Chrome 125 Enterprise and Education release notes

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

These release notes were published on May 8, 2024.

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

Chrome 125 release summary

Chrome browser updates	Security/Privacy	User productivity/Apps	Management
Chrome Third-Party Cookie Deprecation (3PCD)	✓		
Automatic deep file scanning for Enhanced Safe Browsing users	✓		
Chrome Desktop support for Windows ARM64			✓
Chrome updater changes			✓
Chrome Security Insights	✓	✓	✓
Chrome bandwidth updates			✓
Extensions Safety Check	✓		
Insecure form warnings on iOS	✓		
Legacy Browser Support for Edge upgraded to Manifest V3			✓
Remove enterprise policy used for Base URL inheritance	✓		
Send download reports without explicit user decision	✓		
Tab Groups on Tab Grid		✓	
UI Automation accessibility framework provider on Windows		✓	
Update Google Play Services to fix issues with account passwords		✓	
Extending Storage Access API (SAA) to non-cookie storage	✓		
Interoperable mousemove default action		✓	

Remove window-placement alias for permission and permission policy descriptors			✓
New and updated policies in Chrome browser			✓
Removed policies in Chrome browser			✓
ChromeOS updates	**Security/Privacy**	**User productivity/Apps**	**Management**
SAML always-on VPN fix			✓
ChromeOS Passpoint settings	✓		
ChromeOS Audio Bluetooth telephony			✓
Add PrivateIP to DoH with identifiers	✓		
Locale expansion for Live Captions and Dictation		✓	
Gallery video playback speed control UI		✓	
Reduce Animations toggle for ChromeOS		✓	
Captive Portal sign-in window	✓		
Install dialog for PWAs			✓
Warn users before disconnecting Bluetooth HID	✓		✓
Admin console updates	**Security/Privacy**	**User productivity/Apps**	**Management**
Inactive browser deletion in Chrome Enterprise Core	✓		✓
ChromeOS device enrollment and token generation redesign			✓

New ZTE pre-provisioning token features	✓		
Expanded token management features	✓		✓
URL-keyed anonymized data collection in Managed Guest Session	✓		
New policies in the Admin console			✓
Upcoming Chrome browser updates	**Security/Privacy**	**User productivity/Apps**	**Management**
Deprecate Safe Browsing Extended reporting	✓		
Extract text from PDFs for screen reader users		✓	
Network Service on Windows will be sandboxed	✓		
Removing support for UserAgentClientHintsGREASEUpdateEnabled	✓		
Tab Groups on iPad		✓	
Telemetry about pages that trigger keyboard and pointer Lock APIs	✓		
Updated password management experience on Android	✓	✓	
Watermarking	✓		
Align navigator.cookieEnabled with spec	✓		
Automatic fullscreen content setting		✓	
Keyboard-focusable scroll containers	✓		

Cross-site ancestor chain bit for CookiePartitionKey of partitioned cookies	✓		
App-bound encryption for cookies	✓		
Chrome extension telemetry integration with Chronicle	✓		
Migrate extensions to Manifest V3 before June 2025	✓	✓	✓
Simplified sign-in and sync experience on Android		✓	
Deprecate mutation events	✓		
Remove enterprise policy used for legacy same site behavior			✓
User link capturing on PWAs		✓	✓
X25519Kyber768 key encapsulation for TLS	✓		
Chrome will no longer support macOS 10.15	✓		✓
Deprecate the includeShadowRoots argument on DOMParser	✓		
Private network access checks for navigation requests: warning-only mode	✓		
Upcoming ChromeOS updates	**Security/Privacy**	**User productivity/Apps**	**Management**
New policy to control Kiosk wake and sleep times			✓
Show wildcard URLs in Data Controls Reporting			✓
Upcoming Admin console updates	**Security/Privacy**	**User productivity/Apps**	**Management**

Policy parity: Custom configurations for IT admins			✓
Interactive setup guides for Chrome Enterprise Core			✓
Legacy Technology report			✓

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

Chrome Third-Party Cookie Deprecation (3PCD)

Third party cookies will be restricted in a future release of Chrome. Currently, they are restricted by default for 1% of Chrome users to allow sites to preview the user experience without third-party cookies. Most enterprises are excluded from this group automatically and admins can use the BlockThirdPartyCookies and CookiesAllowedForUrls policies to re-enable third-party cookies if needed.

End users can use the eye icon in the omnibox to temporarily re-enable third-party cookies for 90 days on a given site when necessary. See this help article for more details on how to toggle these settings for the desired configuration. Bounce tracking protections are enforced when the bouncing site is not permitted to use 3P cookies, and are controllable with the same policies. Enterprise SaaS integrations used in a cross-site context for non-advertising use cases can register for the third-party deprecation trial or the first-party deprecation trial for continued access to third-party cookies for a limited period of time.

For more details on how to prepare, provide feedback and report potential site issues, refer to our updated landing page on preparing for the end of third-party cookies.

- **Starting in Chrome 120 on ChromeOS, Linux, macOS, Windows**
  1% of global traffic has third-party cookies disabled. Enterprise users are excluded from this automatically where possible, and a policy is available to override the change.

Automatic deep file scanning for Enhanced Safe Browsing users

Deep scanning of downloads for Enhanced Safe Browsing users has been launched since Chrome 91. At that time, users had to consent to each file they wanted deep-scanned automatically. Starting in Chrome 125, users no longer have to do that. Deep scanning is performed automatically as part of the improved protections offered by Enhanced Safe Browsing. Admins wishing to disable this feature can ensure their users are not in Enhanced Safe Browsing mode at all with the SafeBrowsingProtectionLevel policy, or disable deep scans with SafeBrowsingDeepScanningEnabled.

- **Chrome 125 on LaCrOS, Linux, Mac, Windows:** Feature rolls out

Chrome Desktop support for Windows ARM64

Chrome rolled out support for Windows ARM64. Enterprise installers are coming soon, and the ARM64 version can be downloaded at google.com/chrome. If you encounter any issues, file a bug here. At this time, other versions of Chrome running on ARM64 devices will not be automatically upgraded. Please re-install Chrome if you're running on an ARM64 device.

- **Chrome 125 on Windows:** New Enterprise installers will be available towards mid-May

Chrome updater changes

We are in the process of rolling out a new version of Google Update. As part of this change, the location for `GoogleUpdate.exe` on Windows changes and it is renamed `updater.exe`. Note that the previous path continues to persist until the transition is fully completed. `GoogleUpdate.exe` is also modified to point to `updater.exe`.
* Previous: `%PROGRAMFILES(X86)%\Google\Update\GoogleUpdate.exe`
* Current:
`%PROGRAMFILES(X86)%\Google\GoogleUpdater\<VERSION>\updater.exe`

- **Chrome 125 on Windows:** These changes appear on Windows.

Chrome Security Insights

If you have Chrome Enterprise Core (Chrome Browser Cloud Management) and Workspace Enterprise Standard or Workspace Enterprise Plus with assigned licenses, you can now enable Chrome Security Insights. This tool allows you to monitor insider risk and data loss for Chrome activity. For more information, see Monitoring for insider risk and data loss.

- **Chrome 125 on ChromeOS, Linux, Mac, Windows**

Chrome bandwidth updates

Chrome introduces a new mechanism for updating certain Chrome components, which might result in extra bandwidth used within your fleet. You can control this with the GenAILocalFoundationalModelSettings policy.

- **Chrome 125 on Linux, Mac, Windows**

Extensions Safety Check

The Extensions Safety Check notifies users about extensions that might contain malware, policy violations, and extensions that have been unpublished long ago. It provides an interface for users to review these extensions and decide to keep or remove each flagged extension.

To expand the usefulness and the scope of this feature, Chrome 125 adds new triggers so that other potentially risky extensions can also be reviewed by users. There are two new extension types that we now flag for the user to review.

- Extensions that are not installed from the Chrome Web Store

- Extensions that violate store policy by using deceptive installation tactics and are considered unwanted software

Any extensions that are force-installed, installed by policy, version-pinned or blocked by policy are ignored and not flagged by these trigger criteria.

- **Chrome 125 on ChromeOS, Linux, Mac, Windows:** During rollout, the two new triggers will be added to the extension safety check found on the `chrome://extensions/` page

Insecure form warnings on iOS

Chrome 125 blocks form submissions from secure pages to insecure pages on iOS. When Chrome detects an insecure form submission, it displays a warning asking the user to confirm the submission. The goal is to prevent leaking form data over plain text without user's explicit approval. A policy InsecureFormsWarningsEnabled is available to control this feature.

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

Legacy Browser Support for Edge upgraded to Manifest V3

Legacy Browser Support for Edge is upgraded to Manifest V3. This is a major update with a possibility for bugs, so you can try the Beta version of this extension today. We encourage you to test it in your environment. If you encounter any issues, file a bug here.

- **Chrome 125 on Linux, Mac, Windows:** Microsoft Edge Add-ons Store doesn't support gradual rollouts, so this will roll out 0%=>100% in one step. **Target release date is May 30th**, so ~2 weeks into Chrome 125's lifecycle.

Remove enterprise policy used for Base URL inheritance

In Chrome 114, we introduced NewBaseUrlInheritanceBehaviorAllowed to prevent users or Google Chrome variations from enabling NewBaseUrlInheritanceBehavior, in case compatibility issues were discovered. Chrome 125 removes the temporary **NewBaseUrlInheritanceBehaviorAllowed** policy .

- **Chrome 125 on Android, ChromeOS, Linux, Mac, Windows:** NewBaseUrlInheritanceBehaviorAllowed policy will be removed.

Send download reports without explicit user decision

The Client Safe Browsing Report is a telemetry report sent to Safe Browsing when a warning is shown in Chrome. Today, download reports are sent when users discard or bypass a download warning. Based on the learnings from the initial tailored warning experiment, many download warnings are not explicitly discarded or bypassed. Reports are not sent for these warnings, so Safe Browsing doesn't have visibility on the effectiveness of these warnings. This feature aims to close this telemetry gap by sending reports when the download is auto-discarded or the browser is closed.

- **Chrome 125 on ChromeOS, LaCrOS, Linux, Mac, Windows:**

Tab Groups on Tab Grid

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

- **Chrome 125 on iOS**

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.

Starting in Chrome 125, administrators can use the UiAutomationProviderEnabled enterprise policy 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.

Update Google Play Services to fix issues with account passwords

Users with old versions of Google Play Services might be unable to access the passwords saved to their Google accounts. These users now see warnings to update Google Play Services in the password management surface to access their account passwords again. This is part of an ongoing migration that only affects Android users of Google **Password Manager**.

- **Chrome 125 on Android**

Extending Storage Access API (SAA) to non-cookie storage

Chrome extends the Storage Access API to allow access to unpartitioned cookie and non-cookie storage in a third-party context. The current API only provides access to cookies, which have different use-cases than non-cookie storage. The API can be used as follows (JS running in an embedded iframe):

```
// Request a new storage handle via rSA (this should prompt the user)
let handle = await document.requestStorageAccess({all: true});

// Write some cross-site localstorage
handle.localStorage.setItem("userid", "1234");

// Open or create an indexedDB that is shared with the 1P context
let messageDB = handle.defaultBucket.indexedDB.open("messages");
```

The same flow would be used by iframes to get a storage handle when their top-level ancestor successfully called `rSAFor`, just that in this case the `storage-access` permission was already granted and thus the `rSA` call would not require a user gesture or show a prompt, allowing for hidden iframes accessing storage.

- **Chrome 125 on Windows, Mac, Linux, Android**

Interoperable mousemove default action

Canceling mousemove does not prevent text selection or drag-and-drop. Chrome allowed canceling mousemove events to prevent other APIs like text selection (and even drag-and-drop in the past). This does not match other major browsers; nor does it conform to the W3 UI Events specification.

With this feature, text selection is no longer the default action of mousemove. Text selection and drag-and-drop can still be prevented through canceling selectstart and dragstart events respectively, which are spec-compliant and fully interoperable.

- **Chrome 125 on Windows, Mac, Linux, Android**

Remove window-placement alias for permission and permission policy descriptors

Chrome 125 removes the `window-placement` alias for permission and permission policy descriptors. All instances of `window-placement` are replaced with `window-management`, which better describes the related API functionality. This is a follow-up to Window Management API feature enhancements and renaming from Multi-Screen Window Placement API; for more details, see Chrome Platform Status.

- **Chrome 125 on Windows, Mac, Linux**

New and updated policies in Chrome browser

Policy	Description
ProfileLabel	This policy controls a label used to identify a signed-in profile.
EnterpriseLogoUrl	Enterprise Logo URL: URL to an image that is used as an enterprise badge for the profile.
EnterpriseBadgingTemporarySetting	Control the visibility of enterprise badging

ApplicationBoundEncryptionEnabled	Enable Application-bound encryption
UiAutomationProviderEnabled	Enable the browser's UI Automation accessibility framework provider on Windows
ToolbarAvatarLabelSettings	Managed toolbar avatar label setting

Removed policies in Chrome browser

Policy	Description
NewBaseUrlInheritanceBehaviorAllowed	Allows enabling the feature NewBaseUrlInheritanceBehavior

ChromeOS updates

Always-on VPN SAML fix

To better support Enterprise customers who use VPN in always-on strict mode, where no user traffic can get to the internet except via the VPN, and SAML authentication, we've added a new policy AlwaysOnVpnPreConnectUrlAllowlist. This policy allows you to specify URLs users are allowed to go to before the VPN has connected, so that your SAML services are reachable to authenticate the user to the VPN via the system browser.

ChromeOS Passpoint settings

You can now view and manage Wi-Fi Passpoint in ChromeOS **Settings**. You can view and remove your installed passpoint subscription under the passpoint detailed page.

ChromeOS Audio Bluetooth telephony

ChromeOS now supports call control buttons on compatible Bluetooth headsets, including answering, rejecting or terminating a call, and muting the microphone.

Add PrivateIP to DoH with identifiers

A network identifier was added to the secure DNS URI templates with identifiers policy. Admins can now configure a new placeholder in the DNS URI templates, which is replaced with the device local IP addresses when the users are connected to managed networks.

Locale expansion for Live Captions and Dictation

ChromeOS 125 expands support for live captions from 1 to 6 languages and dictation from 1 to 18 locales. We now use a new voice recognition model that provides additional battery savings. Live captions on ChromeOS can be used on videos played with the **Gallery** player app, in YouTube, in Google Meet, in Zoom, or social media sites. To see or change your

current live captions language, select **Settings** > **Audio and captions** > **Live Caption** > **Manage languages**. For more information on live captions, see this Help Center article.

Dictation is available on Google Docs, or in any other text input by enabling dictation in the taskbar, clicking the Mic button, and speaking. To see or change your dictation language, select **Settings > Accessibility > Keyboard and text input > Dictation > Language**. For more information on dictation, see this Help Center article.

Gallery video playback speed control UI

ChromeOS Gallery video player now has a playback speed menu to control the playback rate.

Reduce Animations toggle for ChromeOS

A reduced animations setting is now available on ChromeOS. This setting is available under **Accessibility** > **Display and Magnification** > **Reduced Animations**. Customers who experience motion sickness, distractions or other types of discomfort when seeing animations can benefit from changing this setting.

Captive portal sign-in window

ChromeOS 125 allows easier captive portal sign-in with a dedicated window. The window opens as a tabless popup window; the URL is shown but it is not editable.

Install dialog for PWAs

ChromeOS 125 enables an installation dialog for web apps. This feature unblocks web app installation scenarios and is part of the work to create a more predictable, accessible, and trustworthy install surface for web apps.

Warn users before disconnecting Bluetooth HID

In ChromeOS 125 and later, Chromeboxes and Chromebases display a notification to prevent unintended Bluetooth device disconnections. This notification appears when you attempt to disable Bluetooth while only Human Interface Devices (HIDs) like keyboards or mice connected via Bluetooth are active.

Admin console updates

Inactive browser deletion in Chrome Enterprise Core

Starting in April 2024 until June 2024, the **Inactive period for browser deletion policy** has started to roll out and automatically delete enrolled browsers in the Admin console that have been inactive for more than the inactivity period of time determined by the policy. When releasing the policy, the inactivity period of time has a default value of 540 days. Meaning that by default, all enrolled browsers that have been inactive for more than 540 days are deleted from your account. Administrators can change the inactive period value using this policy. The maximum value to determine the browser inactivity period is 730 days and the minimum value is 28 days (learn more).

If you lower the set policy value, it might have a global impact on any currently enrolled browsers. All impacted browsers will be considered inactive and, therefore, be **irreversibly deleted**. To ensure the deleted browsers re-enroll automatically next time they restart, set the Device Token Management policy value to **Delete token** before lowering the value of this policy. The enrollment tokens on these browsers need to still be valid at the time of the restart.

ChromeOS device enrollment and token generation redesign

Beginning in April 2024, the zero-touch enrollment experience has been enhanced with a new enrollment entry point, token creation guide, the ability to specify SKU and partner permissions and improved token management.

New ZTE pre-provisioning token features

Pre-provisioning tokens have gained the following features:

- Support for Kiosk & Signage Upgrade by allowing zero-touch enrollment pre-provisioning tokens to be created using either Chrome Enterprise Upgrade or Kiosk & Signage Upgrade
- Ability for pre-provisioning partners to specify custom fields (asset ID, location, and user)
- Multiple tokens per organizational unit

Expanded token management features

The Enrollment Tokens page has been updated with the following features:

- The page has been added to the left navigation panel for easier access
- Tokens are now filterable based on status, creation user, annotation and upgrade type
- A new button allows admins to copy the token and Customer ID with one click
- Additional columns provide more information about the token

URL-keyed anonymized data collection in Managed Guest Session

The policy for URL-keyed anonymized data collection, UrlKeyedAnonymizedDataCollectionEnabled, is available in the Admin console. This policy will be enforced starting June 1st and will remain disabled until then.

New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
DevToolsGenAiSettings	Users & Browsers	Chrome ChromeOS	Generative AI
UiAutomationProviderEnabled	Users & Browsers	Chrome	Accessibility
ContextualGoogleIntegrationsEnabled	Users & Browsers	ChromeOS	User experience
ContextualGoogleIntegrationsConfiguration	Users & Browsers	ChromeOS	User experience
ApplicationBoundEncryptionEnabled	Users & Browsers	Chrome	Security
DeviceExtensionsSystemLogEnabled	Device	ChromeOS	User and device reporting
EnterpriseBadgingTemporarySetting	Users & Browser	Chrome	General
EnterpriseLogoUrl	Users & Browser	Chrome	General
ToolbarAvatarLabelSettings	Users & Browser	Chrome	General
ProfileLabel	Users & Browser	Chrome	General
DeviceDlcPredownloadList	Device	ChromeOS	Other settings

Coming soon

Note: The items listed below are experimental or planned updates. They might change, be delayed, or canceled before launching to the Stable channel.

Upcoming Chrome browser changes

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.

- **Chrome 126 on iOS, ChromeOS, Linux, Mac, Windows:** Deprecation of Safe Browsing Extended Reporting

Extract text from PDFs for screen reader users

Chrome browser is launching an Optical character recognition (OCR) AI reader for PDFs, creating the first browser built-in PDF screen reader for inaccessible documents, further filling the gap in accessibility for low vision and blind users across the web.

This feature leverages Google's OCR models to extract, compartmentalize, and section PDF documents to make them more accessible. A local machine intelligence library will be added that uses Screen AI technology to analyze screenshots or the accessibility tree, and

extract more information to help assistive technology, such as texts (OCR) and main content of the page.

- **Chrome 126 on ChromeOS, Linux, Mac, Windows**

Network Service on Windows will be sandboxed on Windows

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 report any issues you encounter.

- **Chrome 126 on Windows:** Network Service sandboxed on Windows

Removing support for UserAgentClientHintsGREASEUpdateEnabled

Deprecate the UserAgentClientHintsGREASEUpdateEnabled policy since the updated GREASE algorithm has been on by default for over a year and then eventually remove it.

- Chrome 124 on Android, ChromeOS, Linux, Mac, Windows: Policy is deprecated
- **Chrome 126 on Android, ChromeOS, Linux, Mac, Windows:** Policy is removed

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 126 on iOS**

Telemetry about pages that trigger keyboard and pointer Lock APIs

When an Enhances Safe Browsing user visits a page that triggers keyboard or pointer lock API, attributes of that page will be sent to Safe Browsing. If the telemetry is sent and the page seems to be malicious, users will see a Safe Browsing warning and their keyboard or pointer will be unlocked if they were locked.

- **Chrome 126 on Android, ChromeOS, LaCrOS, Linux, Mac, Windows, Fuchsia**

Updated password management experience on Android

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

- **Chrome 126 on Android**

Watermarking

This feature will allow admins to overlay a watermark on top of a webpage if navigating to it triggers a specific DLP rule. It will contain a static string displayed as the watermark. Watermarking will be available to Chrome Enterprise Premium customers.

- Chrome 124 on Linux, Mac, Windows: Trusted Tester access
- **Chrome 126 on Linux, Mac, Windows:** Feature rolls out

Align navigator.cookieEnabled with spec

`navigator.cookieEnabled` currently indicates if "the user agent attempts to handle cookies" in a given context. A change in Chrome, shipping as part of third-party cookie deprecation (3PCD), would cause it to indicate whether unpartitioned cookie access is possible (causing it to return false in most cross-site iframes). We should restore the prior behavior of navigator.cookieEnabled which indicated only if cookies were enabled/disabled for the site and rely on the cross-vendor function document.hasStorageAccess to indicate if unpartitioned cookie access is possible.

- **Chrome 126 on Windows, Mac, Linux, Android**

Automatic fullscreen content setting

A new **Automatic Fullscreen** content setting permits `Element.requestFullscreen()` without a user gesture, and permits browser dialogs to appear without exiting fullscreen.

The setting is blocked by default and sites cannot prompt for permission. New UI controls are limited to Chrome's settings pages (`chrome://settings/content/automaticFullScreen`) and the site info bubble. Users can allow Isolated Web Apps, and enterprise admins can allow additional origins with the AutomaticFullscreenAllowedForUrls policy.

Combined with Window Management permission and unblocked popups (`chrome://settings/content/popups`), this unlocks valuable fullscreen capabilities:

- Open a fullscreen popup on another display, from one gesture
- Show fullscreen content on multiple displays from one gesture
- Show fullscreen content on a new display, when it's connected
- Swap fullscreen windows between displays with one gesture
- Show fullscreen content after user gesture expiry or consumption

- **Chrome 126 on Windows, Mac, Linux**

Cross-site ancestor chain bit for CookiePartitionKey of partitioned cookies

Chrome 125 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) or use the Cross-Origin Resource Sharing (CORS) to ensure that embedded iframes have access to the same cookies as the top level domain.

- **Chrome 126 on Windows, Mac, Linux**

Keyboard-focusable scroll containers

Making scroll containers focusable using sequential focus navigation greatly improves accessibility. 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 127 on Windows, MacOS, Linux, Android**

App-bound encryption for cookies

To improve the security of cookies on Windows, the encryption key used for cookie encryption will be further secured by binding it to Chrome's application identity. This can help protect against malware that might attempt to steal cookies from the system. This does not protect against an attacker who is able to elevate privilege or inject into Chrome's processes.

An enterprise policy ApplicationBoundEncryptionEnabled is available to disable Application Bound Encryption.

- **Chrome 127 on Windows**

Chrome extension telemetry integration with Chronicle

Collect relevant extension telemetry data from within Chrome (managed profiles + devices) and send it to Chronicle. Chronicle will analyze the data to provide instant analysis and context on risky activity.

- **Chrome 127 on ChromeOS, LaCrOS, Linux, Mac, Windows**

Migrate extensions to Manifest V3 before June 2025

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.

Beginning June 2024, Chrome will gradually disable Manifest V2 extensions running in the browser. An Enterprise policy - ExtensionManifestV2Availability - can be used to test Manifest V3 in your organization ahead of the migration. Additionally, machines on which

the policy is enabled will not be subject to the disabling of Manifest V2 extensions until the following year - June 2025 - at which point the policy will be removed.

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 Enterprise Core.

- **Chrome 127 on ChromeOS, LaCrOS, Linux, MacOS, Windows:** Chrome will gradually disable Manifest V2 extensions on user devices. Only those with the ExtensionManifestV2Availability enterprise policy enabled would be able to continue using Manifest V2 extensions in their organization.
- Chrome 139 on ChromeOS, LaCrOS, Linux, MacOS, Windows: Remove ExtensionManifestV2Availability policy.

Simplified sign-in and sync experience on Android

Chrome will launch a simplified and consolidated version of sign-in and sync in Chrome on Android. 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 turned off via 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.

The changes are virtually identical to the simplified sign-in and sync experience launched on iOS in 117.

- **Chrome 127 on Android**

Deprecate mutation events

Mutation Events, including `DOMSubtreeModified`, `DOMNodeInserted`, `DOMNodeRemoved`, `DOMNodeRemovedFromDocument`, `DOMNodeInsertedIntoDocument`, and `DOMCharacterDataModified`, are quite bad for page performance, and also significantly increase the complexity of adding new features to the Web. These APIs were deprecated from the spec in 2011, and were replaced (in 2012) by the much better-behaved Mutation Observer API. Usage of the obsolete Mutation Events must now be migrated to Mutation Observer. Starting in Chrome 124, a temporary enterprise policy, **MutationEventsEnabled**, is available to re-enable deprecated or removed mutation events. If you encounter any issues, file a bug here.

Mutation event support will be disabled by default starting in Chrome 127, around July 30, 2024. Code should be migrated before that date to avoid site breakage. If more time is needed, there are a few options:

- The Mutation Events Deprecation Trial can be used to re-enable the feature for a limited time on a given site. This can be used through Chrome 134, ending March 25, 2025.
- A MutationEventsEnabled enterprise policy can also be used for the same purpose, also through Chrome 134.

Please see this blog post for more detail.

- **Chrome 127 on Windows, Mac, Linux, Android**

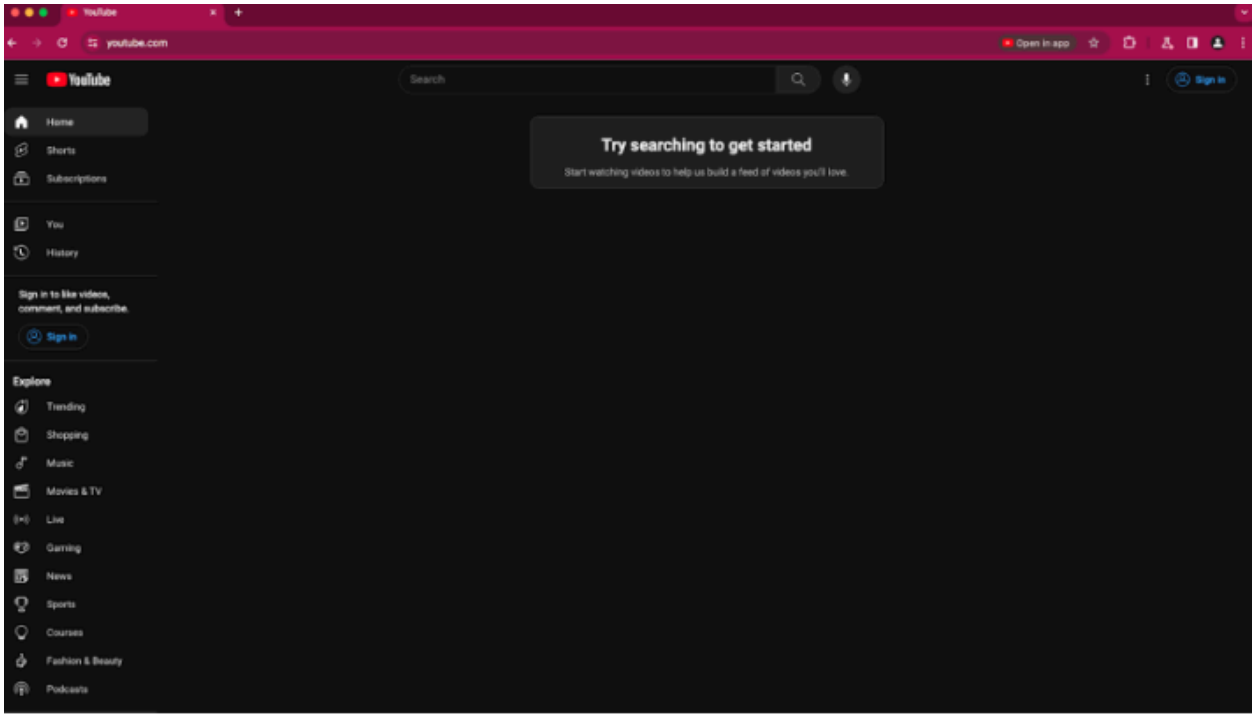
Remove enterprise policy used for legacy same site behavior

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 128 on Android, ChromeOS, Linux, Mac, Windows:** Remove LegacySameSiteCookieBehaviorEnabledForDomainList policy

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 128 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).

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.
Please see this blog post for more detail.

- Chrome 124 on Windows, Mac, Linux
- **Chrome 128 on 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 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() will ship 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 Windows, Mac, Linux, Android**

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. The above checks are made to 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 fails. Instead, a warning will be shown in the DevTools, to help developers prepare for the coming enforcement.

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

Upcoming ChromeOS changes

New policy to control Kiosk wake and sleep times

As early as ChromeOS 126, we will introduce a new kiosk device policy that will allow Admins to schedule when a device will wake and sleep. For more details, see Kiosk settings.

Show wildcard URLs in Data Controls reporting

ChromeOS Data Control rules allow admins to define source and destination URLs as a wildcard (*) value. ChromeOS data control events are reported under the Chrome audit report and can be viewed in the Google Admin console or other platforms through the Chrome Reporting Connector. When examining log events, the URL that triggered the rule is now reported, instead of the wildcard.

Upcoming Admin console changes

Policy parity: Custom configurations for IT admins

The **Custom Configurations** page allows IT admins to configure Chrome policies that are not yet in the Admin console, using JSON scripts. As a result, all Chrome policies are now configurable in Chrome Enterprise Core, either using the **Settings** page or the **Custom Configurations** page. You can also use the page to configure extension installation mode not supported in the Admin console, such as “normal_installed”. This feature is available for browsers enrolled at the machine-level.

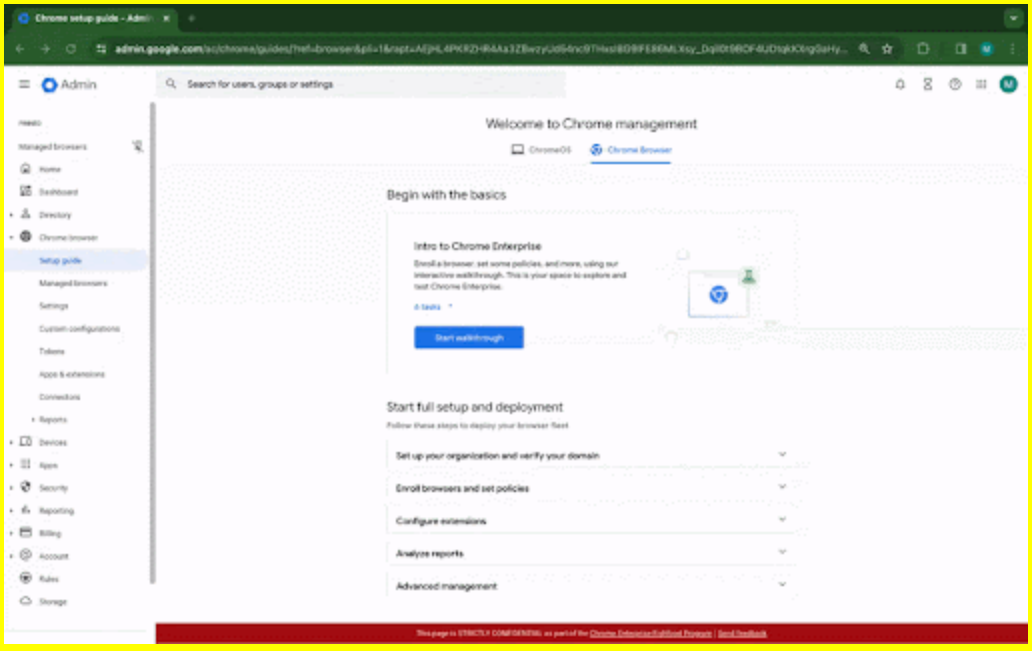
- **As early as Chrome 126 on Android, iOS, Linux, MacOS, Windows:** Trusted Tester access
- As early as Chrome 126 on Android, iOS, Linux, MacOS, Windows: Feature rolls out

Interactive setup guides for Chrome Enterprise Core

The Chrome Enterprise team is introducing new interactive setup guides for **browser management** in the Admin console, where administrators can choose a journey they’re interested in exploring and get hands-on training directly in Chrome Setup Guides. For example, the guides can be used to learn how to:

- Creating test organizational units
- Turn on reporting
- Enroll browsers
- Apply browser policies
- Configure extension settings
- Create an admin user

These guides are ideal for new administrators or for administrators who wish to learn new journeys.



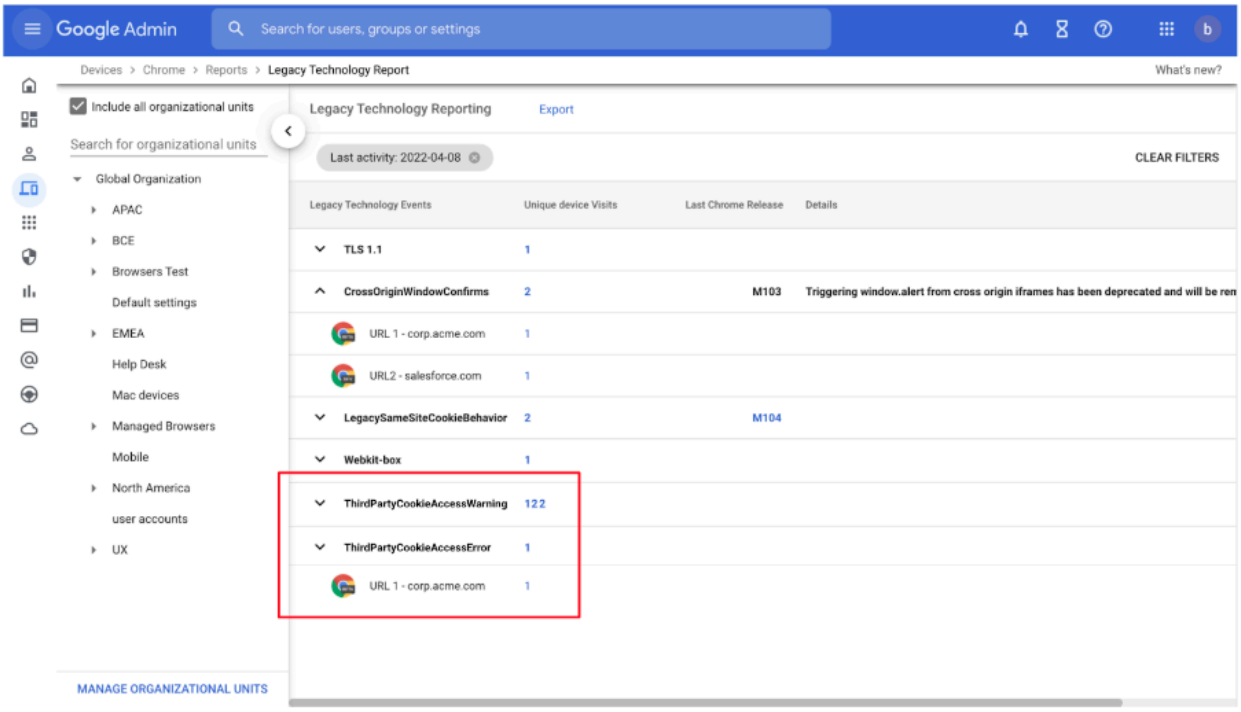
- **As early as Chrome 125:** Trusted Tester access
- As early as Chrome 126: Feature rolls out

Legacy Technology report

As early as Chrome 127, the Legacy Technology report will be available in the Admin console and it will proactively report websites (both internal and external) that are using technology that will be deprecated, for example, SameSite cookie changes, and older security protocols like TLS 1.0/1.1. This information will enable IT administrators to work with developers to plan required tech migrations before the deprecation feature removals goes into effect.

This feature is currently released in our Trusted Tester program. If you're interested in helping us test this feature, you can sign up for the Chrome Enterprise Trusted Tester program here.

- **As early as Chrome 127 on Linux, MacOS, Windows:** Legacy Technology report will be available in the Admin console.


Google Admin
Search for users, groups or settings
Devices > Chrome > Reports > Legacy Technology Report
What's new?
Include all organizational units
Search for organizational units
Global Organization
APAC
BCE
Browsers Test
Default settings
EMEA
Help Desk
Mac devices
Managed Browsers
Mobile
North America
user accounts
UX
MANAGE ORGANIZATIONAL UNITS
Legacy Technology Reporting
Export
Last activity: 2022-04-08
CLEAR FILTERS
Legacy Technology Events
Unique device Visits
Last Chrome Release
Details
TLS 1.1 1
CrossOriginWindowConfirms 2 M103 Triggering window.alert from cross origin iframes has been deprecated and will be ren
URL 1 - corp.acme.com 1
URL2 - salesforce.com 1
LegacySameSiteCookieBehavior 2 M104
Webkit-box 1
ThirdPartyCookieAccessWarning 122
ThirdPartyCookieAccessError 1
URL 1 - corp.acme.com 1

Previous release notes

Chrome version & targeted Stable channel release date	PDF
Chrome 124: April 10, 2024	PDF
Chrome 123: March 13, 2024	PDF
Chrome 122: February 14, 2024	PDF
Chrome 121: January 17, 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