chrome enterprise

Chrome 122 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 February 16, 2024.

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

Chrome 122 release summary

Chrome Browser updates	Security/Privacy	User productivity/Apps	Management
Chrome Third-Party Cookie Deprecation (3PCD)	✓		
Generative AI features		✓	
Default Search Engine choice screen		✓	
Simplified sign-in and sync experience on iOS		✓	✓
SharedImages for PPAPI Video Decode	✓		
Download URL for Chrome Browser Enterprise changing			✓
V8 security setting	✓		
Read aloud		✓	
Network Service on Windows will be sandboxed	✓		
Removal of enterprise policy ChromeAppsWebViewPermissiveBehaviorAllowed			✓
Asynchronous server-side Safe Browsing check	✓		
Improved download warnings on the Chrome Downloads page	✓		
Skip unload events	✓		
Autofill: security code updates		✓	
Removing unenrollment from Unified Password Manager		✓	
Chrome on iOS: bottom address bar		✓	

DefaultSearchProvider policy changes			✓
New and updated policies in Chrome browser			✓
Removed policies in Chrome browser			✓
ChromeOS updates	**Security/Privacy**	**User productivity/Apps**	**Management**
Content scanning with BCE	✓		
Battery Saver		✓	
Enhanced SAML reauthentication flows	✓		
Badge-based authentication	✓		
Edit your recordings with Screencast		✓	
IkeV2 VPN support	✓	✓	
Mandatory extensions in Incognito	✓		✓
New look for ChromeOS media player		✓	
Admin Console Updates	**Security/Privacy**	**User productivity/Apps**	**Management**
Inactive browser deletion in Chrome Browser Cloud Management			✓
New policies in the Admin console			✓
Upcoming Chrome Browser updates	**Security/Privacy**	**User productivity/Apps**	**Management**
User link capturing on PWAs - Windows, MacOS and Linux	✓		
Resume tabs		✓	
Chrome on Android or iOS: cross-device resumption		✓	

Resume the last opened tab on any device		✓	
Permissions prompt for Web MIDI API	✓		
Network Service on Windows will be sandboxed	✓		
Chrome Sync ends support for Chrome 81 and earlier	✓		✓
Deprecate and remove WebSQL	✓		
IdleTimeout and IdleTimeoutActions Policies on iOS			✓
Cross Profile Password Reuse Detection	✓		
Telemetry for permission prompts and accepting notification permissions	✓		
ServiceWorker static routing API	✓		
Private network access checks for navigation requests: warning-only mode	✓		
Bookmarks and reading list improvements on Android		✓	
Deprecate enterprise policy ThrottleNonVisibleCrossOriginIframesAllowed			✓
Remove support for UserAgentClientHintsGREASEUpdateEnabled			✓
Intent to deprecate: Mutation Events		✓	
Remove LegacySameSiteCookieBehaviorEnabledForDomainList policy			✓
Extensions must be updated to leverage Manifest V3	✓	✓	✓

Upcoming ChromeOS updates	**Security/Privacy**	**User**	**Management**

		productivity/Apps	
ChromeOS Flex Bluetooth Migration			✓
Customizing keyboard shortcuts		✓	
Record GIFs with Screen capture		✓	
Faster Split Screen setup		✓	
Upcoming Admin Console Updates	**Security/Privacy**	**User productivity/Apps**	**Management**
Enhanced Settings page experience		✓	
Chrome crash report			✓
Legacy Technology report			✓

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

Current Chrome version release notes

Chrome browser updates

Chrome Third-Party Cookie Deprecation (3PCD)

As previously announced, Chrome 120 started to restrict third-party cookies by default for 1% of Chrome users to facilitate testing, and subsequent releases will ramp up to 100% of users as early as Q3 2024. The ramp up to 100% of users is subject to addressing any remaining competition concerns of the UK's Competition and Markets Authority (CMA). Browsers that are part of the 1% experiment group also see new Tracking Protection user controls. You can try out these changes in Chrome 120 or higher by enabling `chrome://flags/#test-third-party-cookie-phaseout`.

This testing period allows sites to meaningfully preview what it's like to operate in a world without third-party cookies. As bounce-tracking protections are also a part of 3PCD, the users in this group with third-party cookies blocked have bounce tracking mitigations taking effect, so that their state is cleared for sites that get classified as bounce trackers. Most enterprise users are excluded from this 1% experiment group automatically; however, we recommend that admins proactively use the BlockThirdPartyCookies and CookiesAllowedForUrls policies to re-enable third-party cookies and opt out managed browsers ahead of the experiment. This gives enterprises time to make the changes required to avoid relying on this policy or on third-party cookies.

We are launching the Legacy Technology Report to help identify third-party cookies use cases. Admins can set the BlockThirdPartyCookies policy to false to re-enable third-party cookies for all sites but this will prevent users from changing the corresponding setting in Chrome. Alternatively, to prevent breakage, you can set the CookiesAllowedForUrls policy to allowlist your enterprise applications to continue receiving third-party cookies.

For enterprise end users that are pulled into this experiment group and that are not covered by either enterprise admin policy, they 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 also covered by the same policies as cookies and these protections are enforced when the bouncing site is not permitted to use 3P cookies. So setting the BlockThirdPartyCookies policy to false, or setting the CookiesAllowedForUrls policy for a site, prevents bounce tracking mitigations from deleting state for sites.

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.

The heuristics feature grants temporary third-party cookie access in limited scenarios based on user behavior. This mitigates site breakage caused by third-party cookie deprecation in established patterns, such as identity provider pop ups and redirects.

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.

Generative AI features

Starting in Chrome 122, there are 3 **Generative AI (**GenAI) features that are now also available for managed users that have signed into Chrome browser:

- Tab organizer: Chrome can automatically suggest tab groups for users based on the URL and title of opened websites. To use this feature, right-click on a tab, and select **Organize similar tabs**.

- Create themes with AI: Lets users create a unique Chrome theme (a combination of a color and a wallpaper image) using GenAI. To use the feature, open a new tab, and at the bottom right, click **Customize Chrome**. On the side panel, select **Change theme > Create with AI**. Users can then choose from preset options for subject, mood, style, and color.

- Get help writing on the web with AI: This feature helps users write with more confidence and kickstart the writing process in free-form text fields on the web. To use this feature, right-click on a text field, and select **Help me write**.

Initially, these 3 features are only available to users in English in the US. Admins can control these by using the TabOrganizerSettings, CreateThemesSettings and HelpMeWriteSettings policies. For each feature, you have the following options for your organization:

0 = Enable the feature and send data to help improve AI models

1 = Enable the feature but don't send data to help improve AI models

2 = Fully disable feature

You can find more information in the **Tab group suggestionsTab organizer**, **Create themes**, and **Help me write** help center articles.

Default Search Engine choice screen

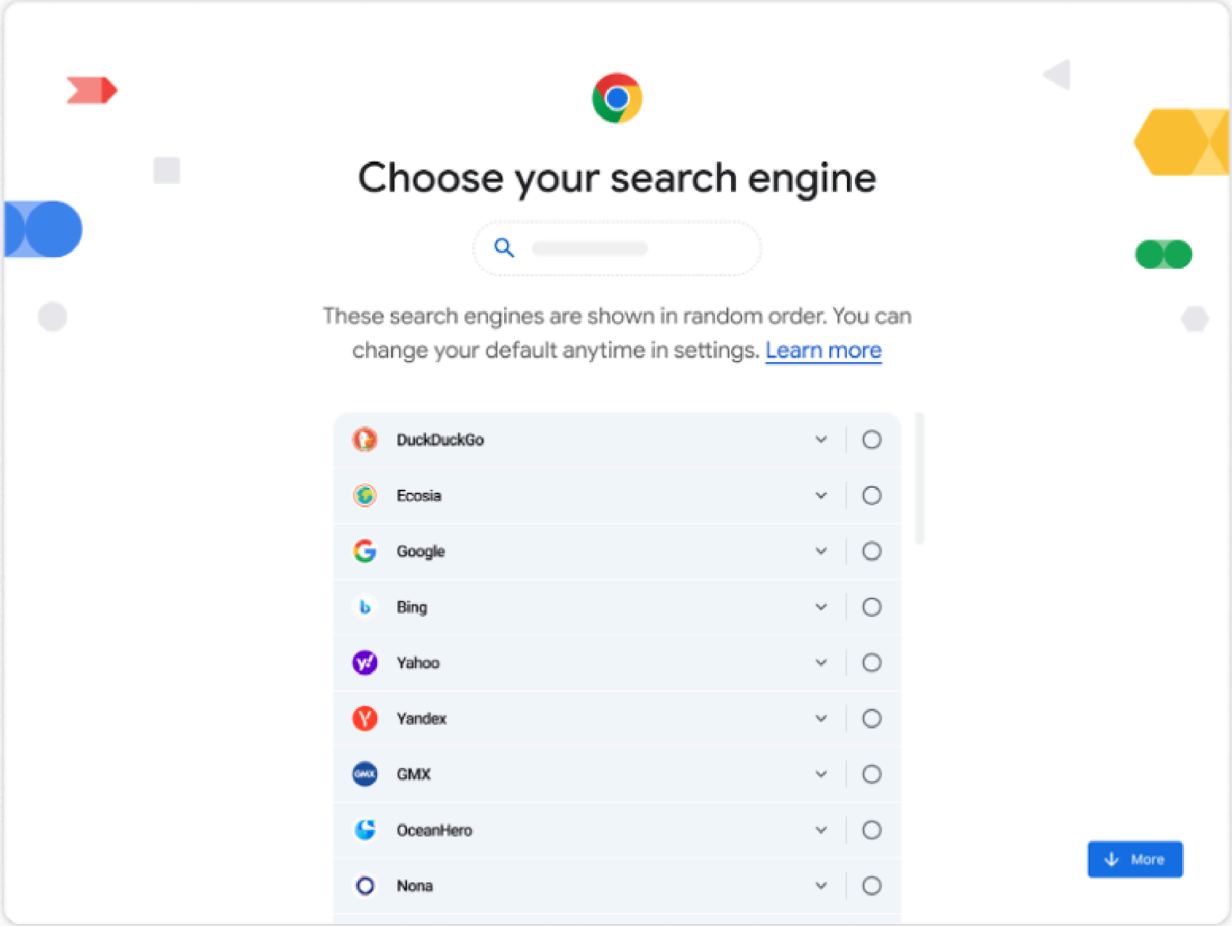
As part of our Digital Markets Act (DMA) compliance, in Chrome 122, Google is introducing choice screens for users to choose their default search engine within Chrome. The choice from the prompt will control the default search engine setting, currently available at `chrome://settings/search`.

For enterprises that have chosen to have their administrator set their enterprise users' search settings using the enterprise policies DefaultSearchProviderEnabled and DefaultSearchProviderSearchUrl, those policies will continue to control their enterprise's 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 120 on iOS, ChromeOS, LaCrOS, Linux, MacOS, Windows: 1% users might start getting the choice screen with Chrome 120.

- **Chrome 122 on iOS, ChromeOS, LaCrOS, Linux, MacOS, Windows: full roll-out for applicable users.**



Choose your search engine

These search engines are shown in random order. You can change your default anytime in settings. Learn more

- DuckDuckGo ○
- Ecosia ○
- Google ○
- Bing ○
- Yahoo ○
- Yandex ○
- GMX ○
- OceanHero ○
- Nona ○

This UI design is sample only and subject to change

Simplified sign-in and sync experience on iOS

Starting in Chrome 122, existing users on iOS with Chrome sync turned on now experience a simplified and consolidated version of sign-in and sync in Chrome. Chrome sync no longer appears 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 that saves and accesses Chrome data in the Google Account can be turned off fully (via SyncDisabled) or partially (via SyncTypesListDisabled). Sign-in to Chrome can be required or disabled via BrowserSignin as before.

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

- Chrome 117: no longer shows Chrome sync as a separate feature for users who didn't have Chrome sync enabled at the time.
- **Chrome 122: no longer shows Chrome sync as a separate feature for users who had Chrome sync enabled by migrating them to an equivalent state.**

SharedImages for PPAPI video decoder

Chrome 122 removes the PPAPISharedImagesForVideoDecoderAllowed policy, used to control the recent refactor for VideoDecoder APIs in PPAPI plugin. This policy was introduced on a temporary basis in Chrome 119.

- Chrome 119 on ChromeOS, LaCrOS: Introduces escape hatch policy.
- **Chrome 122 on ChromeOS, LaCrOS:** Escape hatch policy and corresponding old code paths are removed.

New download URLs for Chrome browser (Enterprise)

From February 8th, the main download pages for Chrome Browser Enterprise (Windows and MacOS) change to:

- Windows https://chromeenterprise.google/download/?modal-id=download-chrome-demo#windows-download
- MacOS https://chromeenterprise.google/download/?modal-id=download-chrome-demo#mac-download

To avoid disruption, enterprises that leverage automation to download Chrome need to change their scripts to capture these URL changes.

New V8 security setting

Chrome 122 adds a new setting on `chrome://settings/security` to disable the V8 JIT optimizers, to reduce the attack surface of Chrome browser. This behavior continues to be controlled by the DefaultJavaScriptJitSetting enterprise policy, and the associated JavaScriptJitAllowedForSites and JavaScriptJitBlockedForSites policies. The setting is integrated into Site Settings. The enterprise policies have been available since Chrome 93.

- **Chrome 122 on ChromeOS, LaCrOS, Linux, MacOS, Windows, Fuchsia**

Read aloud

Read aloud allows users of Chrome on Android to listen to web pages using text to speech technology. Users can now access this feature via the overflow menu and control playback via audio controls.

Read aloud sends the page URL to Google servers to power playback, and users who use it need to enable the settings menu item **Make searches and browsing better**.

Setting the ListenToThisPageEnabled policy to true allows users to have eligible web pages read aloud using text-to-speech. This is achieved by server side content distillation and audio synthesis. Setting to false disables this feature, and if this policy is set to default or left unset, Read aloud is enabled.

- **Chrome 122 on Android:** Feature launches

Removal of enterprise policy ChromeAppsWebViewPermissiveBehaviorAllowed

Chrome 122 removes the temporary enterprise policy ChromeAppsWebViewPermissiveBehaviorAllowed, which was made available in Chrome 116 to give enterprises time to address possible breakage related to Chrome Apps webview usage changes. .

- **Chrome 122 on Linux, MacOS, Windows, ChromeOS**: Enterprise Policy ChromeAppsWebViewPermissiveBehaviorAllowed removed

Asynchronous server-side Safe Browsing check

Today Safe Browsing checks are on the blocking path of page loads, meaning that users cannot see the page until the checks are complete. To improve Chrome's loading speed, checks with the server-side Safe Browsing list no longer block page loads in Chrome 122.

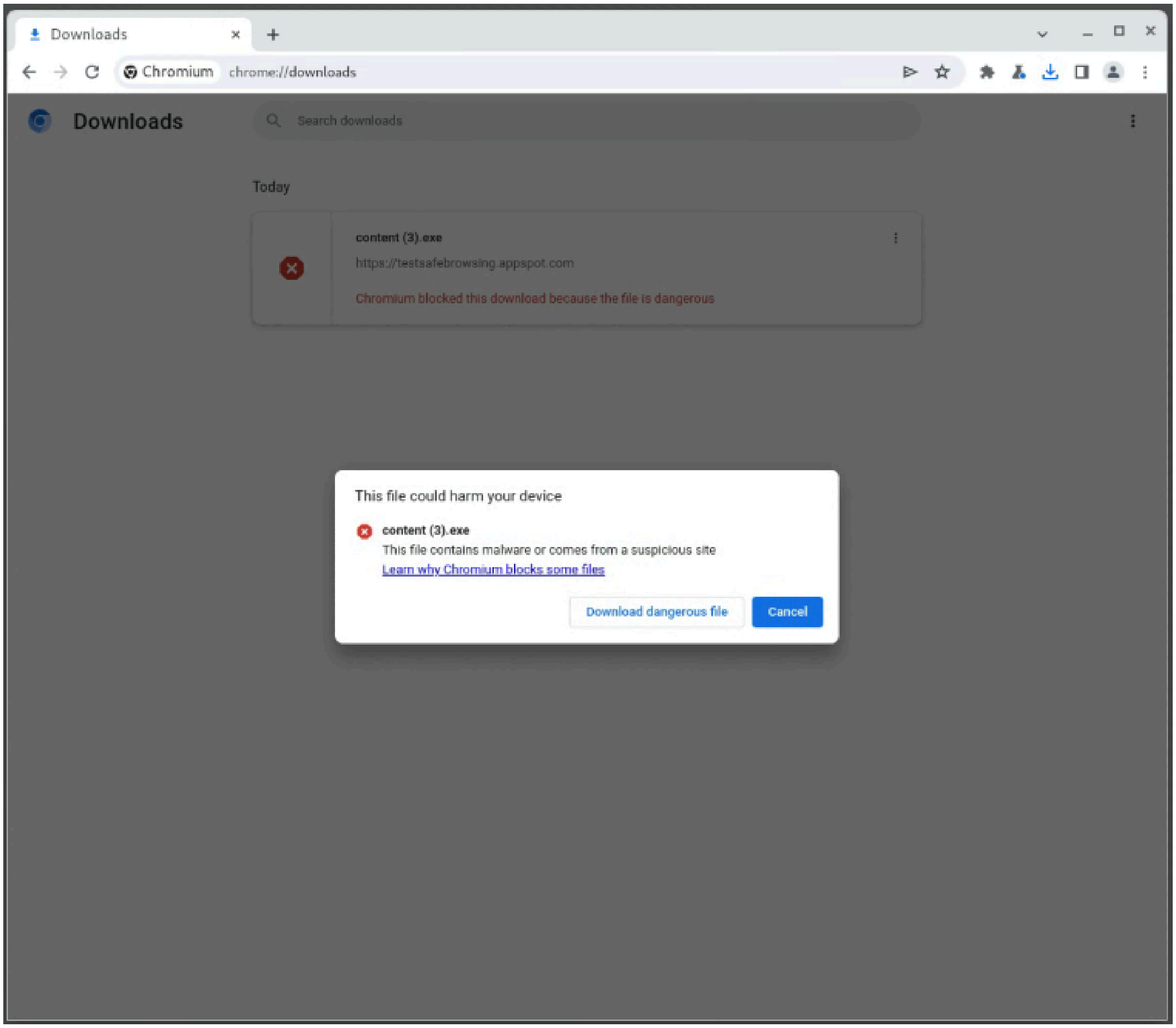
We have evaluated the risk and put mitigations in place:
1) To protect against direct exploits against the browser, local list checks are still conducted in a synchronous manner so that malicious payloads cannot run until the local list check is complete.
2) To protect against phishing attacks, we've looked at data and concluded that it is unlikely the user would have significantly interacted with the page (for example, typed a password) by the time we show a warning.

- **Chrome 122 on Android, ChromeOS, LaCrOS, Linux, MacOS, Windows:** Feature launches

Improved download warnings on the Chrome Downloads page

To help reduce consequences of downloading malware, we're cleaning up desktop download warning strings and patterns to be clear and consistent.

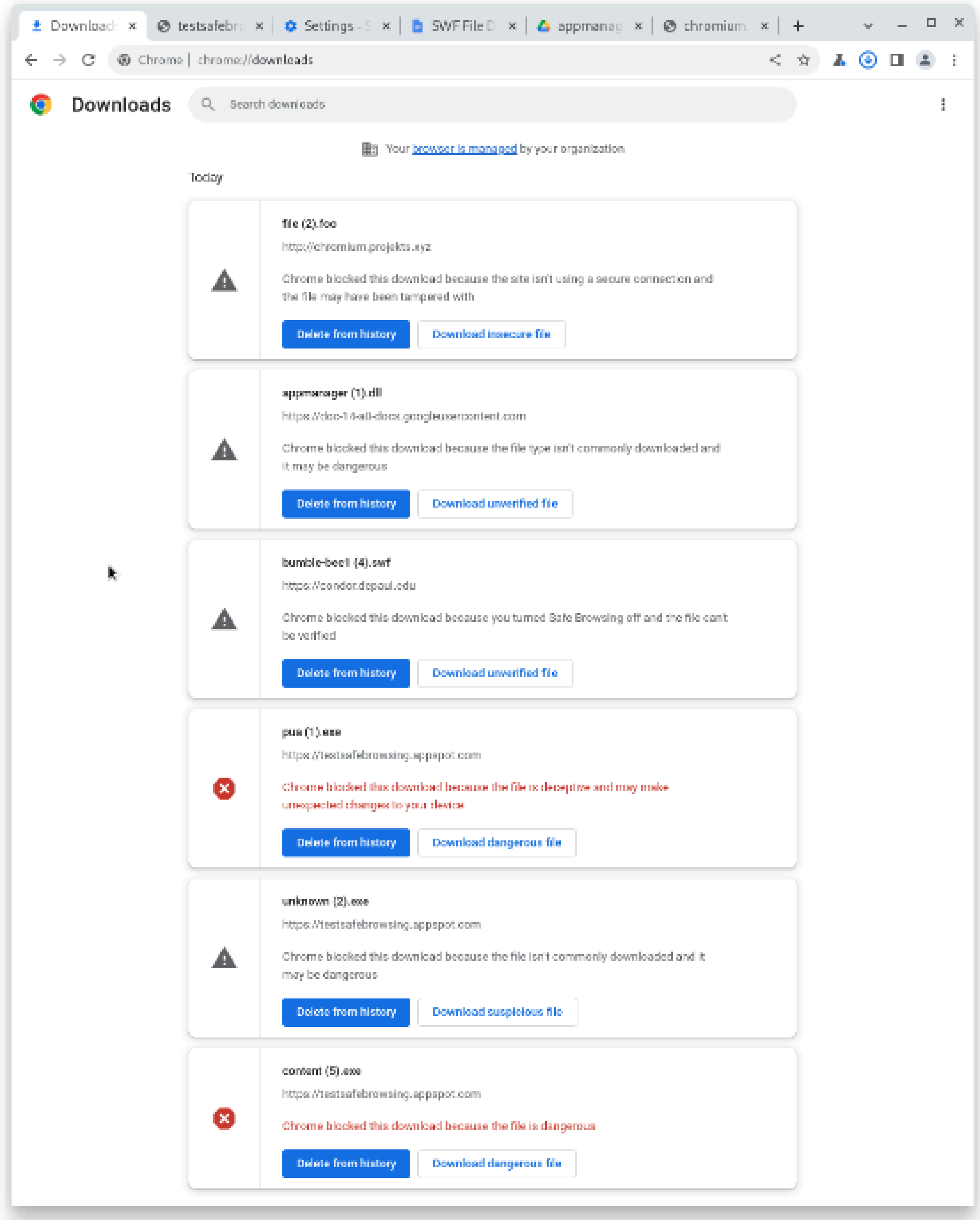
- **Chrome 122 on ChromeOS, LaCrOS, Linux, MacOS, Windows, Fuchsia:** Feature launches



content (3).exe
https://testsafebrowsing.appspot.com
Chromium blocked this download because the file is dangerous

This file could harm your device

content (3).exe
This file contains malware or comes from a suspicious site
Learn why Chromium blocks some files



Your browser is managed by your organization

Today

file (2).foo
http://chromium.projekts.xyz
Chrome blocked this download because the site isn't using a secure connection and the file may have been tampered with

appmanager (1).dll
https://doc-14-a0-docs.googleusercontent.com
Chrome blocked this download because the file type isn't commonly downloaded and it may be dangerous

bumble-bee1 (4).swf
https://condor.depaul.edu
Chrome blocked this download because you turned Safe Browsing off and the file can't be verified

pua (1).exe
https://testsafebrowsing.appspot.com
Chrome blocked this download because the file is deceptive and may make unexpected changes to your device

unknown (2).exe
https://testsafebrowsing.appspot.com
Chrome blocked this download because the file isn't commonly downloaded and it may be dangerous

content (5).exe
https://testsafebrowsing.appspot.com
Chrome blocked this download because the file is dangerous

Skip unload events

The presence of unload event listeners is a primary blocker for back/forward cache on Chromium based browsers and for Firefox on desktop platforms. On the other hand, for mobile platforms, almost all browsers prioritize the bfcache by not firing unload events in most cases. To improve the situation, we've been working with lots of partners and successfully reduced the use of unload event listeners over the last few years. To further accelerate this migration, we propose to have Chrome for desktop gradually skip unload events.

In case you need more time to migrate away from unload events, we'll offer temporary opt-outs in the form of a Permissions-Policy API and an enterprise policy ForcePermissionPolicyUnloadDefaultEnabled, which allow you to selectively keep the behavior unchanged.

- Chrome 117 on ChromeOS, Linux, MacOS, Windows: Dev Trial
- Chrome 119 on ChromeOS, Linux, MacOS, Windows: Introduces ForcePermissionPolicyUnloadDefaultEnabled policy
- **Chrome 122 -132 on ChromeOS, Linux, MacOS, Windows:** Deprecation trial (general rollout of deprecation will be limited scope until deprecation trial is ready)
- Chrome 122 unload handlers will be gradually skipped for 1% of users on top-50 sites, as proposed here.

Autofill: security code updates

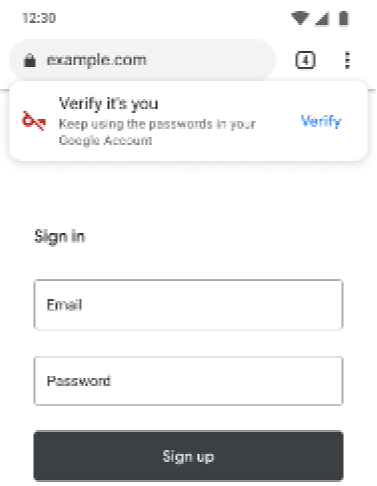
In Chrome 122, payments autofill allows you to save security codes for local and server cards to improve user experience. Security codes are only saved if a user consents to saving it. Users always have the option to turn security code saving off in Chrome Settings.

- **Chrome 122 on Android, MacOS:** feature rolls out

Removing unenrollment from Unified Password Manager

Chrome 122 removes unenrollment from Unified Password Manager on Android. When Google Play Services responds with an error users lose access to Password Manager features (password saving or updating, password generation) until the error is resolved. For some errors, there is an error message with an action button to resolve the problem. Other issues are supposed to be temporary (for example, during Google Play Services update).

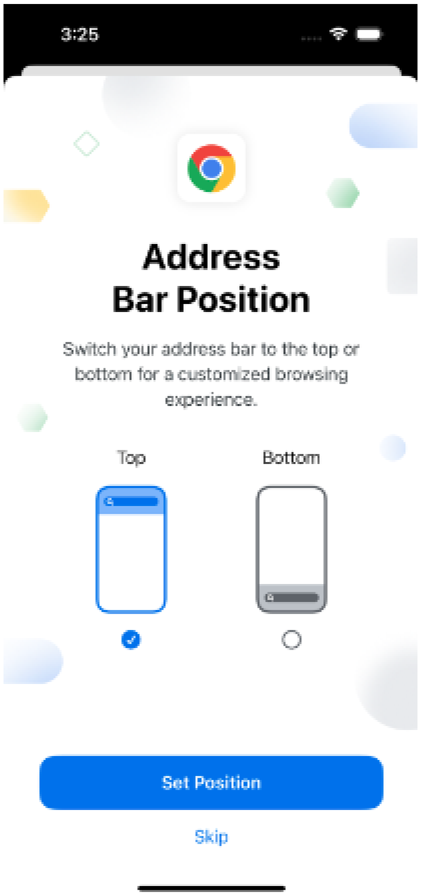
  - **Chrome 122 on Android:** feature rolls out


Verify it's you
Keep using the passwords in your Google Account

Chrome on iOS: bottom address bar on iPhone

We recently launched a customizable address bar that allows users to choose between a top and a bottom address bar on iPhone. The address bar position picker screen is now added to the First Run Experience.

- **Chrome 122 on iOS:** feature rolls out



Address Bar Position

Switch your address bar to the top or bottom for a customized browsing experience.

[✓ Top] ○ Bottom

DefaultSearchProvider policy changes

In Chrome 122, we are making some changes to the DefaultSearchProvider* policies. We have removed the **DefaultSearchProviderIconURL** on all platforms because Chrome now uses the favicon image provided by the search engine. DefaultSearchProviderKeyword and DefaultSearchProviderNewTabURL are not supported on iOS and Android, alongside (but support continues on) Linux, Mac OS and Windows. We fixed the supported platform set to reflect this.

New and updated policies in Chrome browser

Policy	Description
InsecureFormsWarningsEnabled	Enable warnings for insecure forms (now available on iOS)
ListenToThisPageEnabled	Enable read aloud (text distillation and text-to-speech synthesis) for web pages

Removed policies in Chrome browser

Policy	Description
PPAPISharedImagesForVideoDecoderAllowed	Allow Pepper to use shared images for video decoding.
ChromeAppsWebViewPermissiveBehaviorAllowed	Restore permissive Chrome Apps webview behavior
DefaultSearchProviderIconURL	Default search provider icon (removed on all platforms)
DefaultSearchProviderKeyword	Default search provider keyword (removed on Android and iOS only)
DefaultSearchProviderNewTabURL	Default search provider new tab page URL (removed on Android and iOS only)

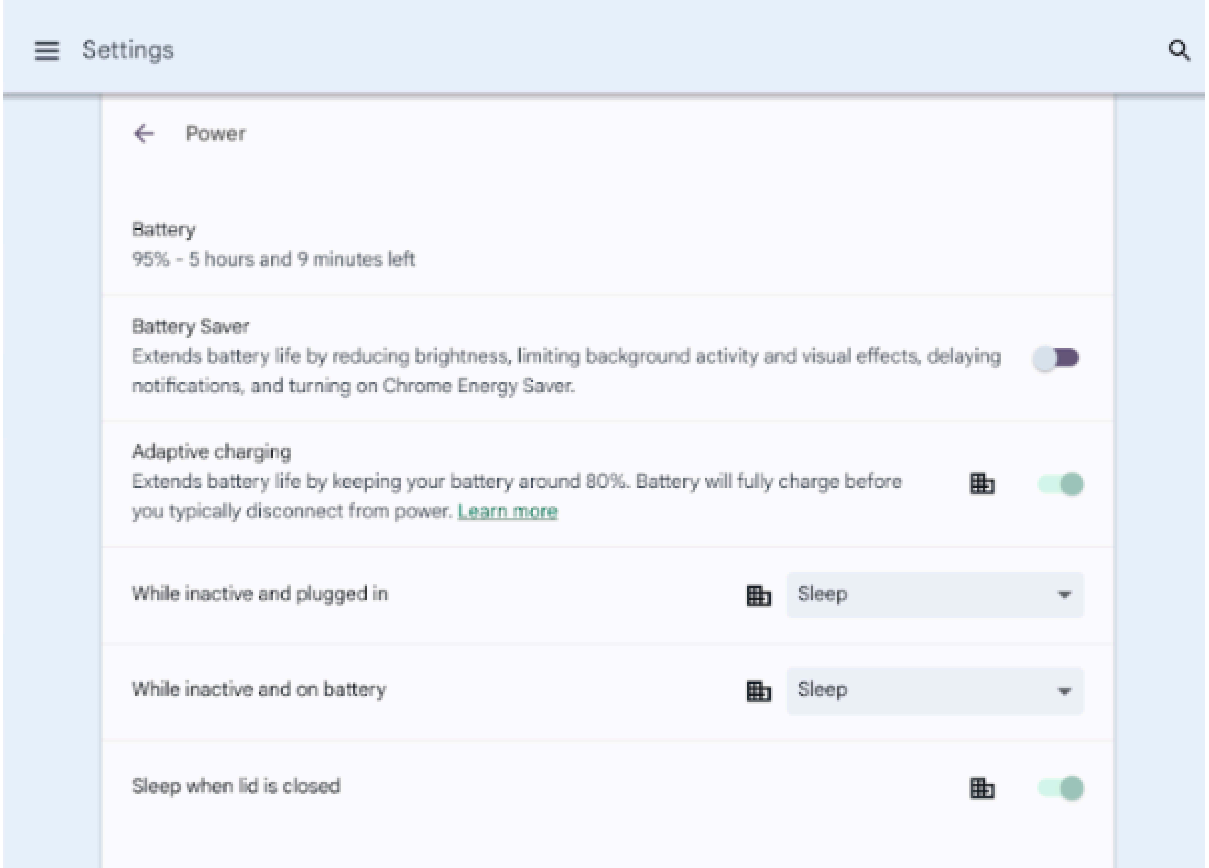
ChromeOS updates

Content scanning with BCE

ChromeOS data controls are a set of controls that are applied by the admin, which protect users from data leakage on endpoints using a Data Loss Prevention (DLP) layer in ChromeOS. For details, see this help center article. BeyondCorp Enterprise (BCE) enables continuous and real-time end-to-end protection. Content scanning with BCE is a new way to evaluate and enforce data controls restrictions on file transfers based on signals from BeyondCorp Enterprise.

Battery Saver

As early as ChromeOS 122, **Battery Saver** is available to reduce brightness on both display and keyboard backlight, throttle display refresh rate and available compute budget, and also turn off certain energy-intensive background functions to allow users squeeze more battery life out of their devices. This helps when users need that last couple minutes to finish a task and don't have a charger handy. When enabled, **Battery Saver** switches on automatically when the user's battery level reaches 20%. You can control this feature using the BatterySaverModeAvailability enterprise policy.



Settings

Power

Battery

95% - 5 hours and 9 minutes left

Battery Saver

Extends battery life by reducing brightness, limiting background activity and visual effects, delaying notifications, and turning on Chrome Energy Saver.

Adaptive charging

Extends battery life by keeping your battery around 80%. Battery will fully charge before you typically disconnect from power. Learn more

While inactive and plugged in: Sleep

While inactive and on battery: Sleep

Sleep when lid is closed

Enhanced SAML reauthentication flows

To optimize the sign-on experience of our customers, we've introduced certain internal changes to our SAML single sign-on implementation. These changes will impact customers with misconfigured SAML settings.

In particular if you set the policy LoginAuthenticationBehavior to *Redirect to SAML IdP by default*, ensure that the Single Sign-on policy is set to *Enable SAML*, otherwise your SAML-based IdP won't be loaded anymore.

Badge-based authentication

From ChromeOS 122, certain third-party Identity Management Providers (IdPs) can use badge authentication on ChromeOS devices. Users can simply start a session with a badge tap, and leave the session with another badge tap. The solution is focused on frontline workers in various industries including retail, hospitality, and manufacturing.

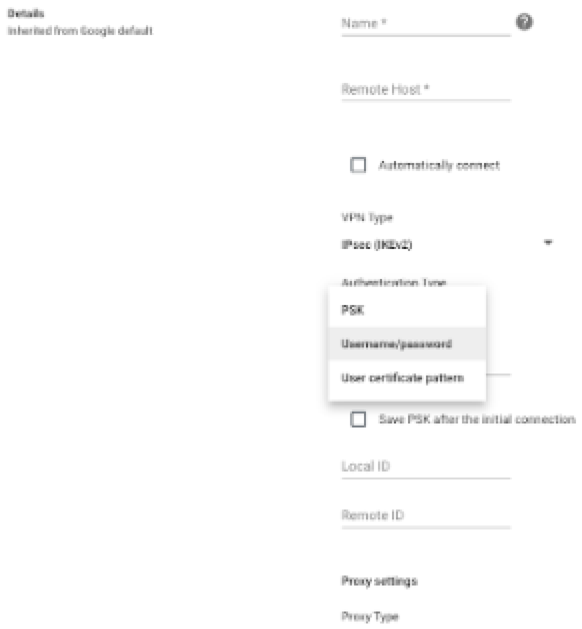
In ChromeOS 122, we are starting with the Ilex Card Management System, but we aim to add additional reader and authentication partners in the upcoming months. If you want to learn more, see Set up badge-based authentication.

Edit your recordings with Screencast

With ChromeOS Screencast, users can create and share transcribed screen recordings. As early as ChromeOS 122, users can trim their screencasts sentence-by-sentence, add and remove paragraph breaks, mute segments of their recordings, and title sections to make long recordings easier to navigate.

IKEv2 VPN support

ChromeOS 122 includes new options in the **Admin console** for Internet Key Exchange Protocol Version 2 (IKEv2) VPN protocol.



Details
Inherited from Google default

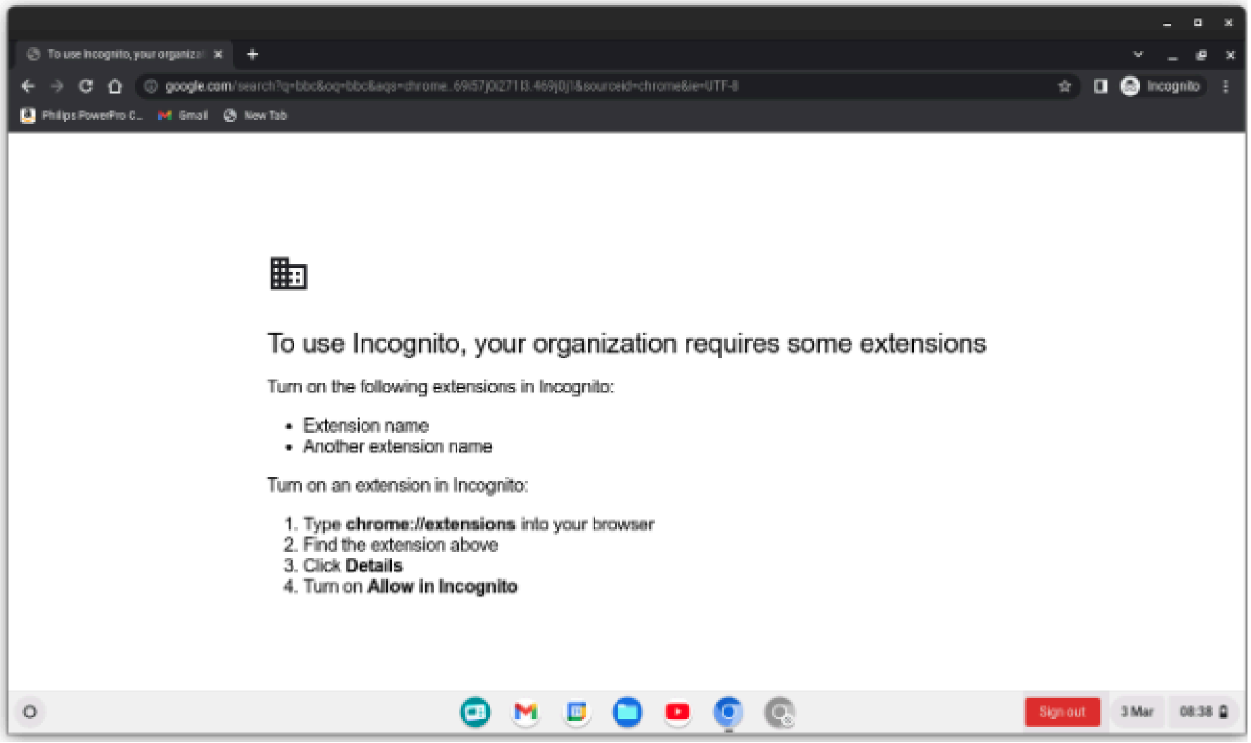
☐ Automatically connect

VPN Type
IPsec (IKEv2)

☐ Save PSK after the initial connection

Mandatory extensions in Incognito

Admins can now specify if there are certain extensions that users must turn on to use **Incognito** mode. There is a new toggle in **Admin console > Apps & extensions** that can be applied for individual extensions. This allows enterprises that have debugging or multi-account use cases that rely on **Incognito** mode to safely leave it enabled across their managed fleet. If they want to use **Incognito** mode, users need to turn on **Allow in Incognito** for all required enterprise extensions..


To use Incognito, your organizat
google.com/search?q=bbc&oq=bbc&aqs=chrome..69i57j0i271l3.469j0j1&sourceid=chrome&ie=UTF-8
Incognito
Philips PowerPro C...
Gmail
New Tab
Sign out
3 Mar
08:38

To use Incognito, your organization requires some extensions

Turn on the following extensions in Incognito:

- Extension name
- Another extension name

Turn on an extension in Incognito:

1. Type **chrome://extensions** into your browser
2. Find the extension above
3. Click **Details**
4. Turn on **Allow in Incognito**

New look for ChromeOS media player

ChromeOS media player will soon have bigger buttons and colors to match your wallpaper. The media player will appear when you are playing any video or audio (like Spotify or YouTube) in Quick Settings. You will be able to click the pin icon to move the media player to the shelf. In addition to controlling media that is being cast, you will be able to start casting web media to any speakers or screens on your local network.

Admin console updates

Inactive browser deletion in Chrome Browser Cloud Management

As early as March 2024, the **Inactive period for browser deletion policy** will automatically delete browser data in the Admin console for managed browsers that have not contacted the server for more than the inactivity period of time determined by the policy. When releasing the policy, the inactivity period of time will have a default value of 540 days. All enrolled browsers that have been inactive for more than 540 days will be deleted from your account shortly after the release of this policy. Administrators can change the inactive period value using this policy. The maximum value to determine the browser inactivity period will be 730 days and the minimum value is 28 days.

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

- **As early as March 2024:** The Inactive period for browser deletion policy UI will be available for early access in the Admin console. For IT admins who find the 18 month default inadequate, this will allow them to explicitly set a policy value (inactivity period of time) a few weeks before the actual deletion starts.

New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
AlwaysOnVpnPreConnectUrlAllowlist	User/MGS	ChromeOS 122+	Network
DeviceSwitchFunctionKeysBehaviorEnabled	Device	ChromeOS 122+	Other settings

MicrosoftOneDriveAccountRestrictions	User	ChromeOS 122+	Content
GoogleWorkspaceCloudUpload	User	ChromeOS 122+	Content
MicrosoftOfficeCloudUpload	User	ChromeOS 122+	Content
MicrosoftOneDriveMount	User	ChromeOS 122+	Content
QuickOfficeForceFileDownloadEnabled	User	ChromeOS 122+	Content
HelpMeWriteSettings	User	Chrome/ChromeOS 121+	Generative AI
CreateThemesSettings	User	Chrome/ChromeOS 121+	Generative AI
TabOrganizerSettings	User	Chrome/ChromeOS 121+	Generative AI

Coming soon

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

Upcoming Chrome browser changes

User link capturing on PWAs - Windows, MacOS and Linux

Web links automatically direct users to installed web apps. To better align with users' expectations around installed web apps, Chrome makes it more seamless to move between the browser and installed web apps. When the user clicks on 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. Clicking on the chip either launches the app directly, or opens a grid of apps that can support that link. For some users, clicking on a link always automatically opens the app.

- Chrome 121 on Linux, MacOS, Windows: When some users click on 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 123 on Linux, MacOS, Windows:** Based on the outcome of the experiment in Chrome 121, we will 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 user clicks on chip on address bar).

Resume tabs

Chrome 123 will introduce a new card on the **New tab** page, which will help users continue with tab suggestions from other devices. Using the NTPCardsVisible policy, admins will be available to control this feature.

- **Chrome 123 on ChromeOS, Linux, Mac, Windows**

Chrome on Android/iOS: cross-device resumption

To help users resume tasks originating from other devices, Chrome will provide cross-device tab suggestions on the **New tab** page or Home surfaces on Chrome on Android and Chrome on iOS. This component will be displayed within the existing continue browsing card on Start and the Magic Stack on Chrome on Android and Chrome on iOS.

- **Chrome 123 on Android, iOS:** Feature launches

Resume the last opened tab on any device

For the last open tab on any device within the last 24 hours with the same signed-in user profile, Chrome will offer users with a quick shortcut to resume that tab. Admins will be able to control this feature using an existing enterprise policy called SyncTypesListDisabled.

- **Chrome 123 on iOS:** Feature launches

Permissions prompt for Web MIDI API

The Web MIDI API connects to and interacts with Musical Instrument Digital Interface (MIDI) Devices. There have been several reported problems around Web MIDI API's drive-by access to client MIDI devices (see related Chromium bug). To address this problem, the W3C Audio Working Group decided to place an explicit permission on general Web MIDI API access. Originally, the explicit permission was only required for advanced Web MIDI usage in Chrome, including the ability to send and receive system exclusive (SysEx) messages, with gated access behind a permissions prompt. We now intend to expand the scope of the permission to regular Web MIDI API usage.

In Chrome 123, all access to the Web MIDI API will require a user permission. No policies will be available to control these changes. If you encounter any issues, file a bug here.

- **Chrome 123 on Windows, MacOS, Linux, Android**

Network Service on Windows will be sandboxed

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

- **Chrome 123 on Windows:** Network Service sandboxed on Windows

Chrome Sync ends support for Chrome 81 and earlier

Chrome Sync will no longer support Chrome 81 and earlier. You need to upgrade to a more recent version of Chrome if you want to continue using Chrome Sync.

- **Chrome 123 on Android, iOS, ChromeOS, Linux, MacOS, Windows:** The change will be implemented.

Deprecate and remove WebSQL

With SQLite over WASM as its official replacement, we plan to remove WebSQL entirely. This will help keep our users secure.

The Web SQL database standard was first proposed in April 2009 and abandoned in November 2010. Gecko never implemented this feature and WebKit deprecated this feature in 2019. The W3C encouraged those needing web databases to adopt Web Storage or Indexed Database.

Ever since its release, it has made it incredibly difficult to keep our users secure. SQLite was not initially designed to run malicious SQL statements, and yet with WebSQL we have to do exactly this. Having to react to a flow of stability and security issues is an unpredictable cost to the storage team.

- Chrome 101: In Chrome 101 the WebSQLAccess policy is added. WebSQL will be available when this policy is enabled, while the policy is available until Chrome 123.
- Chrome 115: Deprecation message added to console.
- Chrome 117: In Chrome 117 the WebSQL Deprecation Trial starts. The trial ends in Chrome 123. During the trial period, a deprecation trial token is needed for the feature to be available.
- Chrome 119: Starting Chrome 119, WebSQL is no longer available. Access to the feature is available until Chrome 123 using the WebSQLAccess policy, or a deprecation trial token.
- **Chrome 123: on ChromeOS, LaCrOS, Linux, MacOS, Windows, Android:** Starting in Chrome 123, the policy WebSQLAccess and the deprecation trial, which allows for WebSQL to be available, will no longer be available.

IdleTimeout and IdleTimeoutActions policies on iOS

Enterprises are now able to enforce taking an action after Chrome has been idle for some amount of time on iOS devices. Admins can use the IdleTimeout policy to set a timeout period and the IdleTimeoutActions policy to specify actions on timeout. The setting will be available as a platform policy and will be available per profile at a future date.

- **Chrome 123 on iOS:** policies available on iOS

Cross-profile password reuse detection

Previously, password reuse detection of corporate credentials was only detectable in the corporate profile. In Chrome 123, password reuse detection will detect corporate credential reuse across all non-Incognito profiles on the managed browser.

- **Chrome 123:** feature rolls out

Telemetry for permission prompts and accepting notification permissions

When Enhanced Protection is turned on, and a user visits a page that prompts the user to accept a notification permission, attributes of that page might be sent to Safe Browsing. If the telemetry is sent and the page is deemed dangerous, users will see a Safe Browsing warning.

When Enhanced Protection or Safe Browsing Extended Reporting is turned on, and a user accepts a notification permission for a blocklisted page, this event will be sent to Safe Browsing.

These features can be controlled by the SafeBrowsingProtectionLevel and SafeBrowsingExtendedReportingEnabled policies.

- **Chrome 123 on Android, ChromeOS, LaCrOS, Linux, Mac, Windows, Fuchsia**

ServiceWorker static routing API

This API allows developers to configure the routing, and allows them to offload simple things ServiceWorkers do. If the condition matches, the navigation happens without starting ServiceWorkers or executing JavaScript, which allows web pages to avoid performance penalties due to ServiceWorker interceptions.

- **Chrome 123 on Windows, Mac, Linux, Android**

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

Before a website navigates to a destination site in a user's private network, Chrome will do the following:

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

The above checks are made to protect the user's private network. Since this feature operates in *warning-only* mode, we do not fail the requests if any of the checks fail. Instead, a warning will be shown in DevTools Chrome console, to help developers prepare for the coming enforcement. To read about these changes, see Private Network Access (PNA) for Navigation Requests. To learn more, see the PNA specification.

- **Chrome 123 on Android (except for WebView), ChromeOS, Linux, MacOS, Windows**

Bookmarks and reading list improvements on Android

On Chrome 124 on Android, some users who sign in to Chrome from the bookmark manager will be able to use and save bookmarks and reading list items in their Google Account. Relevant enterprise policies, such as BrowserSignin, SyncTypesListDisabled, EditBookmarksEnabled, ManagedBookmarks and ShoppingListEnabled will continue to work as before, to configure whether users can use and save items in their Google Account.

- **Chrome 124 on Android:** Feature rolls out

Deprecate enterprise policy ThrottleNonVisibleCrossOriginIframesAllowed

The underlying code change (throttling same-process, cross-origin display:none iframes) that the ThrottleNonVisibleCrossOriginIframesAllowed enterprise policy overrides has been enabled in stable releases since early 2023. Since known issues have been dealt with, we intend to remove the ThrottleNonVisibleCrossOriginIframesAllowed enterprise policy by

Chrome 124. The discussions around the throttling issue (and its resolution) can be found at https://bugs.chromium.org/p/chromium/issues/detail?id=958475.

- **Chrome 124:** Policy is removed

Remove support for UserAgentClientHintsGREASEUpdateEnabled

We plan to deprecate the UserAgentClientHintsGREASEUpdateEnabled policy since the updated GREASE algorithm has been on by default for over a year. The policy will eventually be removed.

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

Intent to 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.

- **Chrome 127 on Android, ChromeOS, Linux, MacOS, Windows:** Mutation Events will stop functioning in Chrome 127, around July 30, 2024.

Remove LegacySameSiteCookieBehaviorEnabledForDomainList policy

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

- **Chrome 128 on Android, ChromeOS, Linux, MacOS, Windows:** Remove LegacySameSiteCookieBehaviorEnabledForDomainList policy

Extensions must be updated to leverage Manifest V3 by June 2025

Extensions must be updated to leverage Manifest V3. Chrome extensions are transitioning to a new manifest version, Manifest V3. This will bring improved privacy for your users—for example, by moving to a model where extensions modify requests declaratively, without the ability to see individual requests. This also improves extension security, as remotely hosted code will be disallowed on Manifest V3.

Beginning June 2024, Chrome will gradually disable Manifest V2 extensions running in the browser. An Enterprise policy - ExtensionManifestV2Availability - is available to control whether Manifest v2 extensions are allowed. The policy 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 Browser Cloud Management. Read more on the Manifest timeline, including:

- Chrome 110 on ChromeOS, LaCrOS, Linux, MacOS, Windows: Enterprise policy ExtensionManifestV2Availability is available to control whether Manifest v2 extensions are allowed. The policy can be used to test Manifest V3 in your organization ahead of the migration. After the migration the policy will allow you to extend the usage of Manifest V2 extensions.
- **Chrome 127 on ChromeOS, LaCrOS, Linux, MacOS, Windows:** Chrome will gradually disable Manifest V2 extensions on user devices. Only those with the ExtensionManifestV2Availability enterprise policy enabled would be able to continue using Manifest V2 extensions in their organization.
  - Chrome 139 on ChromeOS, LaCrOS, Linux, MacOS, Windows: Remove ExtensionManifestV2Availability policy.

Upcoming ChromeOS changes

ChromeOS Flex Bluetooth migration

In ChromeOS 123, ChromeOS Flex will upgrade to the Floss Bluetooth stack. As part of this upgrade, the listed devices no longer support Bluetooth functionality. If Bluetooth functionality is critical for these devices, we recommend moving these devices to the LTS channel to extend the Bluetooth functionality through to October 2024.

- HP Probook 4530s
- Lenovo ThinkPad T420
- HP Elitebook 8460p
- Apple iMac 11,2
- Lenovo ThinkPad x220
- Dell Vostro 3550
- HP 3115m
- HP Elitebook 2560p
- HP ProBook 6465b
- Lenovo ThinkPad L420

If your devices are unable to connect to Bluetooth after updating to ChromeOS 123, switch the Chrome flag **Use Floss instead of BlueZ** to *Disabled*. □□

Customizing keyboard shortcuts

Using shortcuts boosts productivity, and we all have our favorites. As early as ChromeOS 123, with shortcut customization, you will be able to assign your preferred key combination to personalize your shortcuts. Whether you want them to be easier to do with one hand, simpler to remember, or identical to the ones you're familiar with, this feature will simplify your day-to-day workflows.

Record GIFs with Screen capture

As early as ChromeOS 124, **Screen capture** will let you record your screen in .GIF format to easily capture, share, and play the recording inline in chat, slides, docs, and more.

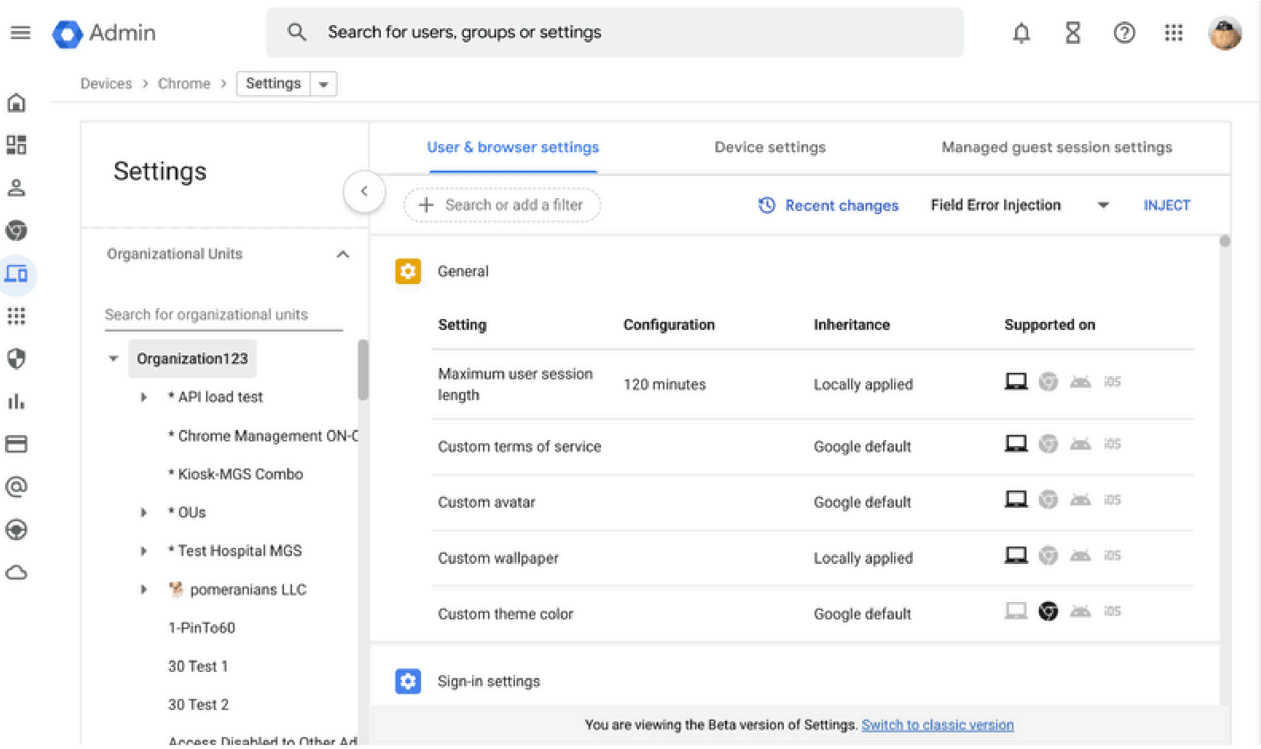
Faster Split Screen setup

Chromebooks provide a variety of ways to arrange the windows on your screen to help make you more productive — one of which is Split Screen. Just as it sounds, Faster Split Screen Setup will offer a quicker way to set up your window layout by showing an overview of your open windows on the other side of the screen. With Faster Split Screen, once you "snap" (or lock) a window in place on one side, you can choose an already-open window from Overview to snap into the other side, or select something from the shelf (the row of apps located at the bottom or side of your screen).

Upcoming Admin Console changes

Enhanced Settings page experience

Starting in March 2024, all admins will use our updated **Settings** page experience–that means you'll no longer be able to use the legacy **Settings** page experience. Most of you already use the updated experience. This just means that admins will no longer be able to access the legacy view, but you'll still have access to all the same functionality in the updated view.



Setting	Configuration	Inheritance	Supported on
Maximum user session length	120 minutes	Locally applied	iOS
Custom terms of service		Google default	iOS
Custom avatar		Google default	iOS
Custom wallpaper		Locally applied	iOS
Custom theme color		Google default	iOS

You are viewing the Beta version of Settings. Switch to classic version

Chrome crash report

As early as Chrome 123, you will be able to visualize crash events in the Admin console using the new Chrome crash report page. In this report, you will find a dynamic chart representing Chrome crash events over time, grouped by versions of Chrome. Additional filtering is available for the following fields: OS platforms, Chrome channels and dates. This report will help you proactively identify potential Chrome issues within your organization.

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

- Chrome 121 on Linux, MacOS, Windows: Trusted Tester program
- **Chrome 123 on Linux, MacOS, Windows:** Feature rolls out

Legacy Technology report

As early as Chrome 123, the Legacy Technology report will be available in the Admin console and it will proactively report websites (both internal and external) that are using technology that will be deprecated, for example, third-party cookies, SameSite cookie changes, and older security protocols like TLS 1.0/1.1 and third-party cookies. This information will enable IT administrators to work with developers to plan required tech migrations before the deprecation feature removals goes into effect.

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

- **As early as Chrome 123 on Linux, MacOS, Windows**

Previous release notes

Chrome version & targeted Stable channel release date	PDF
Chrome 121: January 17, 2023	PDF
Chrome 120: November 29, 2023	PDF
Chrome 119: October 25, 2023	PDF
Chrome 118: October 04, 2023	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