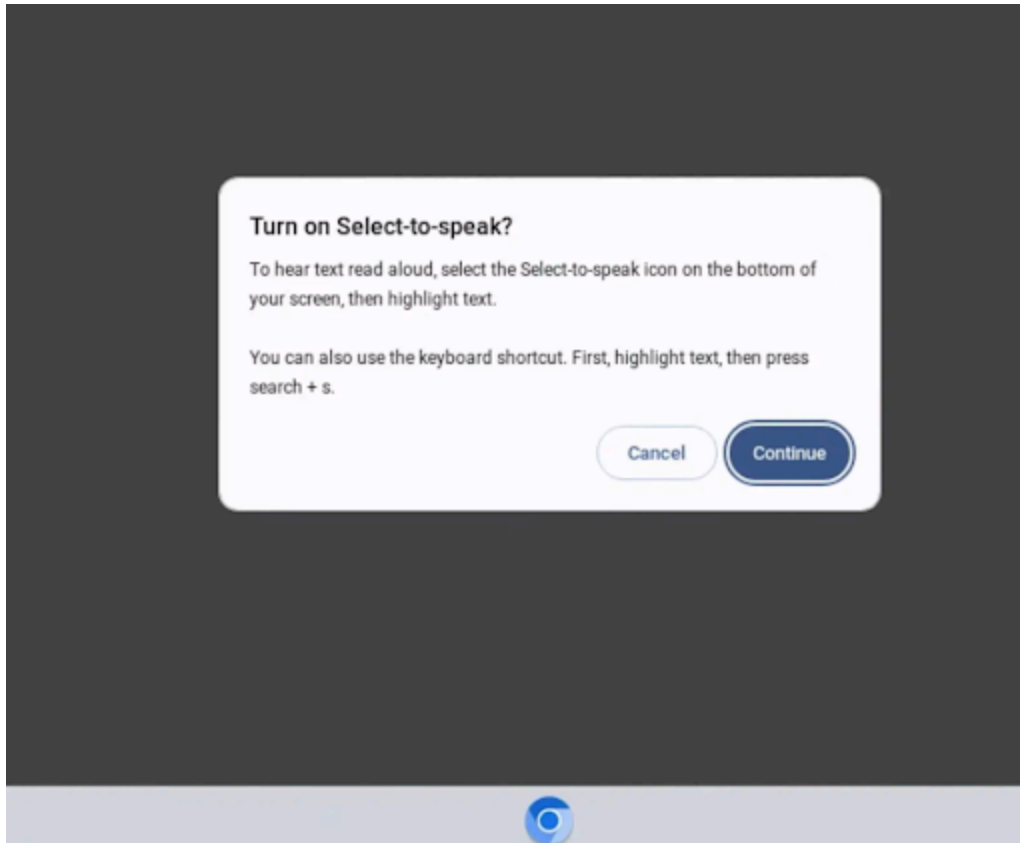


Keyboard brightness controls

Chromebook users can now easily adjust keyboard brightness and control the ambient light sensor directly from the Settings app. This new feature lets you set your keyboard brightness to the perfect level and turn the ambient light sensor on or off as needed. These updates make it simpler to use your device and help manage battery life. Meanwhile, if the Chromebook supports RGB, the [Keyboard Settings page](#) will have a direct link to the Personalization Hub's RGB color selection options.

Keyboard shortcut for Select-to-Speak

The Select-to-Speak keyboard shortcut (Search + s) now works when it is first pressed. You no longer need to enable it in Settings first. A dialog displays confirming that you want to turn on select to speak the first time you press the keyboard shortcut.



PIN as an authentication factor

This launch enables PIN as an authentication factor in all authentication surfaces across ChromeOS.

Automatic reload of sign-in screen

Starting from version 129, ChromeOS optimizes the support of 3P identity provider based logins. In the most common scenario, administrators show a permanent 3P identity provider login on the sign in screen. Many identity providers time out after a specific cadence, for example, 15 mins, leading to errors for the user. The new [DeviceAuthenticationFlowAutoReloadInterval](#) policy allows for a repeated refresh of 3P identity providers on the login screen, avoids timeouts, and therefore significantly increases the reliability of 3P identity provider logins.

CSE Workspace file types now supported in Google Drive

Client side encryption (CSE) is a Google Workspace and Drive feature that allows customers and users to encrypt files with customer provided keys so that data is encrypted and never stored on our servers in the clear. This launch provides basic CSE support in the Files app on ChromeOS. This includes making CSE files visible, opening CSE files in the browser and flagging non Google Workspace CSE files as unsupported.

Battery Icon updates

We are launching an update to the battery icon to ensure that the battery state no longer covers the battery level. Now you can easily see how much battery you have left.

Admin console updates

Extension Risk Score on the Apps and Extensions Usage report

This feature adds a new column in the Admin Console for browser management that displays the risk assessment for installed extensions in the admin's environment. This new addition allows IT admins to quickly identify extensions with a high, medium or low risk score using the sorting and filtering functionality of the report.

- **As early as Chrome 129 on Linux, macOS, Windows, ChromeOS:** Feature will be available for Trusted Testers early access.

Coming soon

Upcoming Chrome browser updates

Entrust certificate distrust

In response to sustained compliance failures, Chrome 127 changes how publicly-trusted TLS server authentication, that is, website 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, macOS, 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, macOS, Windows:** The blocking action will begin for certificates issued after October 31, 2024. This will also affect Chrome 127, 128 and 129.

Fallback styles for <meter> elements

As early as Chrome 130, [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 130 on Windows, macOS, Linux, Android**

Compression dictionary transport with Shared Brotli and Shared Zstandard

This feature adds support for using designated previous responses, as an external dictionary for [Brotli](#) or Zstandard-compressing HTTP responses.

Enterprises might experience potential compatibility issues with enterprise network infrastructure. The [CompressionDictionaryTransportEnabled](#) policy is available to turn off the compression dictionary transport feature.

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

Keyboard-focusable scroll containers

Improves accessibility by making scroll containers focusable using sequential focus navigation. Today, the tab key doesn't focus scrollers unless tabIndex is explicitly set to 0 or more.

By making scrollers focusable by default, users who can't (or don't want to) use a mouse will be able to focus clipped content using a keyboard's tab and arrow keys. This behavior is enabled only if the scroller does not contain any keyboard focusable children. This logic is necessary so we don't cause regressions for existing focusable elements that might exist within a scroller like a <textarea>.

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

Support non-special scheme URLs

Chrome 130 will support [non-special scheme URLs](#), for example, `git://example.com/path`, correctly. Previously, Chromium's URL parser didn'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 <http://bit.ly/url-non-special>.

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

Simplified sign-in and sync experience

Starting in Chrome 131, existing users with Chrome sync turned on will experience a simplified and consolidated version of sign-in and sync in Chrome. Chrome sync will no longer be shown as a separate feature in settings or elsewhere. Instead, users can sign in to Chrome to use and save information like passwords, bookmarks and more in their Google Account, subject to the relevant enterprise policies.

As before, the functionality previously part of Chrome sync that saves and accesses Chrome data in the Google Account can be controlled by [SyncTypesListDisabled](#). Sign-in to Chrome can be disabled via [BrowserSignin](#) as before.

Note that the changes do not affect users' ability to sign in to Google services on the web (like Gmail) without signing in to Chrome, their ability to stay signed out of Chrome, or their ability to control what information is synced with their Google Account.

- **Chrome 131 on Android**

Chrome extension telemetry integration with Google SecOps

We will begin to collect relevant [Chronicle extension telemetry](#) data from within Chrome, for managed profiles and devices, and send it to Google [SecOps](#). Google SecOps will analyze the

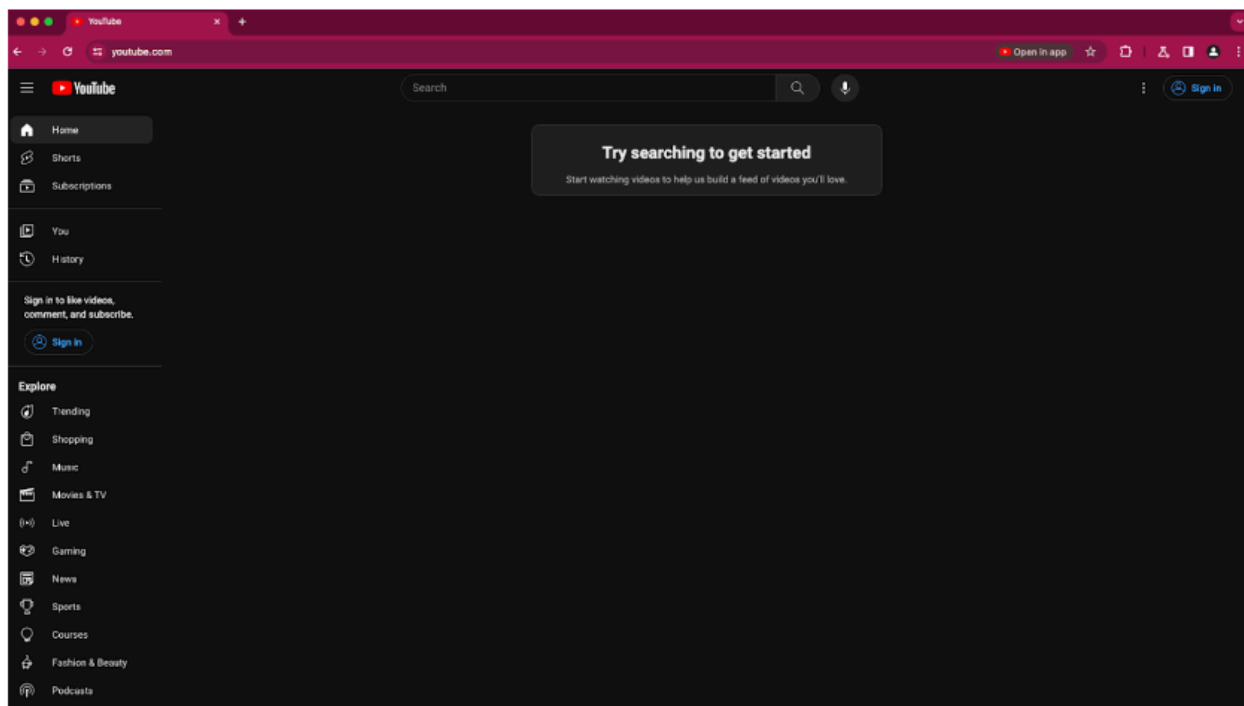
data to provide instant analysis and context on risky activity; this data is further enriched to provide additional context and is searchable for a year.

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

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. Clicking a link always automatically opens the app.

- Chrome 121 on Linux, macOS, 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 131 on Linux, macOS, 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).



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](#).

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

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, macOS, 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 enterprise network devices such as firewalls and proxies (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 at least Chrome 141 in 2025.. 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.

Starting in Chrome 131, Chrome will switch the key encapsulation mechanism from the draft version of Kyber, to the final standard version of ML-KEM. Using any form of post-quantum key exchange (Kyber or ML-KEM) will continue to be controlled by the [PostQuantumKeyAgreementEnabled](#) policy.

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

- Chrome 124 on Windows, macOS, Linux
- **Chrome 131**

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 can 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

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 and video-conference meeting backgrounds 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.

- **As early as Chrome 130 on Android, Linux, macOS, 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](#). If you have devices enrolled in Chrome Enterprise core, this policy is automatically applied to those devices to prevent sending data for AI model training. The existing policies that will have the updated default setting are:

- [CreateThemesSettings](#) (available in the US-only for now)
- [DevToolsGenAiSettings](#) (available in most countries)
- [HelpMeWriteSettings](#) (available in the US-only for now)
- [HistorySearchSettings](#) (available in the US-only for now)
- [TabOrganizerSettings](#) (available in the US-only for now)
- [TabCompareSettings](#) (available in the US-only for now)

GenAI control policy

Starting with 130, Chrome Enterprise Core will include a policy to control the behavior of multiple GenAI policies. This will be a convenient feature, allowing Admins to control the default behavior of a set of policies in one place, for example, off by default. This policy will control the following policies:

- [CreateThemesSettings](#)
- [DevToolsGenAiSettings](#)
- [HelpMeWriteSettings](#)
- [HistorySearchSettings](#)
- [TabOrganizerSettings](#)
- [TabCompareSettings](#)
- GenAIVcBackgroundSettings (launching in Chrome 130)
- GenAIWallpaperSettings (launching in Chrome 130)

Support for user-level settings on the Custom Configurations page

The **Custom configurations** page was recently launched in Chrome 127 and it allows IT admins to configure Chrome policies that are not yet in the Admin console, using JSON scripts. **As early as October 1st**, Custom configurations will support applying settings at the user-level, in addition to machine-level support. In other words, you will be able to enforce policies when users sign in to a managed Google account using the [Custom configurations page](#).

- **As early as October 1st on Android, iOS, Linux, macOS, Windows:** Feature rolls out for user policies

To get started, you can find the **Custom configurations** in the Admin console, under **Chrome browser > Reports** — you will need the Chrome Enterprise Core SKU:

The screenshot shows the 'Custom configurations' page in the Admin console. On the left, there is a sidebar with the title 'Custom configurations' and a section for 'Organisational units' with a search bar and a button labeled 'Global Organization'. The main content area has a back arrow and an 'Overview' section explaining that Chrome policies not in 'Settings' can be configured here using JSON. It includes links to 'sample.JSON code' and 'Settings'. Below this are sections for 'Supported platforms' (noting JSON settings are not supported on ChromeOS), 'Inheritance rules for JSON-based settings' (explaining inheritance for organisational units), and 'Precedence for JSON-based settings' (explaining that JSON values override Google defaults). A 'Show less' link is present. At the bottom, there is an 'Inheritance' section showing 'Inherited from Google default' and a 'Configurations' section with a list containing one item with the value '{}'. A character count '2 / 5000' is shown. At the very bottom are 'Save' and 'Cancel' buttons.

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.