chrome enterprise

Chrome 127 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 July 17, 2024.

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

Chrome 127 release summary

Chrome browser updates	Security / Privacy	User productivity / Apps	Management
App-bound encryption for cookies	✓		
Chrome Profile Separation - policy improvements			✓
Enhanced Safe Browsing promos on iOS	✓		
Entrust certificate distrust	✓		
Generating insights for DevTools console warnings and errors			✓
HTTPS-First Mode in Incognito	✓		
Migrate extensions to Manifest V3 before June 2025	✓	✓	✓
Policy to configure ACG for browser process			✓
Simplified sign-in and sync experience on Android		✓	
Additional Safe Browsing telemetry about pages	✓		
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	✓		
New and updated policies in Chrome browser			✓
Removed policies in Chrome browser			✓
ChromeOS updates	**Security/Privacy**	**User productivity/Apps**	**Management**
ChromeOS video conferencing: DLC states for features		✓	
ChromeOS audio Bluetooth telephony		✓	
OCR on Backlight		✓	
Firmware update instructions			✓
Read Aloud in Reading Mode		✓	
Classroom Glanceables		✓	
PDF page deletion and reordering		✓	
Admin console updates	**Security/Privacy**	**User productivity/Apps**	**Management**
Configure ChromeOS User & browser settings with Google groups			✓
Add managed browsers to groups for group-based policy management			✓
Filter for popular and recently added settings with policy tags			✓
Revamped ChromeOS Device List and Details			✓
New policies in the Admin console			✓
Upcoming Chrome browser updates	**Security / Privacy**	**User productivity / Apps**	**Management**
Isolated Web Apps	✓		

Rust JSON parser	✓		
Clear device data on sign out on iOS			✓
Attribution tags for search engine			✓
Tab Groups on iPad		✓	
Cross-site ancestor chain bit for CookiePartitionKey of partitioned cookies	✓		
Rename position-try-options to position-try-fallbacks	✓		
Ad-hoc code signatures for PWA shims on macOS		✓	
Chrome will no longer support macOS 10.15	✓		✓
Deprecate Safe Browsing Extended reporting	✓		
Deprecation of non-standard declarative shadow DOM serialization	✓		
Deprecate the includeShadowRoots argument on DOMParser	✓		
Network Service on Windows will be sandboxed			✓
Chrome Third-Party Cookie Deprecation (3PCD)	✓		
Insecure form warnings on iOS	✓		
User Link capturing on PWAs		✓	✓
Private network access checks for navigation requests: warning-only mode			✓
Insecure form warnings on iOS	✓		
Remove policy used for legacy same site behavior			✓

X25519Kyber768 key encapsulation for TLS	✓		
UI Automation accessibility framework provider on Windows		✓	
Upcoming ChromeOS changes	**Security / Privacy**	**User productivity / Apps**	**Management**
Snap Groups		✓	
Data processor mode: EU-wide rollout	✓		
Privacy Hub: Geolocation			
Upcoming Admin console changes	**Security/Privacy**	**User productivity/Apps**	**Management**
Chrome browser managed profile reporting			✓
Admin console widget for data controls			✓

The enterprise release notes are available in 9 languages. You can read about Chrome's updates in English, German, French, Dutch, Spanish, Portuguese, Korean, Indonesian, and Japanese. Allow 1 to 2 weeks for translation for some languages.

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

Current Chrome version release notes

Chrome browser updates

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 running at the same privilege as Chrome 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 Profile Separation - policy improvements

Chrome profiles offer a user-friendly way to keep personal and work browsing data separate, simplifying the experience, preventing data breaches, and ensuring privacy and compliance. We have created three intuitive policies to help you control profile separation in your organization: ProfileSeparationSettings, ProfileSeparationDataMigrationSettings and ProfileSeparationDomainExceptionList. These policies replace ManagedAccountsSigninRestriction and EnterpriseProfileCreationKeepBrowsingData.

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

Enhanced Safe Browsing promos on iOS

In Chrome 127, users who do not already have Enhanced Safe Browsing enabled see an infobar promoting Enhanced Safe Browsing on the Safe Browsing warning page. We also show a promotion for Enhanced Safe Browsing on the Chrome settings page, for users who do not already have Enhanced Safe Browsing enabled. These promos are not shown to users when the SafeBrowsingProtectionLevel enterprise policy is set to any value.

- **Chrome 127 on iOS**

Entrust certificate distrust

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

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

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

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

For additional information and testing resources, see Sustaining Digital Certificate Security - Entrust Certificate Distrust.

To learn more about the Chrome Root Store, see this FAQ.

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

Generating insights for DevTools Console warnings and errors

In Chrome 127, this Generative AI (GenAI) feature becomes available for managed Chrome Enterprise and Education users in supported regions: Generating insights for Chrome DevTools Console warnings and errors. These insights provide a personalized description and suggested fixes for the selected errors and warnings. 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:** Chrome 127 on ChromeOS, Linux, Mac, Windows: Feature becomes available for managed Chrome Enterprise and Education users in supported regions.

HTTPS-First Mode in Incognito

Starting in Chrome 127, as part of Chrome's move towards HTTPS by default, HTTPS-First Mode is enabled by default in Incognito mode. Users will see a warning before they navigate to sites over insecure HTTP. This can be controlled using the existing enterprise policies HttpsOnlyMode and HttpAllowlist.

- **Chrome 127 on Android, 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, starting with Chrome 127 pre-stable versions, Chrome begins to gradually disable Manifest V2 extensions running in the browser.
You can use the ExtensionManifestV2Availability policy 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, Windows, Mac, Linux:** 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.

Policy to configure ACG for browser process

A new policy called DynamicCodeSettings is available in Chrome 127. Setting this policy to '1' switches on Arbitrary Code Guard (ACG) for the browser process. ACG prevents dynamic code being generated from within the browser process, which can help prevent potentially hostile code making unauthorized changes to the behavior of the browser process.

Switching on ACG might cause compatibility issues with third-party software that must run inside the browser process.

- **Chrome 127 on Windows**

Simplified sign-in and sync experience on Android

Chrome 127 launches a simplified and consolidated version of sign-in and sync in Chrome on Android. Chrome sync is no longer 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 in earlier releases, 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 still be disabled via BrowserSignin.

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**

Additional Safe Browsing telemetry about pages

When an Enhanced Safe Browsing user visits a page that triggers vibration, keyboard or pointer lock API, attributes of that page are now sent to Safe Browsing. If the telemetry is sent and the page seems to be malicious, users see a Safe Browsing warning and their keyboard or pointer is unlocked, if they were locked. If you'd like your users to avail of this feature, set MetricsReportingEnabled to true and set the SafeBrowsingProtectionLevel policy to 2.

- **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 can now use and save passwords in their Google Account. Relevant policies such as BrowserSignin, SyncTypesListDisabled and PasswordManagerEnabled continue to work as before and can be used to configure whether users can use and save passwords in their Google Account.

- **Chrome 127 on Android**

Watermarking

This feature allows admins to overlay a watermark on top of a webpage if navigating to it triggers a specific Data loss Prevention (DLP) rule. It will contain a static string displayed as the watermark. Watermarking is available to Chrome Enterprise Premium customers only.

- 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 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**

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. In Chrome 124, a temporary enterprise policy, MutationEventsEnabled, was introduced to re-enable deprecated or removed mutation events.

Starting in Chrome 127, mutation event support is disabled by default , from 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.

For more details, see this post on the Chrome developer blog. You can report any issues on the Chromium issue tracker.

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

Keyboard-focusable scroll containers

Chrome 127 improves accessibility by making scroll containers focusable using sequential focus navigation.
In previous releases, the tab key did not focus scrollers unless tabIndex was explicitly set to 0 or more.
By making scrollers focusable by default, users who can't (or don't want to) use a mouse can now focus clipped content using keyboard 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**

New and updated policies in Chrome browser

Policy	Description
DynamicCodeSettings	Policy controls the dynamic code settings
CSSCustomStateDeprecatedSyntaxEnabled	Controls whether the deprecated :--foo syntax for CSS custom state is enabled
KeyboardFocusableScrollersEnabled	Enable keyboard focusable scrollers

Removed policies in Chrome browser

Policy	Description
BlockTruncatedCookies	Block truncated cookies
UserAgentClientHintsGREASEUpdateEnabled	Control the User-Agent Client Hints GREASE Update feature

ChromeOS updates

ChromeOS Video Conferencing: DLC States for features

ChromeOS 127 introduces a visual enhancement for Downloadable Content (DLC) in the video control panel. This release now adds status indicators for Noise Cancellation, Live Captions, Relighting, and Blur.

Audio Bluetooth Telephony

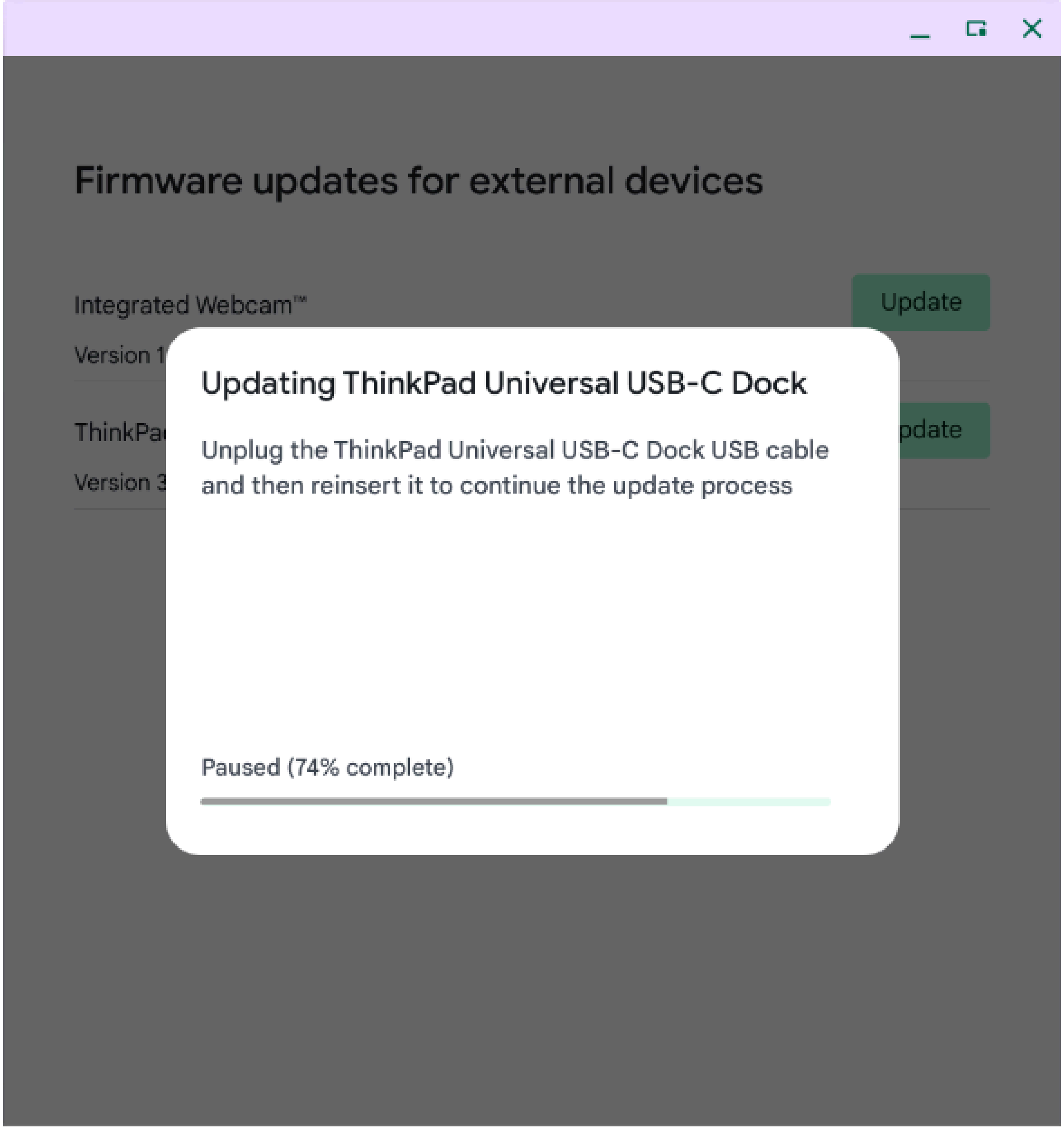
ChromeOS now supports call control buttons on compatible Bluetooth headsets, including answering, rejecting or terminating a call, and muting the microphone.

OCR on Backlight

ChromeOS is launching a PDF OCR AI reader on Gallery, enabling reading for inaccessible documents, further filling the gap in accessibility for low vision and blind users that use a screen reader. ChromeOS leverages its machine learning models to extract, compartmentalize, and section PDF documents to make them more accessible on the Gallery app for ChromeVox users.

Firmware update app: Update Instructions for peripheral devices

The Firmware Updates app on ChromeOS now supports updating peripherals that require user action during the update, for example, unplugging and re-plugging the peripheral. When an update is available for one of these devices, the user will be guided with clear, step-by-step instructions. For most existing peripherals, the update experience remains unchanged.



Firmware updates for external devices

Updating ThinkPad Universal USB-C Dock

Unplug the ThinkPad Universal USB-C Dock USB cable and then reinsert it to continue the update process

Paused (74% complete)

Read aloud in Reading Mode

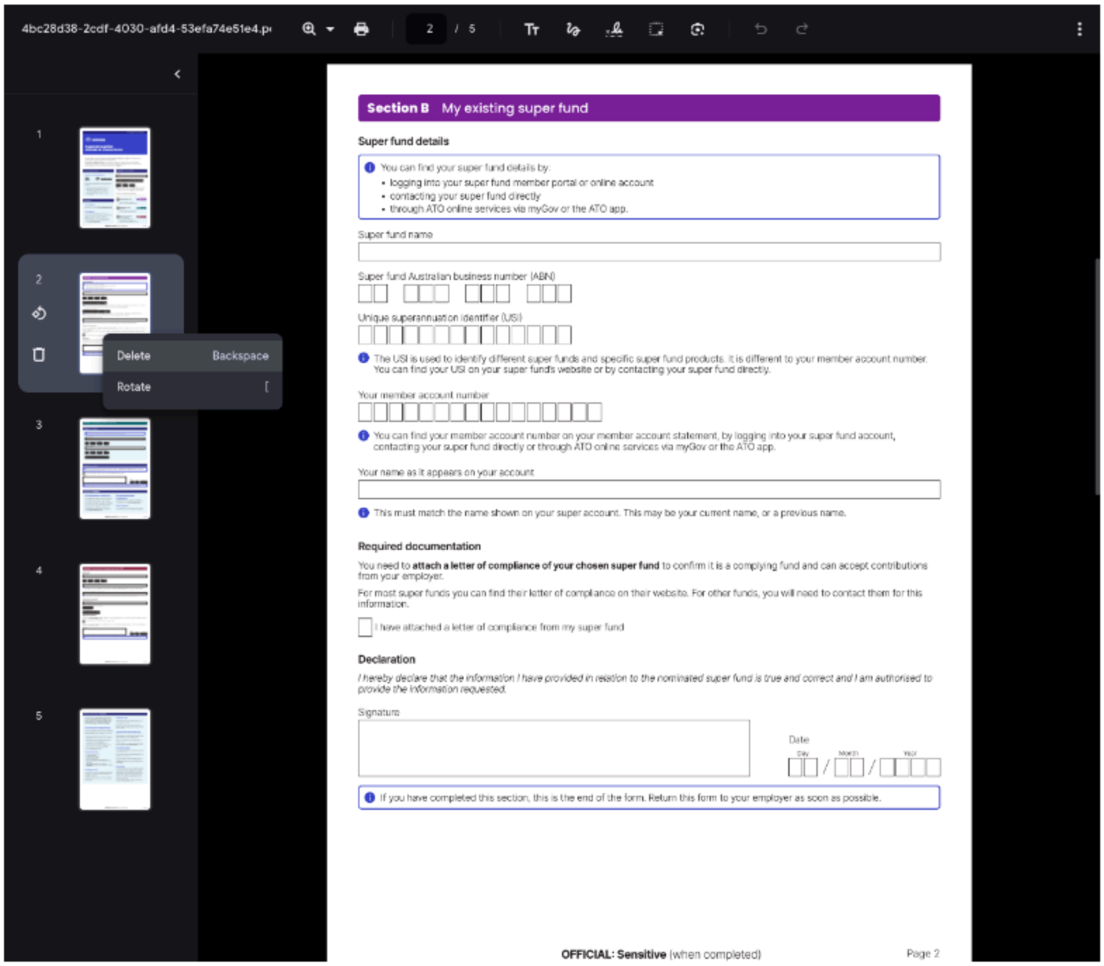
As early as ChromeOS 127, Read Aloud will bring Google's high quality voices to Chrome Reading Mode for users to leverage Text to Speech to read content on the web. The goal of Read Aloud is to help people who have difficulty reading to understand long-form text. The new Read Aloud feature in Reading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

Classroom Glanceables

Students can now quickly view and access their upcoming Classroom assignments one click away on their Chromebook home screen. Users can see this new feature if they are logged into a Chromebook with an account where they are enrolled in active courses in Google Classroom. Users can find this feature by clicking on the date chip on the shelf of their Chromebook if they are logged into an account, where they will see the new panel which can view lists of their upcoming, due, missing and completed assignments.

PDF Page deletion and reordering

The Gallery app in ChromeOS now supports more options for editing PDF pages. You can now delete or reorder pages within a PDF via mouse or by using keyboard shortcuts.
PDF page deletion:



Section B My existing super fund

Super fund details

You can find your super fund details by:

- logging into your super fund member portal or online account
- contacting your super fund directly
- through ATO online services via myGov or the ATO app.

Super fund name

Super fund Australian business number (ABN)

□□ □□□ □□□ □□□

Unique superannuation identifier (USI)

□□□□□□□□□□□□□□

The USI is used to identify different super funds and specific super fund products. It is different to your member account number. You can find your USI on your super fund's website or by contacting your super fund directly.

Your member account number

□□□□□□□□□□□□□□□□

You can find your member account number on your member account statement, by logging into your super fund account, contacting your super fund directly or through ATO online services via myGov or the ATO app.

Your name as it appears on your account

This must match the name shown on your super account. This may be your current name, or a previous name.

Required documentation

You need to **attach a letter of compliance of your chosen super fund** to confirm it is a complying fund and can accept contributions from your employer.

For most super funds you can find their letter of compliance on their website. For other funds, you will need to contact them for this information.

□ I have attached a letter of compliance from my super fund

Declaration

I hereby declare that the information I have provided in relation to the nominated super fund is true and correct and I am authorised to provide the information requested.

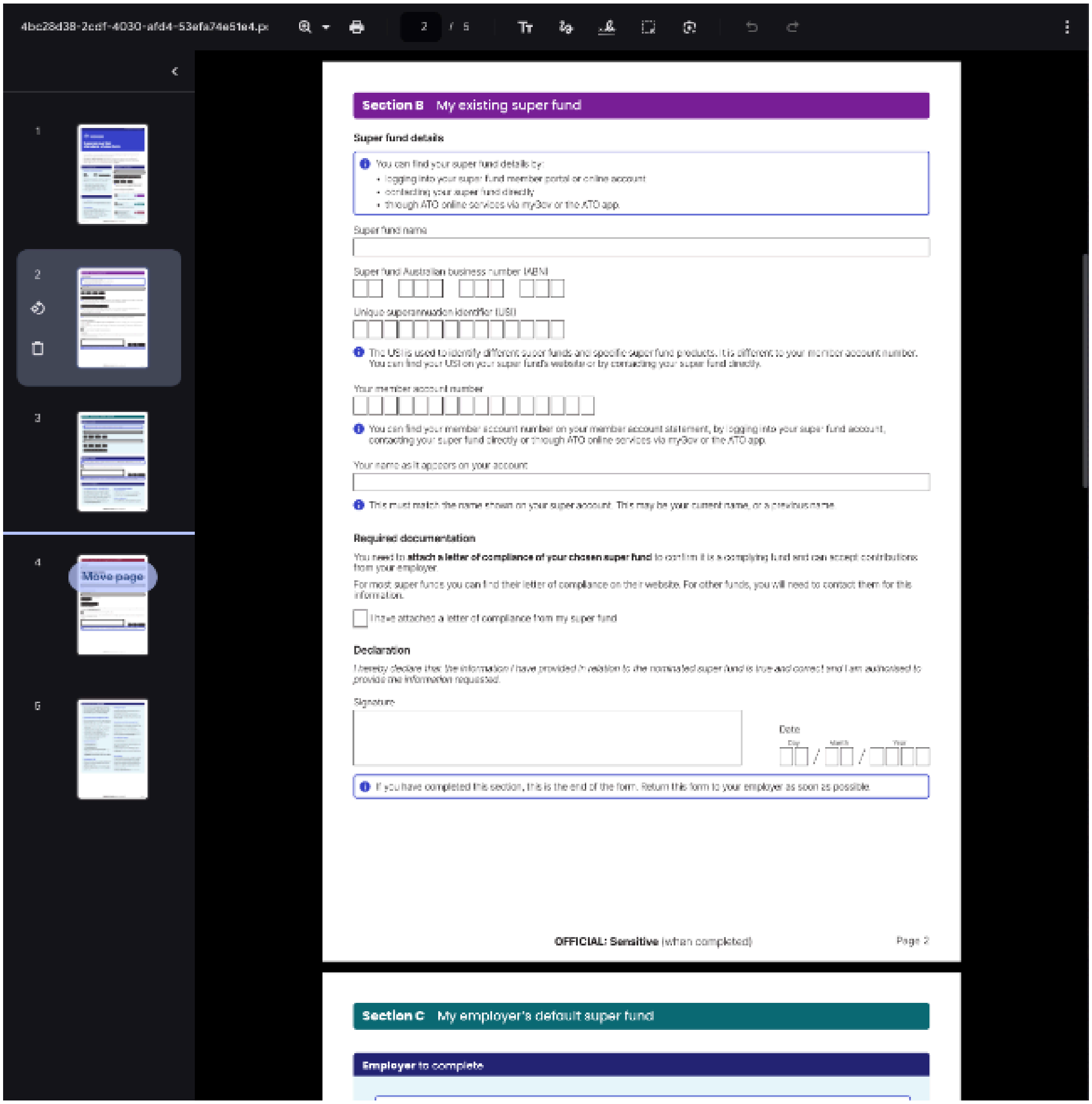
Signature

Date
Day Month Year
□□ / □□ / □□□□

If you have completed this section, this is the end of the form. Return this form to your employer as soon as possible.

OFFICIAL: Sensitive (when completed) Page 2

PDF page reorder:



Section B My existing super fund

Super fund details

You can find your super fund details by:

- logging into your super fund member portal or online account
- contacting your super fund directly
- through ATO online services via myGov or the ATO app.

Super fund name

Super fund Australian business number (ABN)

Unique superannuation identifier (USI)

The USI is used to identify different super funds and specific super fund products. It is different to your member account number. You can find your USI on your super fund's website or by contacting your super fund directly.

Your member account number

You can find your member account number on your member account statement, by logging into your super fund account, contacting your super fund directly or through ATO online services via myGov or the ATO app.

Your name as it appears on your account

This must match the name shown on your super account. This may be your current name, or a previous name.

Required documentation

You need to **attach a letter of compliance of your chosen super fund** to confirm it is a complying fund and can accept contributions from your employer.

For most super funds you can find their letter of compliance on their website. For other funds, you will need to contact them for this information.

□ I have attached a letter of compliance from my super fund

Declaration

I hereby declare that the information I have provided in relation to the nominated super fund is true and correct and I am authorised to provide the information requested.

Signature

Date
Day / Month / Year

If you have completed this section, this is the end of the form. Return this form to your employer as soon as possible.

OFFICIAL: Sensitive (when completed) Page 2

Section C My employer's default super fund

Employer to complete

Admin console updates

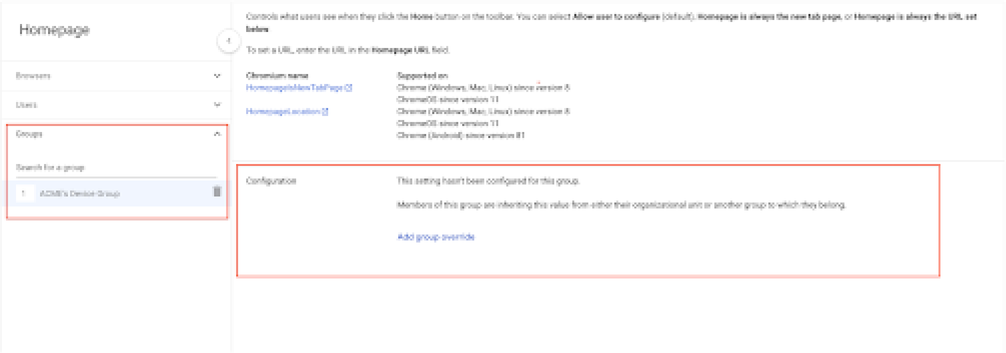
Configure ChromeOS User & browser settings with Google groups

Admins can now use Google groups to manage ChromeOS **User & browser settings** in the Admin console and API. Admins can use new or existing Google Groups to configure **User & browser settings** in their organizations. When admins need to configure a policy for a specific set of users–who might belong to different organizational units (OUs)–they can use the flexibility of groups without needing to reconfigure their OUs. To learn more, see Managing group-based policies.

Today, the majority of user settings are configurable by Groups, with most of the remaining settings available in the coming months. Available settings are automatically filtered and displayed when admins select a particular group.

Add managed browsers to groups for group-based policy management

Admins can now add managed Chrome browsers to Google groups, thereby allowing them to specify **User & browser** policies and extension settings for 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.



Homepage

Controls what users see when they click the **Home** button on the toolbar. You can select **Allow user to configure** (default), **Homepage is always the new tab page**, or **Homepage is always the URL set below**.

To set a URL, enter the URL in the **Homepage URL** field.

Chromium name	Supported on
HomepageIsNewTabPage	Chrome (Windows, Mac, Linux) since version 8 ChromeOS since version 11
HomepageLocation	Chrome (Windows, Mac, Linux) since version 8 ChromeOS since version 11 Chrome (Android) since version 81

Configuration: This setting hasn't been configured for this group.

Members of this group are inheriting this value from either their organizational unit or another group to which they belong.

Filter for popular and recently added settings with policy tags

The Admin console now provides 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.

Revamped ChromeOS device list and details

The Admin console devices page redesigned with a proactive and actionable notification for your fleet of devices.
Notifications module: Easily identify and address device issues with the new Notifications module, providing an overview of ongoing problems in your fleet.
Centralized dashboards: Quickly access all the information and reports you need about your fleet, all in one convenient location – the Dashboards tab.
Revamped device list page: Find more detailed information about your devices with new tabs (General, OS, Hardware, Network, and Policy), device-specific notifications, and a new card design for improved readability.

Coming soon

Upcoming Chrome browser updates

Isolated Web Apps

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

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

In this initial release IWAs will only be installable through an admin policy on enterprise-managed ChromeOS devices.

- **Chrome 128 on ChromeOS**

Rust JSON parser

As early as Chrome 128, Chrome will parse JSON using Rust, rather than C++. This will remove the risk of memory safety vulnerabilities in the JSON parser, improving security. This change should be transparent to users. There is a small risk that some invalid JSON (which Chrome currently accepts) no longer being accepted, although the Rust parser remains extremely lenient.

- **Earliest Chrome 128:** Chrome will parse JSON using Rust

Clear device data on sign out on iOS

Starting Chrome 128, signing out from a managed account in an unmanaged browser will delete browsing data that is saved on the device. Managed users will be presented a confirmation dialog on sign-out explaining that the data will be cleared. Data will be cleared only from the time of sign-in, otherwise all data will be cleared; time of sign-in is only known if the user signed in on Chrome 122 or later.

The data that will be deleted includes:

- browsing history
- cookies and site data
- Passwords
- site settings
- Autofill
- cached images and files

- **Chrome 128 on iOS**

Attribution tags for Search Engine

As part of our Digital Markets Act (DMA) compliance, Google is introducing choice screens for users to choose their default search engine within Chrome. The choice from the prompt controls the default search engine setting, currently available at `chrome://settings/search`.

Selections from this screen will have their search URL appended with an attribution tag for use by third party search engines to attribute traffic from selections originating from the search engine choice screen. This change will not be applied for Education-configured organizations or Enterprises with metrics or usage statistics turned off.

For enterprises that have chosen to have their administrator set their enterprise users' search settings using the enterprise policies DefaultSearchProviderEnabled and DefaultSearchProviderSearchUrl, those policies continue to control their enterprise search settings. Where the administrator has not set their enterprise users' search settings by policy, enterprise users might see a prompt to choose their default search engine within Chrome. Read more about these policies and the related atomic group.

- **Chrome 128 on Android, iOS, 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 128 on iOS**

Cross-site ancestor chain bit for CookiePartitionKey of partitioned cookies

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

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

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

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

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

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

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 129 on Mac**

Chrome will no longer support macOS 10.15

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

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

Deprecate Safe Browsing Extended reporting

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

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

Deprecation of non-standard declarative shadow DOM serialization

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

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

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

Deprecate the includeShadowRoots argument on DOMParser

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

Now that a standardized version of this API, in the form of setHTMLUnsafe() and parseHTMLUnsafe() shipped in Chrome 124, the non-standard `includeShadowRoots` argument needs to be deprecated and removed. All usage should shift accordingly:

Instead of:

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

This can be used instead:

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

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

Network Service on Windows will be sandboxed

To improve security and reliability, the network service, already running in its own process, will be sandboxed on Windows. As part of this, third-party code that is currently able to tamper with the network service may be prevented from doing so. This might cause interoperability issues with software that injects code into Chrome's process space, such as Data Loss Prevention software. The NetworkServiceSandboxEnabled policy allows you to disable the sandbox if incompatibilities are discovered. You can test the sandbox in your environment using these instructions. You can use the Chromium bug tracker to report any issues you encounter.

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

Chrome Third-Party Cookie Deprecation (3PCD)

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. For more details, see Allow or restrict third party cookies. 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 the Privacy Sandbox section on Google for Developers.

- **Chrome 130 on Android, iOS, ChromeOS, LaCrOS, Linux, Mac, Windows:** A new enterprise policy will be added to control 3rd party cookies

User Link capturing on PWAs

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

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

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

Before a website A navigates to another site B in the user's private network, this feature does the following:
1. Checks whether the request has been initiated from a secure context.
2. Sends a preflight request, and checks whether B responds with a header that allows private network access.
There are already features for subresources and workers, but this one is for navigation requests specifically. These checks protect the user's private network.
Since this feature is the *warning-only* mode, we do not fail the requests if any of the checks fail. Instead, a warning will be shown in the DevTools console, to help developers prepare for the coming enforcement.

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

Insecure form warnings on iOS

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

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

Remove enterprise policy used for legacy same site behavior

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

- **Chrome 132 on Android, ChromeOS, Linux, Mac, Windows:** Remove LegacySameSiteCookieBehaviorEnabledForDomainList policy

X25519Kyber768 key encapsulation for TLS

Starting in Chrome 124, Chrome enables by default on all desktop platforms a new post-quantum secure TLS key encapsulation mechanism X25519Kyber768, based on a NIST standard (ML-KEM). This protects network traffic from Chrome with servers that also support ML-KEM from decryption by a future quantum computer. This is exposed as a new TLS cipher suite. TLS automatically negotiates supported ciphers, so this change should be transparent to server operators. This cipher will be used for both TLS 1.3 and QUIC connections.

However, some TLS middleboxes might be unprepared for the size of a Kyber (ML-KEM) key encapsulation, or a new TLS ClientHello cipher code point, leading to dropped or hanging connections. This can be resolved by updating your middlebox, or disabling the key

encapsulation mechanism via the temporary PostQuantumKeyAgreementEnabled enterprise policy, which will be available through the end of 2024. However, long term, post-quantum secure ciphers will be required in TLS and the enterprise policy will be removed.
Post-quantum cryptography is required for CSNA 2.0.
For more detail, see this Chromium blog post.

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

UI Automation accessibility framework provider on Windows

Starting in Chrome 126, Chrome will start directly supporting accessibility client software that uses Microsoft Windows's UI Automation accessibility framework. Prior to this change, such software interoperated with Chrome by way of a compatibility shim in Microsoft Windows. This change is being made to improve the accessible user experience for many users. It provides complete support for Narrator, Magnifier, and Voice Access; and will improve third-party apps that use Windows's UI Automation accessibility framework. Users of Chrome will find reduced memory usage and processing overhead when used with accessibility tools. It will also ease development of software using assistive technologies.

Administrators might use the UiAutomationProviderEnabled enterprise policy, available from Chrome 125, to either force-enable the new provider (so that all users receive the new functionality), or disable the new provider. This policy will be supported through Chrome 136, and will be removed in Chrome 137. This one-year period is intended to give enterprises sufficient time to work with third-party vendors so that they may fix any incompatibilities resulting from the switch from Microsoft's compatibility shim to Chrome's UI Automation provider.

- Chrome 125 on Windows:The UiAutomationProviderEnabled policy is introduced so that administrators can enable Chrome's UI Automation accessibility framework provider and validate that third-party accessibility tools continue to work.
- Chrome 126 on Windows: The Chrome variations framework will be used to begin enabling Chrome's UI Automation accessibility framework provider for users. It will be progressively enabled to the full stable population, with pauses as needed to

address compatibility issues that can be resolved in Chrome. Enterprise administrators may continue to use the UiAutomationProviderEnabled policy to either opt-in early to the new behavior, or to temporarily opt-out through Chrome 136.
- **Chrome 137 on Windows:** The UiAutomationProviderEnabled policy will be removed from Chrome. All clients will use the browser's UI Automation accessibility framework provider.

Upcoming ChromeOS changes

Snap groups on ChromeOS

As early as ChromeOS 128, **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.

Data processor mode: EU-wide rollout

In ChromeOS 128, new data processor mode features and ChromeOS terms will be made available to the entire EU through the Google Admin console. For more details, see Overview of ChromeOS data processor mode.
As a ChromeOS administrator, you'll have the option to activate **Data processor mode**, which covers a set of ChromeOS features and services referred to as **Essential Services**.

Privacy Hub: Geolocation

As early as ChromeOS 128, we will make privacy on Chromebooks easier to manage by adding the ability to control geolocation access to the privacy controls page. Users will be able to set geolocation access to Allowed, System Only, or Blocked depending on their preference.
We will allow users to block all apps or websites, or entire systems access to geolocation regardless of previously granted permissions, and provide users easy to use controls to re-enable them whenever it would be helpful.

Upcoming Admin console changes

Chrome browser managed profile reporting

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

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

Admin console widget for data controls

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

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

Previous release notes

Chrome version & targeted Stable channel release date	PDF
Chrome 126: June 5, 2024	PDF
Chrome 125: May 8, 2024	PDF
Chrome 124: April 10, 2024	PDF
Chrome 123: March 13, 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