chrome enterprise

Chrome 126 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 June 5, 2024.

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

Chrome 126 release summary

Chrome browser updates	**Security / Privacy**	**User productivity / Apps**	**Management**
Chrome Third-Party Cookie Deprecation (3PCD)	✓		
Extract text from PDFs for screen reader users		✓	
Memory Saver aggressiveness		✓	
Out of process iframe PDF viewer		✓	
Reactive prefetch on Desktop	✓		
Tab Groups on iPad		✓	
UI Automation accessibility framework provider on Windows		✓	
Removing support for UserAgentClientHintsGREASEUpdateEnabled	✓		✓
Align navigator.cookieEnabled with spec	✓		
Search with Google Lens		✓	
New and updated policies in Chrome browser			✓
ChromeOS updates	**Security/Privacy**	**User productivity/Apps**	**Management**
Extended auto-update opt-in			✓
Digital zoom with Super Resolution		✓	
Set up new Chromebook with Android phone		✓	

Instant Hotspot		✓	
Enhanced firmware updates	✓		✓
Web apps to capture multiple surfaces		✓	
Remote CRD for idle devices	✓		
Captive portal for managed networks	✓		✓
Turn off overscroll behavior		✓	
Turn off cursor blink rate		✓	
Magnifier can follow Select to Speak focus		✓	
Supervised user extensions installation flow		✓	
Multi-calendar support		✓	
New policy to control Kiosk wake and sleep times			✓
Locale expansion for Live Captions and Dictation		✓	
Show wildcard URLs in Data Controls reporting			✓
Admin console updates	**Security/Privacy**	**User productivity/Apps**	**Management**
Custom configurations for IT admins			✓
Interactive setup guides for Chrome Enterprise Core			✓
New policies in the Admin console			
Upcoming Chrome browser updates	**Security / Privacy**	**User productivity / Apps**	**Management**
App-bound encryption for cookies	✓		

Chrome extension telemetry integration with Chronicle	✓		
Generating insights for DevTools console warnings and errors			✓
Migrate extensions to Manifest V3 before June 2025	✓	✓	✓
Network Service on Windows will be sandboxed	✓		
Simplified sign-in and sync experience on Android		✓	
Telemetry about pages that trigger keyboard and pointer Lock APIs	✓		
Updated password management experience on Android	✓	✓	
Watermarking	✓		
Automatic Fullscreen content setting		✓	
Cross-site ancestor chain bit for CookiePartitionKey of partitioned cookies			✓
Deprecate mutation events	✓		
Keyboard-focusable scroll containers	✓		
Support for *not* condition in ServiceWorker static routing API	✓		
Ad-hoc code signatures for PWA shims on macOS		✓	
Deprecate Safe Browsing Extended reporting	✓		
Chrome will no longer support macOS 10.15	✓		✓

User Link capturing on PWAs		✓	✓
Deprecate the includeShadowRoots argument on DOMParser			
Insecure form warnings on iOS	✓		
Private network access checks for navigation requests: warning-only mode			✓
Remove enterprise policy used for legacy same site behavior			✓
X25519Kyber768 key encapsulation for TLS	✓		
Upcoming ChromeOS changes	**Security / Privacy**	**User productivity / Apps**	**Management**
Snap Groups		✓	
Read Aloud in Reading Mode		✓	
Upcoming Admin console changes	**Security/Privacy**	**User productivity/Apps**	**Management**
Filter for popular and recently added settings with policy tags			✓
Chrome browser managed profile reporting			✓
Group based policy for Chrome browser			✓

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

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.

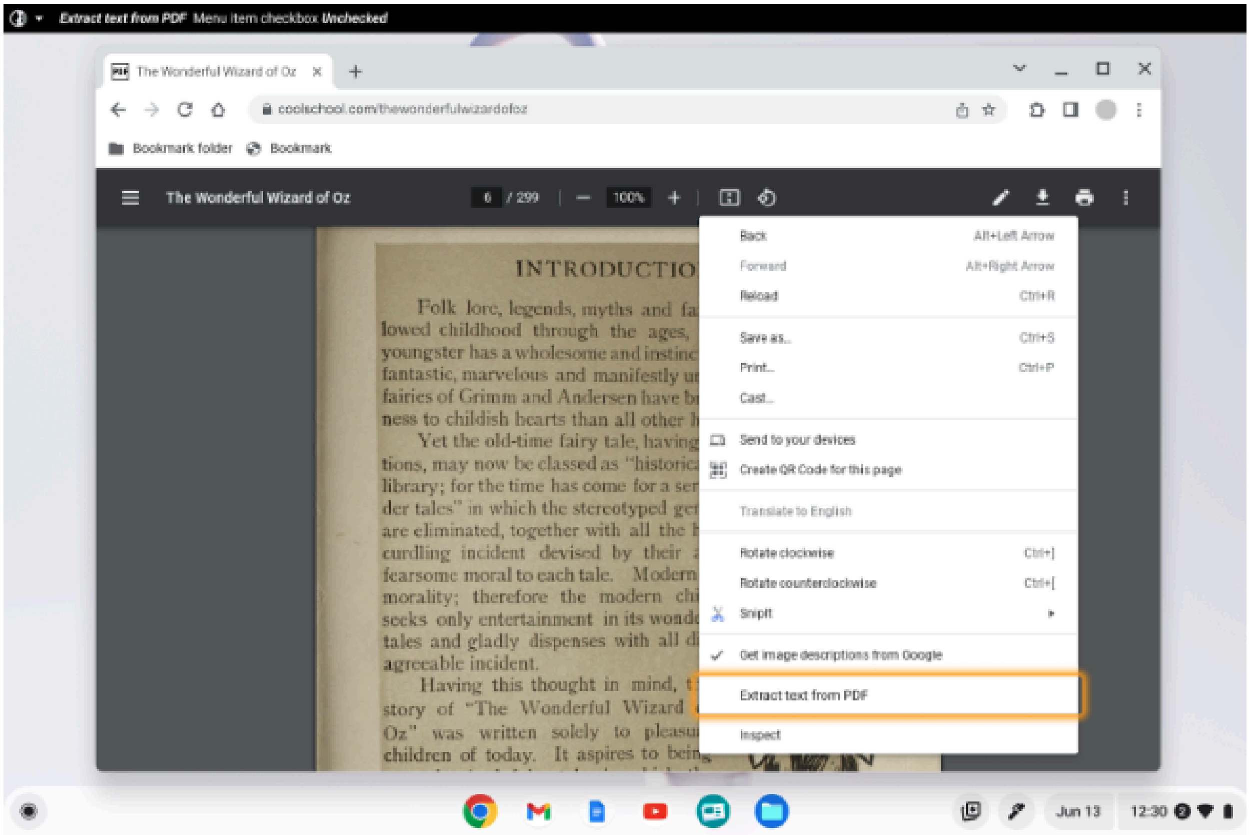
- **Starting in Chrome 120 on ChromeOS, Linux, macOS, Windows**
  1% of global traffic has third-party cookies disabled. Enterprise users are excluded from this automatically where possible, and a policy is available to override the change.

Extract text from PDFs for screen reader users

Chrome browser now launches an optical character recognition (OCR) AI reader for PDFs, creating a 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:** Already fully launched in ChromeOS. Ramping up from 50% Canary/Dev/Beta to Stable on Linux, Mac, and Windows.


Extract text from PDF Menu item checkbox Unchecked
The Wonderful Wizard of Oz
coolschool.com/thewonderfulwizardofoz
Bookmark folder
Bookmark
The Wonderful Wizard of Oz
6 / 299
100%
INTRODUCTIO
Folk lore, legends, myths and fa
lowed childhood through the ages,
youngster has a wholesome and instinc
fantastic, marvelous and manifestly un
fairies of Grimm and Andersen have br
ness to childish hearts than all other h
Yet the old-time fairy tale, having
tions, may now be classed as "historic
library; for the time has come for a ser
der tales" in which the stereotyped ge
are eliminated, together with all the h
curdling incident devised by their a
fearsome moral to each tale. Modern
morality; therefore the modern chi
seeks only entertainment in its wond
tales and gladly dispenses with all di
agreeable incident.
Having this thought in mind, t
story of "The Wonderful Wizard
Oz" was written solely to pleasu
children of today. It aspires to bein
Back Alt+Left Arrow
Forward Alt+Right Arrow
Reload Ctrl+R
Save as... Ctrl+S
Print... Ctrl+P
Cast...
Send to your devices
Create QR Code for this page
Translate to English
Rotate clockwise Ctrl+]
Rotate counterclockwise Ctrl+[
SnipIt
✓ Get image descriptions from Google
Extract text from PDF
Inspect
Jun 13
12:30

Memory Saver aggressiveness

Memory Saver is a feature that deactivates unused tabs to free up memory on a user's device. There is an existing policy, HighEfficiencyModeEnabled, which allows administrators to control the Memory Saver feature. A new policy called MemorySaverModeSavings allows you to configure how aggressive the Memory Saver is when deciding to deactivate tabs. Choose the conservative option to deactivate fewer tabs or the aggressive one to get the most memory savings.

- **Chrome 126 on ChromeOS, LaCrOS, Linux, Mac, Windows:** The feature will roll out gradually to all platforms.

Out of process iframe PDF viewer

In Chrome 126, some users use an out-of-process iframe (OOPIF) architecture for the PDF viewer. This is the new PDF viewer architecture, as it is simpler and makes adding new features easier. An enterprise policy, PdfViewerOutOfProcessIframeEnabled, is available to revert to using the original PDF viewer architecture.

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

Reactive prefetch on Desktop

This feature enables prefetching of subresources during a navigation, to speed up navigations and load new pages faster. The subresources prefetched are predicted by a Google-owned service, and the browser shares the URL of pages being navigated to with this service, to retrieve predictions. You can control this feature using the UrlKeyedAnonymizedDataCollectionEnabled policy.

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

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**

UI Automation accessibility framework provider on Windows

Starting in Chrome 126, Chrome starts to directly support accessibility client software that uses Microsoft Windows's UI Automation accessibility framework. Prior to this change, such software interoperated with Chrome using a compatibility shim in Microsoft Windows. This change improves the user experience for many users. It provides complete support for Narrator, Magnifier, and Voice Access; and it improves third-party apps that use Windows's UI Automation accessibility framework. Chrome users now find reduced memory usage and processing overhead when using accessibility tools. It also eases development of software using assistive technologies.

Administrators can use the UiAutomationProviderEnabled enterprise policy, introduced in 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 can 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.

Removing support for UserAgentClientHintsGREASEUpdateEnabled

Chrome 126 removes the **UserAgentClientHintsGREASEUpdateEnabled** policy since the updated GREASE algorithm has been on by default for over a year.

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

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**

Search with Google Lens

As early as Chrome 126, users will be able to search any images or text they see on their screen with Google Lens. To use this feature, go to a website and click **Search with Google Lens** on the on-focus omnibox chip, on the right-click menus, or on the 3-dot menu. Users can click, highlight, or drag anywhere on the screen to search its contents, and refine their search by adding keywords or questions to the searchbox. Admins can control the feature through a policy called **LensOverlaySettings**. To perform the search, a screenshot of the screen is sent to Google servers but it is not linked to any IDs or accounts, it is not viewed by any human, and data about its contents is not logged.

We are rolling out this feature gradually in Chrome 126 and we plan to launch fully in Chrome 127.

- **Chrome 126 on ChromeOS, Linux, Mac, Windows:** Rollout of the feature at 1% Stable and LensOverlaySettings becomes available

- Chrome 127: Rollout to 100% stable

New and updated policies in Chrome browser

Policy	Description
LensOverlaySettings	Settings for the Lens Overlay feature
MemorySaverModeSavings	Change Memory Saver Mode Savings
ProvisionManagedClientCertificateForUser	Enables the provisioning of client certificates for a managed user or profile
PdfViewerOutOfProcessIframeEnabled	Use out-of-process iframe PDF Viewer

ChromeOS updates

Extended auto-update opt-in and policy

ChromeOS provides 10 years of OS updates for security, stability, and performance improvements. Most devices will receive these updates automatically. For a subset of older devices, users and administrators can now opt in to extended updates to get a full 10 years of support.
For details, see our Help Center article.

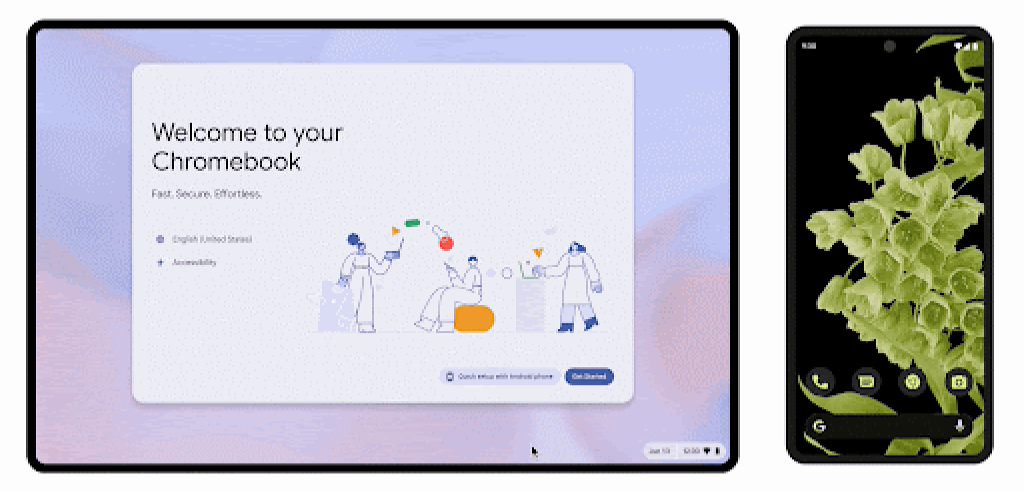
Digital zoom with Super Resolution

The built-in Camera app now supports zooming on cameras that do not have optical zoom motors, including the built-in camera. On selected high-performance Chromebooks, AI-based Super Resolution may be applied to further enhance the images.

Set up new Chromebook with Android phone

You can now set up a new Chromebook using your Android phone. By establishing a secure connection between your phone and the Chromebook, you can automatically transfer your

Wi-Fi and Google Account login information without needing to manually enter your passwords. This is available for unmanaged users only.



Instant Hotspot

ChromeOS 126 renames the **Instant Tethering** feature to **Instant Hotspot**.

Enhanced firmware updates

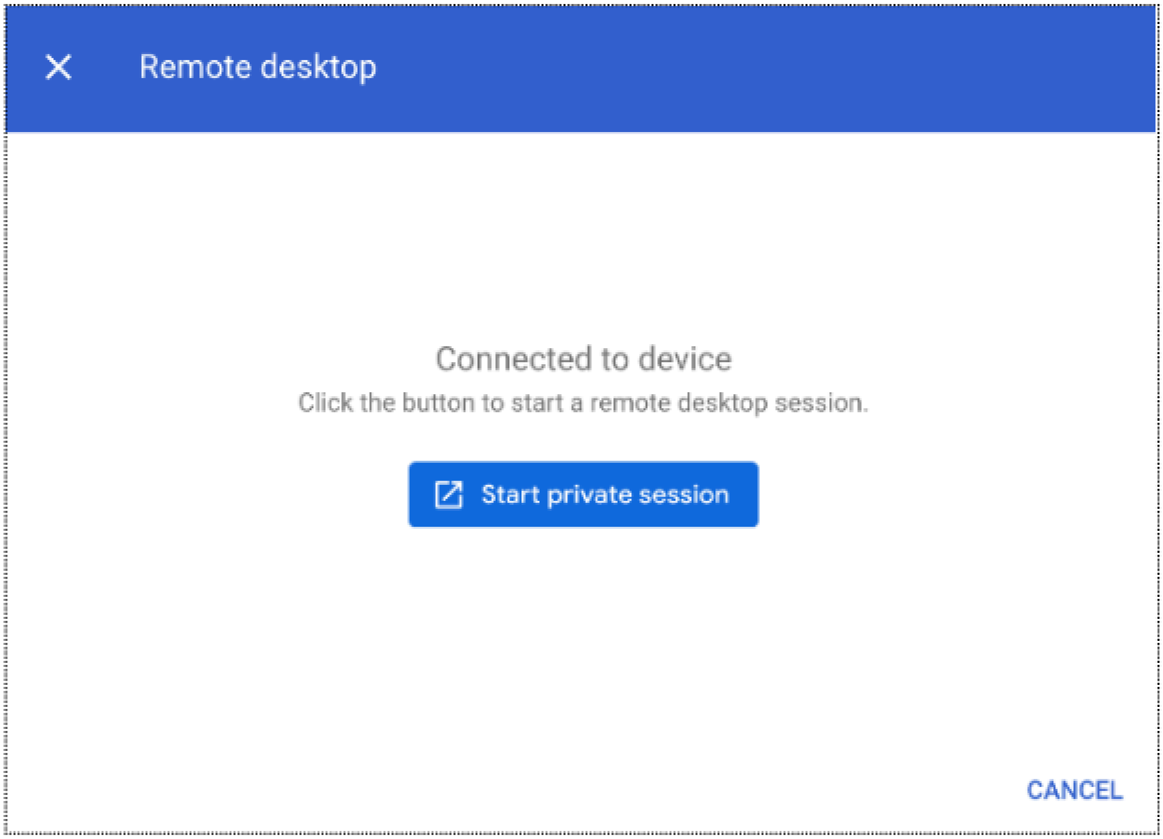
ChromeOS 126 supports firmware updates on a wide variety of additional peripherals. This significantly reduces the overhead and time needed to make new firmware updates available.

Web apps to capture multiple surfaces

Web apps can now capture multiple surfaces at once. This feature introduces a new API **getAllScreensMedia**() that allows developers to request several surfaces at once (instead of only one with **getDisplayMedia**()). This API auto-accepts capture requests, for managed sessions only, guarded by policies that have to be explicitly set by the device owners and with clear usage indicators so that users are aware of capturing at all times. For details, see our Help Center article.

Remote management for idle devices

Chrome Remote Desktop (CRD) is a feature that allows for remote control of ChromeOS devices, primarily for troubleshooting purposes, where a device is idle and unused. Admins can now initiate a CRD connection to a ChromeOS device sitting on the login screen. This enables an admin to sign-in to a managed device with their own set of credentials for troubleshooting or testing.



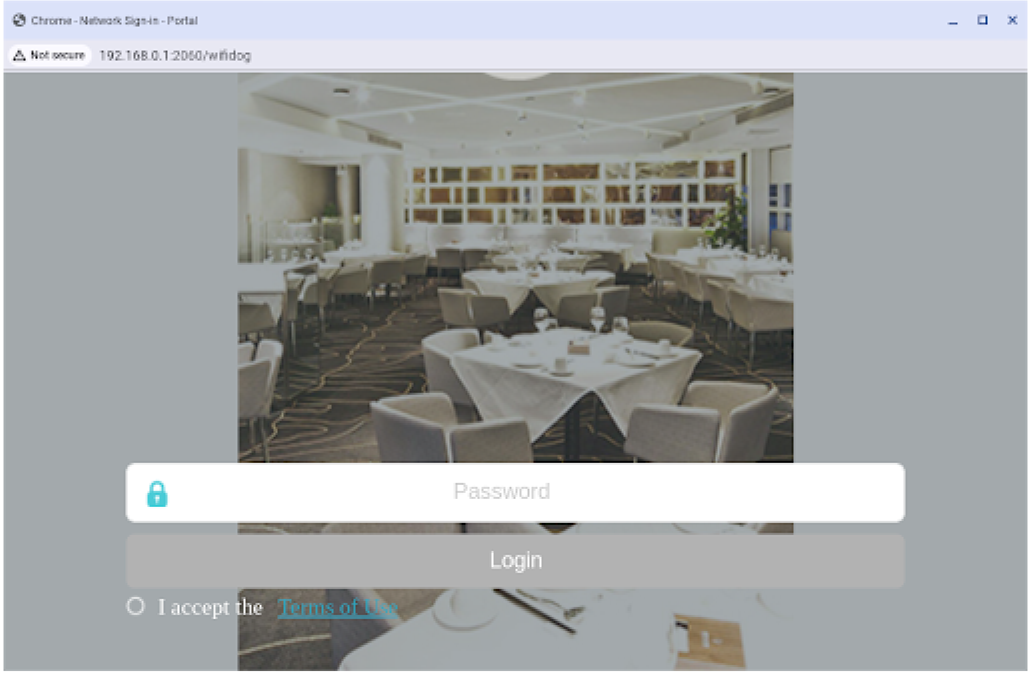
Remote desktop

Connected to device

Click the button to start a remote desktop session.

Captive portal for managed networks

Given that captive portal detection is always disabled for managed networks, administrators are unable to configure the ChromeOS device to auto connect to captive portal networks or to detect that the captive portal exists. If they do make the captive portal network managed, users have to manually open a browser and connect to an HTTP site that can then be redirected to a portal sign in page. We've added a new policy, CaptivePortalAuthenticationIgnoresProxy, which allows admins to force portal detection.


Chrome - Network Sign-in - Portal
Not secure
192.168.0.1:2060/wifidog
Password
Login
○ I accept the Terms of Use

Turn off overscroll behavior

A new setting is available to turn on and off the swipe gesture to navigate between pages. This feature is also known as overscroll or overscrolling pages. This setting is found under **Settings > Accessibility > Cursor and touchpad > Use a swipe gesture to navigate between pages.**

Turn off cursor blink rate

A new setting is available to turn off the blinking text cursor under **Settings > Accessibility > Keyboard and text input > Text cursor blink rate**. Customers with photosensitive seizure triggers and cognitive differences may want to turn off the blinking text cursor.

Magnifier to follow Select to Speak

Magnifier following Select to Speak is a feature designed for people who have low vision, but may be beneficial for anyone who enjoys reading text at larger sizes. When you read text aloud using Select to Speak, the screen magnifier will automatically follow the words, so you never lose your place. To try this out you can enable both Magnifier and Select to Speak in your settings. Zoom in to your preferred zoom level using Ctrl + Alt + Brightness up and Ctrl +

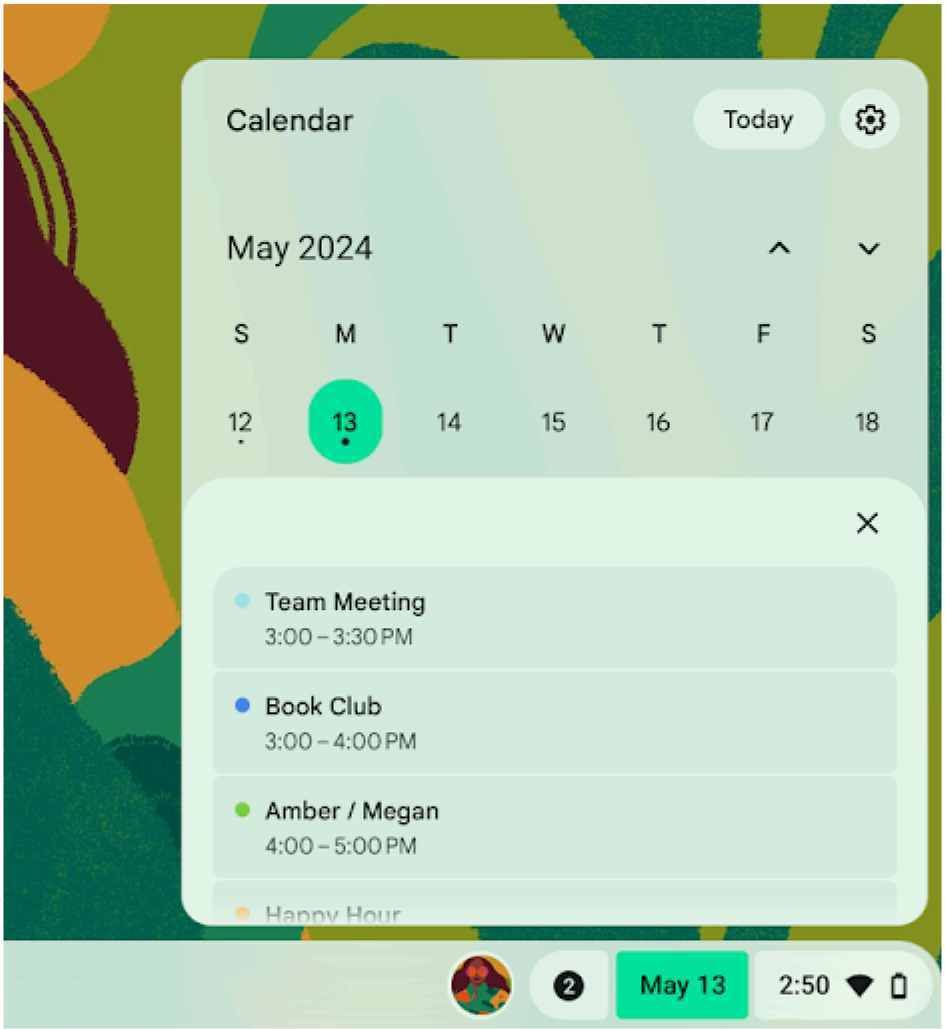
Alt + Brightness down. Select the text you want to read out and press the Select to Speak play button, or Search + S. A setting is available under the Magnifier settings to adjust this behavior.

Supervised user extensions installation

For supervised accounts managed via Family Link, we are separating the parental control for **Permissions for sites, extensions, and apps** to give parents more granular control. Parents now have two options to choose from: **Permissions for apps** and **Extensions**. The impact on supervised accounts is that a parent can now allow extensions installations with or without approval. Previously, parents could block extensions but had no way to allow them without approval.

Multi-calendar support

We are launching multi-calendar support to allow users view all events from multiple calendars that they have selected within their Google Calendar.



Team Meeting
3:00 – 3:30 PM

Book Club
3:00 – 4:00 PM

Amber / Megan
4:00 – 5:00 PM

Happy Hour

New policy to control Kiosk wake and sleep times

ChromeOS 126 introduces a new kiosk device policy that allows Admins to schedule when a device will wake and sleep. For more details, see Kiosk settings.

Locale expansion for Live Captions and Dictation

ChromeOS 126 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.

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 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.

Admin console updates

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.

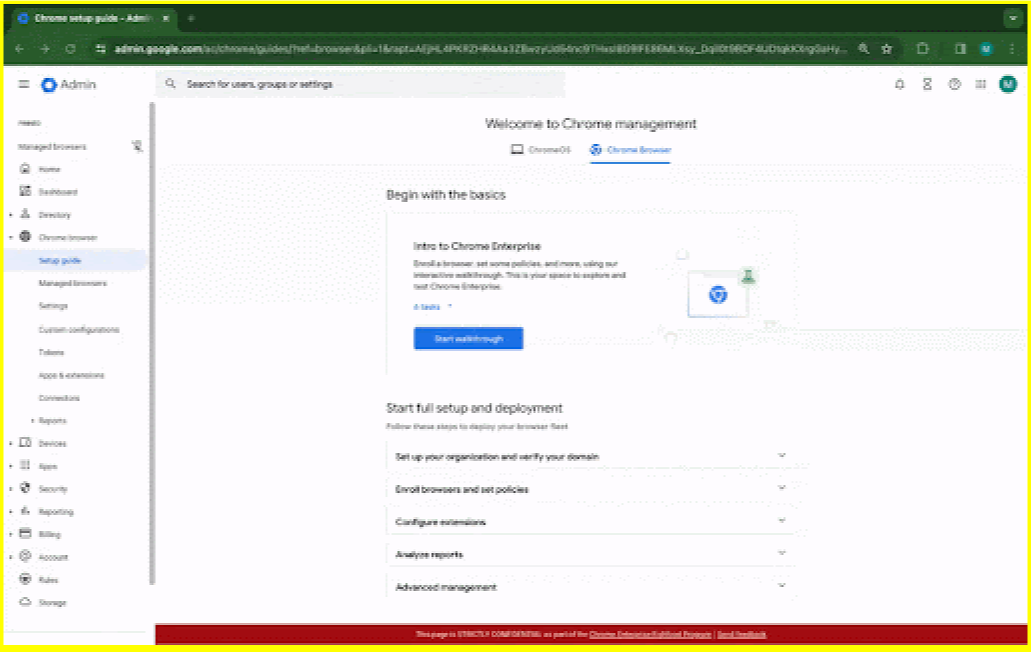
- **As early as Chrome 126 on Android, iOS, Linux, MacOS, Windows:** Trusted Tester access
- As early as Chrome 127 on Android, iOS, Linux, MacOS, Windows: Feature rolls out

Interactive setup guides for Chrome Enterprise Core

The Chrome Enterprise team introduces new interactive setup guides for browser management in the Admin console, where administrators can choose a journey they're interested in and get hands-on training in related 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.



Welcome to Chrome management

Begin with the basics

Intro to Chrome Enterprise

Enroll a browser, set some policies, and more, using our interactive walkthrough. This is your space to explore and test Chrome Enterprise.

Start full setup and deployment

Follow these steps to deploy your browser fleet

- Set up your organization and verify your domain
- Enroll browsers and set policies
- Configure extensions
- Analyze reports
- Advanced management

This page is STRICTLY CONFIDENTIAL as part of the [illegible] | Send feedback

- **As early as Chrome 126:** Feature rolls out

New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
DeviceExtendedAutoUpdateEnabled	Device	ChromeOS	Device update settings
LocalUserFilesAllowed	Users & Browser	ChromeOS	User experience
ScreenCaptureLocation	Users & Browser	ChromeOS	User experience

Coming soon

Upcoming Chrome browser updates

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

We plan 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 insight and context on risky activity.

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

Generating insights for DevTools console warnings and errors

In Chrome 125, a new Generative AI (GenAI) feature became available for unmanaged users: Generating insights for Chrome DevTools Console warnings and errors. These insights provide a personalized description and suggested fixes for the selected errors and warnings. Initially, this feature is only available to users (18+) in English. Admins can control this feature by using the DevToolsGenAiSettings policy.

- Chrome 125 on ChromeOS, Linux, Mac, Windows: Feature becomes available to unmanaged users globally, except Europe, Russia, and China.
- **Chrome 127 on ChromeOS, Linux, Mac, Windows:** Feature becomes available to managed Chrome Enterprise and Education users in supported regions.

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, starting with Chrome 127 pre-stable versions, 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. Read more on the Manifest timeline, including:

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

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 report any issues you encounter.

- **Chrome 127 on Windows:** Network Service sandboxed on Windows

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**

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 127 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 127 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.

- Chrome 124 on Linux, Mac, Windows: Trusted Tester access
- **Chrome 127 on Linux, Mac, Windows:** Feature rolls out

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 127 on Windows, Mac, Linux**

Cross-site ancestor chain bit for CookiePartitionKey of partitioned cookies

Chrome 127 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 127 on Windows, Mac, Linux**

Deprecate mutation events

Synchronous mutation events, including DOMSubtreeModified, DOMNodeInserted, DOMNodeRemoved, DOMNodeRemovedFromDocument, DOMNodeInsertedIntoDocument, and DOMCharacterDataModified, negatively affect 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 be removed or migrated to Mutation Observer. Starting in Chrome 124, a temporary enterprise policy, MutationEventsEnabled, will be 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. Report any issues here.

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

Support for *not* condition in ServiceWorker static routing API

The ServiceWorker static routing API is an API used for routing the request to the network, the ServiceWorker fetch handler, or directly looking up from cache, and so on. Each route consists of a condition and a source, and the condition is used for matching the request. For Chromium implementations, the *or* condition is only the supported condition. However, to write the condition more flexibly, supporting the *not* condition is expected, which matches the inverted condition inside.

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

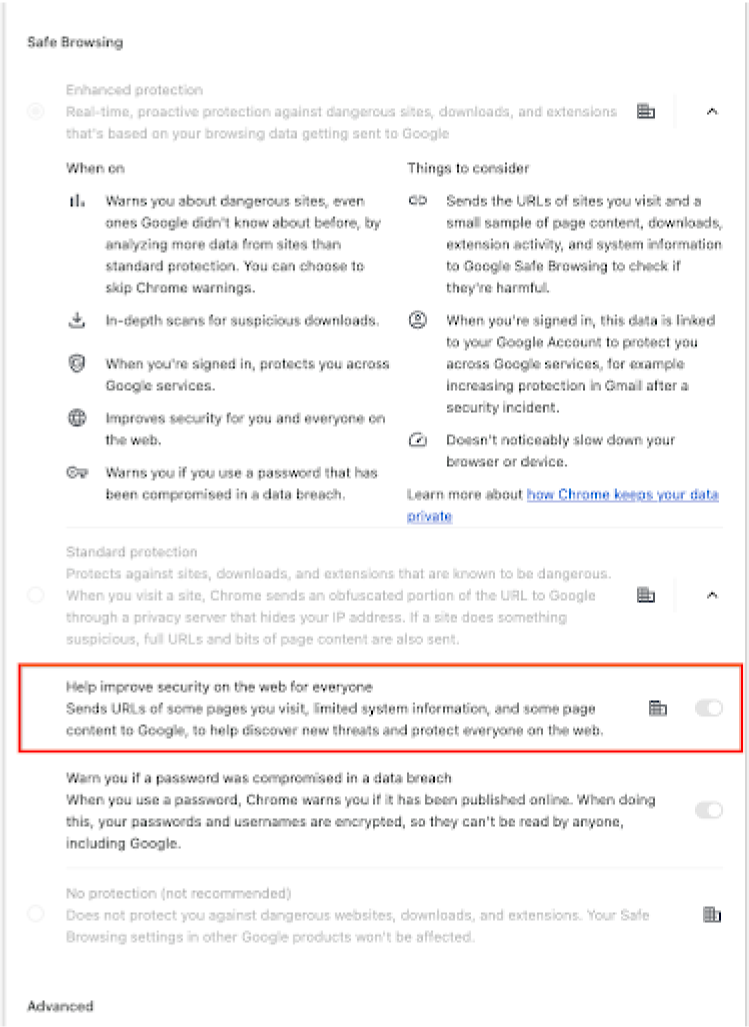
Ad-hoc code signatures for PWA shims on macOS

Code signatures for the application shims that are created when installing a Progressive Web App (PWA) on macOS are changing to use ad-hoc code signatures that 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 128 on Mac**

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

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

Chrome will no longer support macOS 10.15

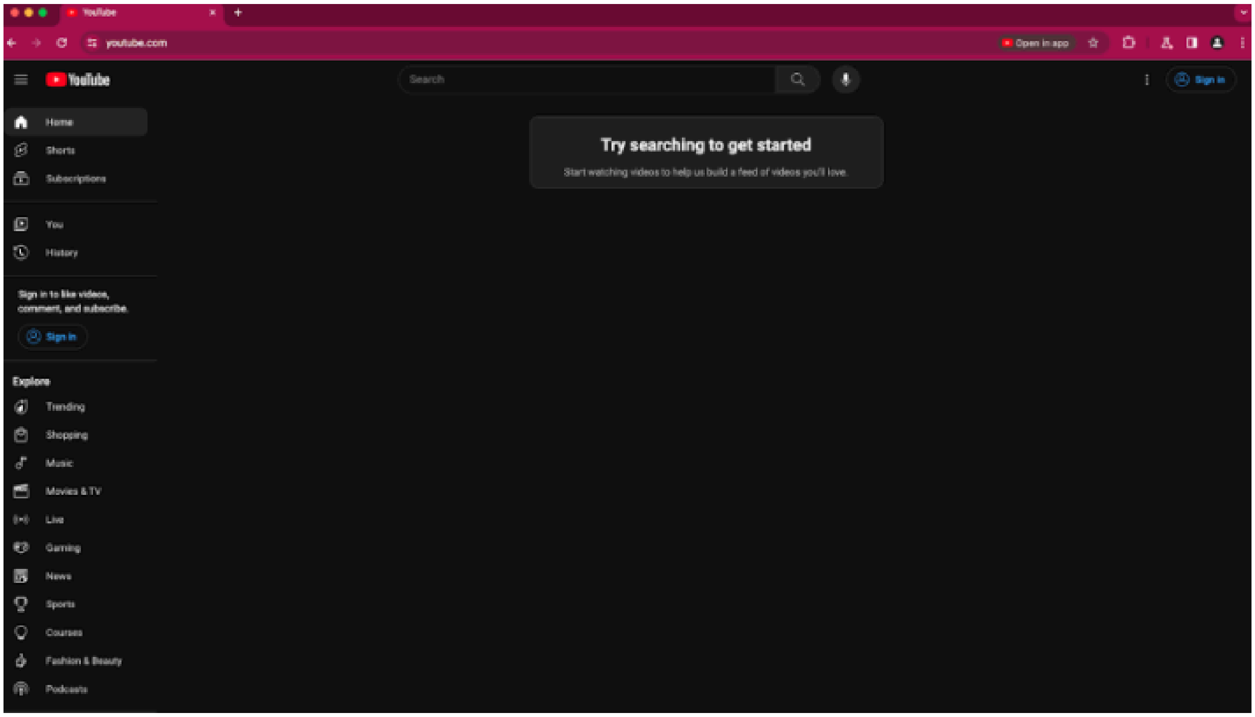
Chrome will no longer support macOS 10.15, which is already outside of its support window with Apple. Users have to update their operating systems in order to continue running Chrome browser. Running on a supported operating system is essential to maintaining security. If run on macOS 10.15, Chrome continues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

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 129 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).



Sign in to like videos, comment, and subscribe.

Try searching to get started

Start watching videos to help us build a feed of videos you'll love.

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 129, 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**

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 will display 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 called InsecureFormsWarningsEnabled is available to control this feature.

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

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, to help developers prepare for the coming enforcement.

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

Remove enterprise policy used for legacy same site behavior

In Chrome 79, we introduced the **InsecureFormsWarningsEnabled** 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.
Please see this blog post for more detail.

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

Upcoming ChromeOS changes

Snap groups on ChromeOS

As early as ChromeOS 127, **Snap groups** will allow you to group windows on ChromeOS. A snap group is formed when a user pairs two windows for a split-screen. The windows can then be brought back together, resized simultaneously, or moved as a group.

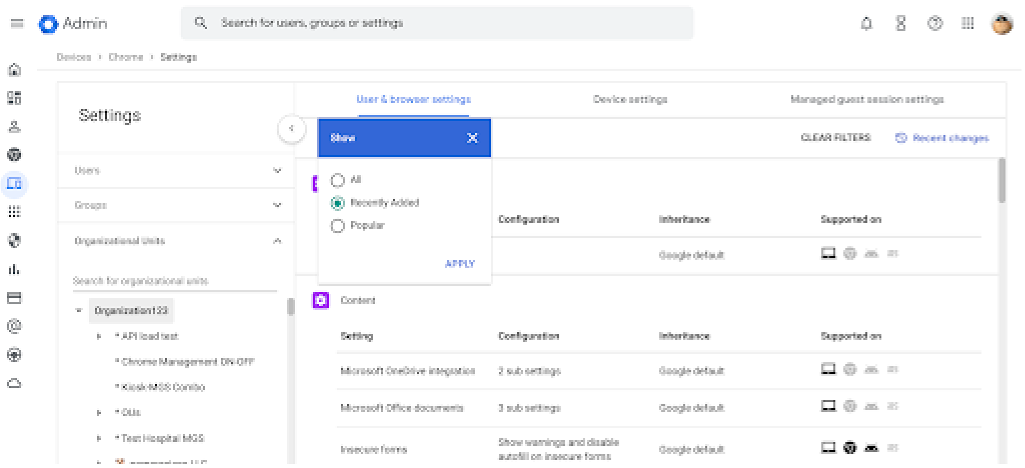
Read aloud in Reading Mode

As early as ChromeOS 127, Read Aloud will bring Google's high quality voices to Chrome Reading Mode for users to leverage Text to Speech to read content on the web. The goal of Read Aloud is to help people who have difficulty reading to understand long-form text. The new Read Aloud feature in Reading Mode on Chrome desktop allows users to hear the text they are reading, which improves focus and comprehension.

Upcoming Admin console changes

Filter for popular and recently added settings with policy tags

The Admin console will soon provide options to filter settings by *recently added* and *popular*. With these new filters, you'll be able to see our newest settings as well as see some of our most popular and relevant Chrome settings.



Show
○ All
● Recently Added
○ Popular

Setting	Configuration	Inheritance	Supported on
		Google default	

Content

Setting	Configuration	Inheritance	Supported on
Microsoft OneDrive integration	2 sub settings	Google default	
Microsoft Office documents	3 sub settings	Google default	
Insecure forms	Show warnings and disable autofill on insecure forms	Google default	

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 127 on Android, Linux, MacOS, Windows:** Early Trusted Tester access
- As early as Chrome 130 on Android, iOS, Linux, MacOS, Windows: Feature rolls out

Group based policy for Chrome browser

As an administrator, you will be able to use Google groups to add managed Chrome browsers to groups and set User & browser policies and Extension settings to a group of browsers. Managed browsers can be assigned to multiple groups, which allows IT administrators to have more flexibility to manage Chrome browsers using cloud management.

- **As early as Chrome 126 on Android, Linux, MacOS, Windows:** Trusted Tester access
- As early as Chrome 127 on Android, iOS, Linux, MacOS, Windows: Feature rolls out

Previous release notes

Chrome version & targeted Stable channel release date	PDF
Chrome 125: May 8, 2024	PDF
Chrome 124: April 10, 2024	PDF
Chrome 123: March 13, 2024	PDF
Chrome 122: February 14, 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.