chrome enterprise

Chrome 121 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 January 17, 2024.

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

Chrome 121 release summary

Chrome Browser updates	**Security/Privacy**	**User productivity/Apps**	**Management**
Chrome Third-Party Cookie Deprecation (3PCD)	✓		
Rename FirstPartySets Enterprise Policies to RelatedWebsiteSets	✓		✓
Generative AI features		✓	
Safer encrypted archives for Standard Safe Browsing users	✓		
User Link Capturing on PWAs - Windows, MacOS and Linux	✓		
Side Panel Navigation: Pinning or unpinning		✓	
Autofill: display in server cards and local cards	✓		
Autofill: changes in card verification	✓		
CSS Highlight Inheritance	✓		
Chrome user policies for iOS			✓
Skip unload events	✓		
New and updated policies in Chrome browser			✓
Removed policies in Chrome browser			✓
ChromeOS updates	**Security/Privacy**	**User productivity/Apps**	**Management**
ChromeOS Flex End of Device Support			✓
Enable dictation using the keyboard		✓	
ChromeVox Accessibility service		✓	

No more onboarding messages for Assistant		✓	
New trackpad gesture on ChromeOS		✓	
Integrate the DLP events rule Id and name into the security investigation tool	✓		
Enterprise DataControls (DLP) file restrictions	✓		
Borderless printing		✓	
Admin Console Updates	**Security/Privacy**	**User productivity/Apps**	**Management**
Configure IP address on device with Ethernet adapter	✓		✓
Apps & Extensions usage report: Highlight extensions removed from the Chrome Web Store			✓
Chrome crash report			✓
Fix for certain Android WiFi certificates			✓
New policies in the Admin console			✓
Upcoming Chrome Browser updates	**Security/Privacy**	**User productivity/Apps**	**Management**
Default Search Engine choice screen		✓	
Simplified sign-in and sync experience		✓	✓
Permissions prompt for Web MIDI API	✓		
SharedImages for PPAPI Video Decode	✓		
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	✓		
Resume the last opened tab on any device		✓	
Chrome Sync ends support for Chrome 81 and earlier	✓		✓
Deprecate and remove WebSQL	✓		
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 productivity/Apps**	**Management**
ChromeOS Flex Bluetooth Migration			✓
New look for ChromeOS media player		✓	
App disablement by Admin in MGS			✓
Battery Saver		✓	

Upcoming Admin Console Updates	**Security/Privacy**	**User productivity/Apps**	**Management**
Inactive browser deletion in Chrome Browser Cloud Management			✓
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 121 restricts third-party cookies by default for 1% of Chrome users to facilitate testing, and plans to ramp up to 100% of users from 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 will also see new Tracking Protection user controls. You can try out these changes in Chrome 121 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 should be 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 their managed browsers ahead of the experiment. This gives enterprises time to make the changes required to not rely on this policy or 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 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.

Rename FirstPartySets policies to RelatedWebsiteSets

The FirstPartySetsEnabled and FirstPartySetsOverrides enterprise policies are renamed to RelatedWebsiteSetsEnabled and RelatedWebsiteSetsOverrides respectively. There is no change in policy behavior. Administrators should use the new policies RelatedWebsiteSetsEnabled and RelatedWebsiteSetsOverrides going forward. To learn more about the rename, follow https://developer.chrome.com/blog/related-website-sets/

Generative AI features

Starting in Chrome 121, Chrome launches a number of new Generative AI (GenAI) features to signed-in users, in the US only. Users can opt in using a new option on the `chrome://settings` page. These features are initially available to unmanaged users only,

and are inaccessible to managed Chrome Enterprise & Education users in this release. We expect to relax this restriction in the near future.
New policies will be available over the next few releases to control these features. In the coming weeks, we will provide more details about the new GenAI features in Chrome.

- **Chrome 121 on ChromeOS, Linux, Mac, Windows:** signed-in unmanaged users in the US can opt in
- Earliest Chrome 122 on ChromeOS, Linux, Mac, Windows: signed-in Chrome Enterprise & Education users in the US can opt in and policies will be available

Safer encrypted archives for Standard Safe Browsing users

On some encrypted archive downloads, Chrome prompts Standard Safe Browsing users for a password (not shared with Google and cleared after retrieving the metadata). This collects more metadata about the download (such as contained file hashes and executable signatures), which is sent to Google for better quality verdicts. The password remains local and not shared with Google. You can control this feature with the SafeBrowsingDeepScanningEnabled policy.

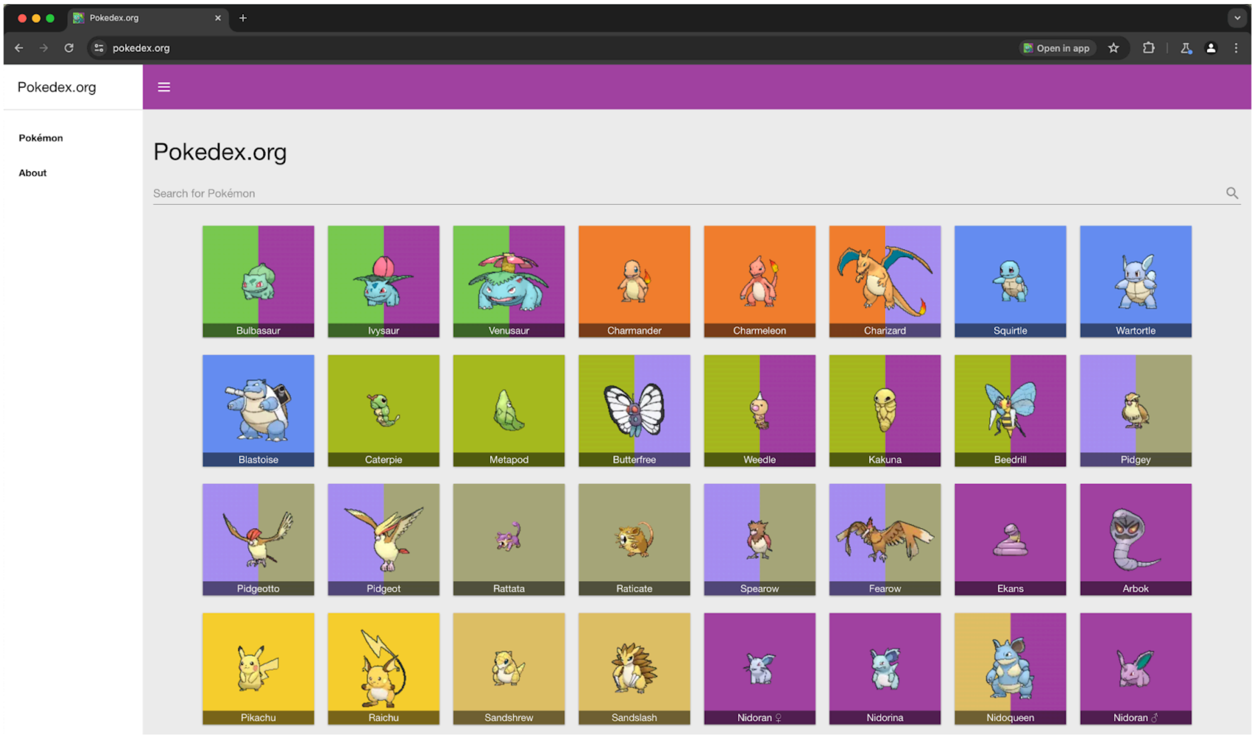
- **Chrome 121 on Linux, MacOS, Windows**

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`.

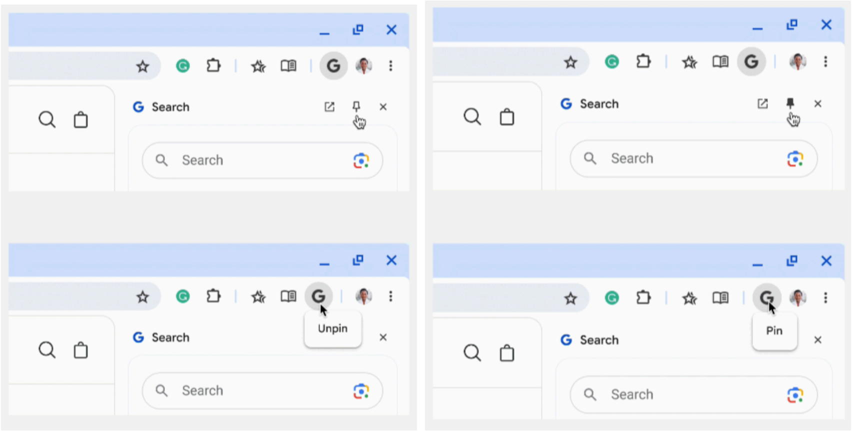
- Chrome 123 on Linux, MacOS, Windows: Based on the outcome of the experiment in Chrome 121, we will launch to 100% of Stable with either a default on (always launch apps on link clicks) or a default off (always open in a tab, only launch if user clicks on chip on address bar).



Side Panel Navigation: Pinning or unpinning

As early as Chrome 121, Chrome removes the side panel icon in favor of evolving the side panel navigation to offer customization through toolbar pinning. This allows for efficient direct access to a suite of panels. You can open most side panel features through the Chrome menu (⋮).

- **Chrome 121 on Chrome OS, LaCrOS, Linux, MacOS, Windows, Fuchsia**



Autofill: display in server cards and local cards

Autofill helps users seamlessly fill out their card information into payment forms. Credit or debit cards, which can be autofilled, are stored on the Chrome client. There are 2 types: Server cards and Local cards. A server card only has the last 4 digits and the expiry date of the card whereas a local card has all the digits of a card along with the expiry date.

There are instances when a local and server card of the same card exist on the same client. When that happens, Chrome typically dedupes the server card and only offers the local card for autofilling. With this change, the opposite is true, and server card usage is now offered to users instead. This brings the security and usability benefits of GPay server cards to users with duplicate cards, as well as makes the experience more consistent across devices.

- **Chrome 121 on Chrome OS, LaCrOS, Linux, MacOS, Windows, Fuchsia**

Autofill: security code updates

In Chrome 121, to improve user experience, payments autofill now unmasks card information using Google's industry leading verification methods instead of relying on security codes to verify and unmask cards. Users can choose to turn on device unlock if they want to add an extra layer of security for unmasking their card.

- **Chrome 121 on Android, MacOS**

CSS Highlight Inheritance

With CSS Highlight Inheritance, the CSS Highlight pseudo classes, such as `::selection` and `::highlight`, inherit their properties through the pseudo highlight chain, rather than the element chain. The result is a more intuitive model for inheritance of properties in highlights. Specifically, when any supported property is not given a value by the cascade, its specified value is determined by inheritance from the corresponding highlight pseudo-element of its originating element's parent element. For more details, see the Highlight Pseudo-elements specification.

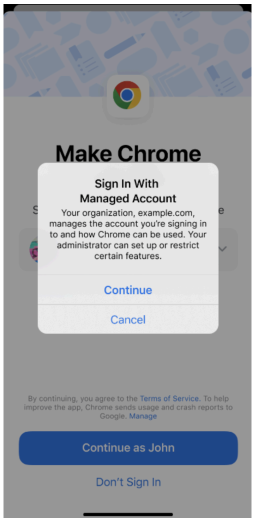
- **Chrome 121 on Windows, MacOS, Linux, Android**

Chrome user policies for iOS

With Chrome user policies for iOS, admins can apply policies and preferences across a user's devices. Settings apply whenever the user signs in to Chrome browser with their managed account on any device, including personal devices.

In Chrome 120, we began rollout but rolled back due to a non-impacting bug. Starting in Chrome 121, managed end-users start to see a management notice stating that their organization manages the account they are signing into. Admins can turn on this functionality in the Admin console under the **Chrome on iOS** setting. For more information, see Set Chrome policies for users or browsers.

- Chrome 120 on iOS: Started rollout to 5%, rolled back due to non-impacting bug
- **Chrome 121 on iOS:** Begin gradual rollout, targeting 100% by M122

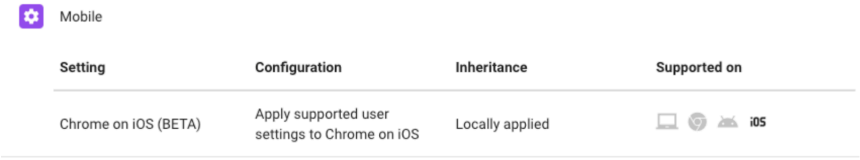


Make Chrome

Sign In With Managed Account

Your organization, example.com, manages the account you're signing in to and how Chrome can be used. Your administrator can set up or restrict certain features.

By continuing, you agree to the Terms of Service. To help improve the app, Chrome sends usage and crash reports to Google. Manage



Mobile

Setting	Configuration	Inheritance	Supported on
Chrome on iOS (BETA)	Apply supported user settings to Chrome on iOS	Locally applied	iOS

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 Chrome OS, Linux, MacOS, Windows: Dev Trial
- Chrome 119 on Chrome OS, Linux, MacOS, Windows: Introduces ForcePermissionPolicyUnloadDefaultEnabled policy
- **Chrome 121 -131 on Chrome OS, Linux, MacOS, Windows:** Deprecation trial (general rollout of deprecation will be limited scope until deprecation trial is ready)

New and updated policies in Chrome browser

Policy	Description
AllowChromeDataInBackups	Allow backup of Google Chrome data
CloudUserPolicyMerge	Enables merging of user cloud policies into machine-level policies (now available on iOS)
ProfileReauthPrompt	Prompt users to re-authenticate to the profile

Removed policies in Chrome browser

Policy	Description
ChromeRootStoreEnabled	Determines whether the Chrome Root Store and built-in certificate verifier will be used to verify server certificates
ContextAwareAccessSignalsAllowlist	Enable the Chrome Enterprise Device Trust Connector attestation flow for a list of URLs
WebRtcAllowLegacyTLSProtocols	Allow legacy TLS/DTLS downgrade in WebRTC
OffsetParentNewSpecBehaviorEnabled	Control the new behavior of HTMLElement.offsetParent
SendMouseEventsDisabledFormControlsEnabled	Control the new behavior for event dispatching on disabled form controls
AttestationEnabledForDevice	Enable remote attestation for the device

ChromeOS updates

ChromeOS Flex End of Device Support

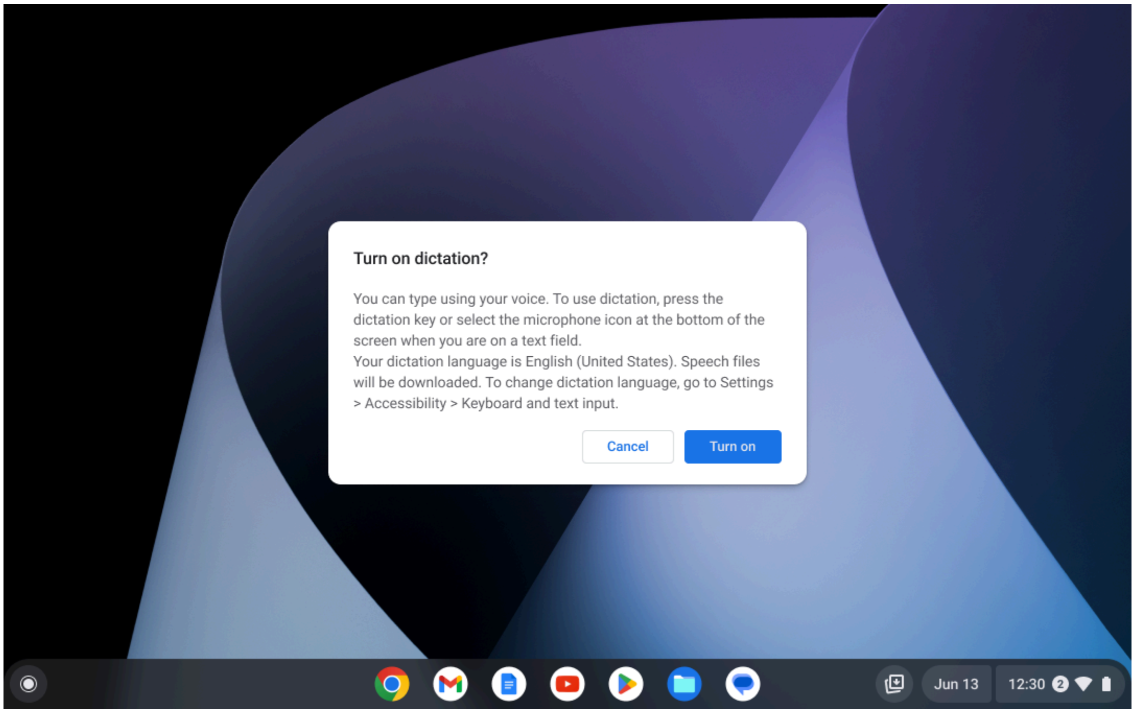
As of January 01, 2024, devices scheduled to end support in 2023 will no longer be supported. Decertified devices include those listed below; for the full list of devices ending support you can review our Certified models list.

- HP Compaq 6005 Pro
- HP Compaq Elite 8100
- Lenovo ThinkCentre M77
- HP ProBook 6550b
- HP 630
- Dell Optiplex 980

The devices will continue to receive ChromeOS Flex updates but these updates will no longer be tested or maintained by the Flex team. We recommend that customers upgrade to newer ChromeOS Flex certified models or ChromeOS devices to benefit from new features and security improvements. You can learn more about supported devices in our help center.

Enable dictation using the keyboard

Logitech keyboards with a dictation button and other keyboards using the Search + D shortcut now turn on the Dictation accessibility feature if it is off. If Dictation is already on, then the key (and the shortcut) will activate Dictation. When enabling dictation, a dialog will appear to inform users they are about to enable Dictation, certain speech files might be downloaded and how to use the dictation feature once it is enabled.



Turn on dictation?

You can type using your voice. To use dictation, press the dictation key or select the microphone icon at the bottom of the screen when you are on a text field.
Your dictation language is English (United States). Speech files will be downloaded. To change dictation language, go to Settings > Accessibility > Keyboard and text input.

ChromeVox Accessibility service

Users of App Streaming on Chromebooks will now be able to use ChromeVox to navigate the streaming Android app. The streaming Android app's accessibility tree is streamed in tandem with the app itself and can be interacted with using ChromeOS screen reader capabilities.

No more onboarding messages for Assistant

ChromeOS 121 removes the welcome or onboarding messages offered to a new user when launching **Assistant** on ChromeOS for the first time. This is a deprecation.

New trackpad gesture on ChromeOS

ChromeOS 121 launches a new trackpad gesture to help users dismiss notification popups in the notification center.

Integrate the DLP events rule Id and name into the security investigation tool

ChromeOS Data Control events will have additional fields to enrich admin insights in the security investigation tool.

Enterprise DataControls (DLP) file restrictions

In ChromeOS 121, ChromeOS Data Controls enable IT and Security teams to protect important business and customer data. It is available for events like copy and paste, screen capture, screen sharing, and printing. IT administrators can create an information protection strategy with rules based on the data source, destination and user.
We now have new functionality to control what users can do with files on ChromeOS devices through source and destination based rules.

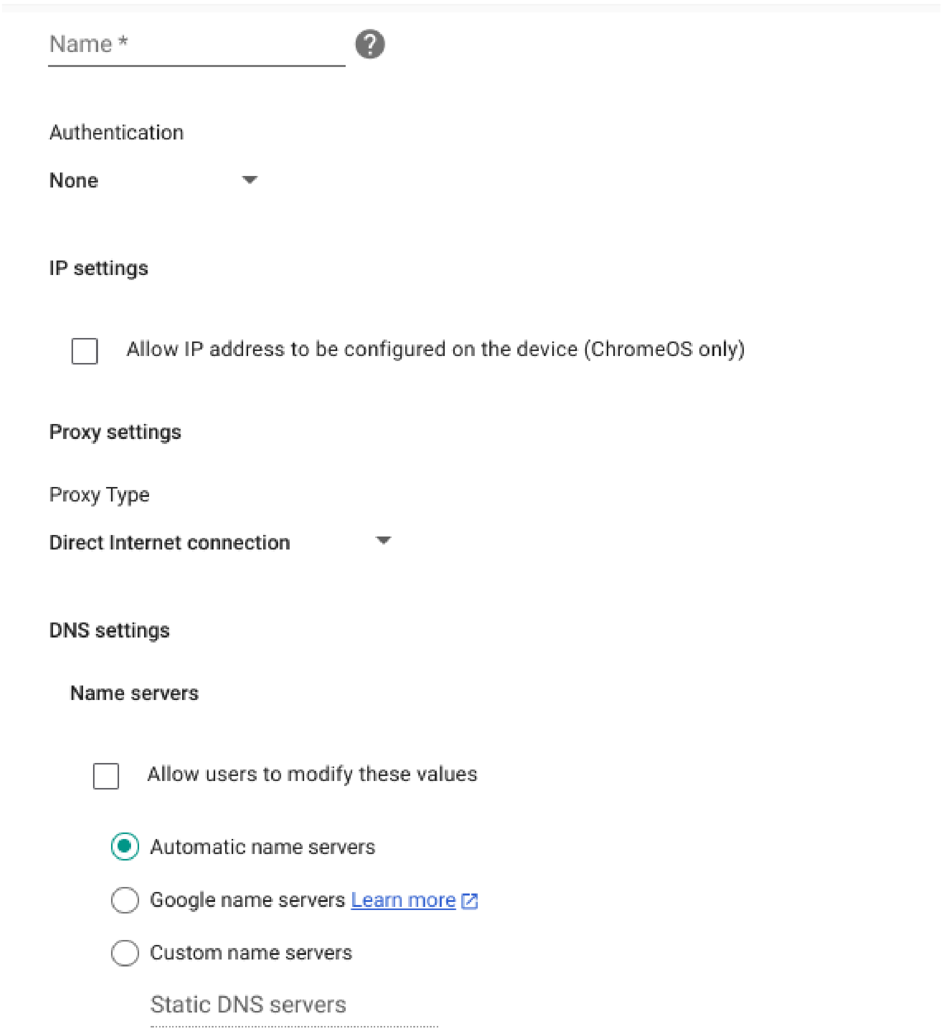
Borderless printing

ChromeOS now supports borderless printing. With a compatible printer, you can now print photographs on photograph paper, without borders.

Admin console updates

Configure IP address on device with Ethernet adapter

The Admin console setting **Allow IP address to be configured on the device (ChromeOS only)** and **Allow users to modify these values** (in **DNS settings**) is now also respected for Ethernet adapters.



Name *

Authentication

None

IP settings

□ Allow IP address to be configured on the device (ChromeOS only)

Proxy settings

Proxy Type

Direct Internet connection

DNS settings

Name servers

□ Allow users to modify these values

● Automatic name servers

○ Google name servers Learn more

○ Custom name servers

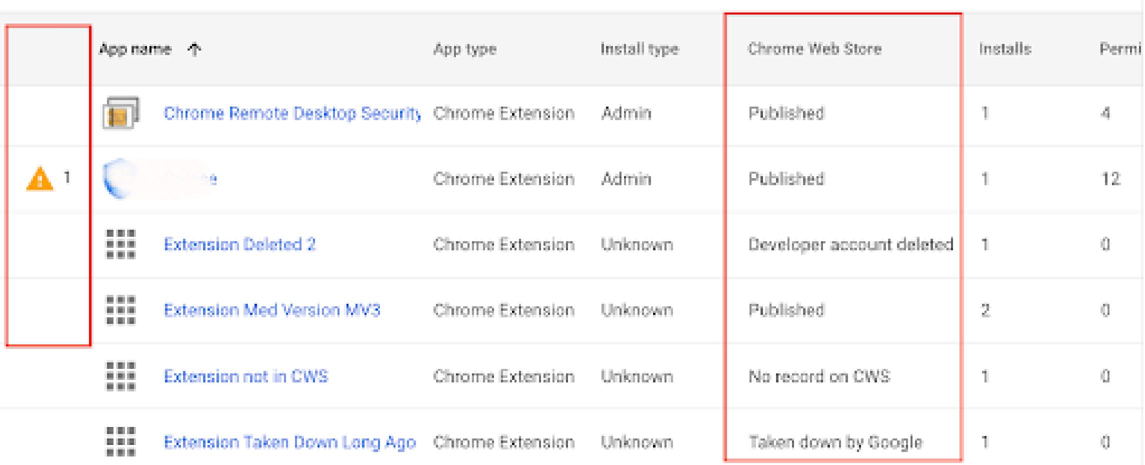
Static DNS servers

Apps & Extensions usage report: Highlight extensions removed from the Chrome Web Store

In Chrome 121, new information on the Apps & Extensions usage report is available to help you identify if an extension was recently removed from the Chrome Web Store via a new notifications column and a new **Chrome Web Store** column that represents the listing status of an extension. On the **App Details** page, you can find the reason why an extension was removed from the Chrome Web Store. This feature will help IT administrators identify the impact of using the policy to disable unpublished extensions.

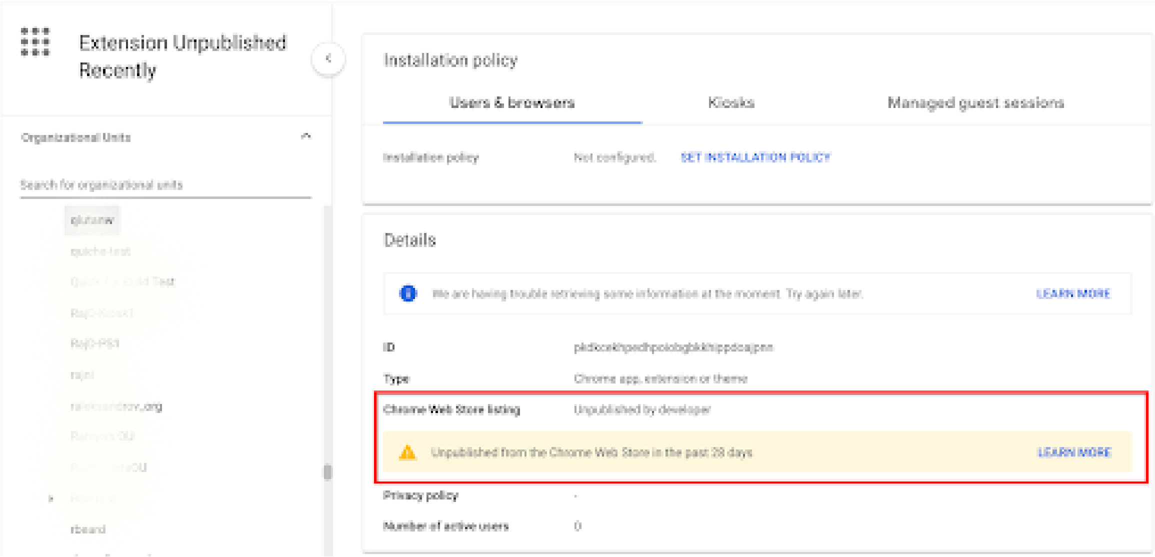
- Chrome 120 on Linux, MacOS, Windows: Trusted Tester program
- **Chrome 121 on Linux, MacOS, Windows: Feature rolls out**

Apps & Extensions usage report:



	App name ↑	App type	Install type	Chrome Web Store	Installs	Permi
	Chrome Remote Desktop Security	Chrome Extension	Admin	Published	1	4
⚠ 1	[illegible]	Chrome Extension	Admin	Published	1	12
	Extension Deleted 2	Chrome Extension	Unknown	Developer account deleted	1	0
	Extension Med Version MV3	Chrome Extension	Unknown	Published	2	0
	Extension not in CWS	Chrome Extension	Unknown	No record on CWS	1	0
	Extension Taken Down Long Ago	Chrome Extension	Unknown	Taken down by Google	1	0

App Details page:



Extension Unpublished Recently
Organizational Units
Search for organizational units
gluzarw
quiche-test
RajD-PS1
rajnl
rbeard

Installation policy

Installation policy Not configured. SET INSTALLATION POLICY

Details

We are having trouble retrieving some information at the moment. Try again later. LEARN MORE

ID	pkdkcekhpedhpolobgbkkhippdcajpnn
Type	Chrome app, extension or theme
Chrome Web Store listing	Unpublished by developer

⚠ Unpublished from the Chrome Web Store in the past 28 days LEARN MORE

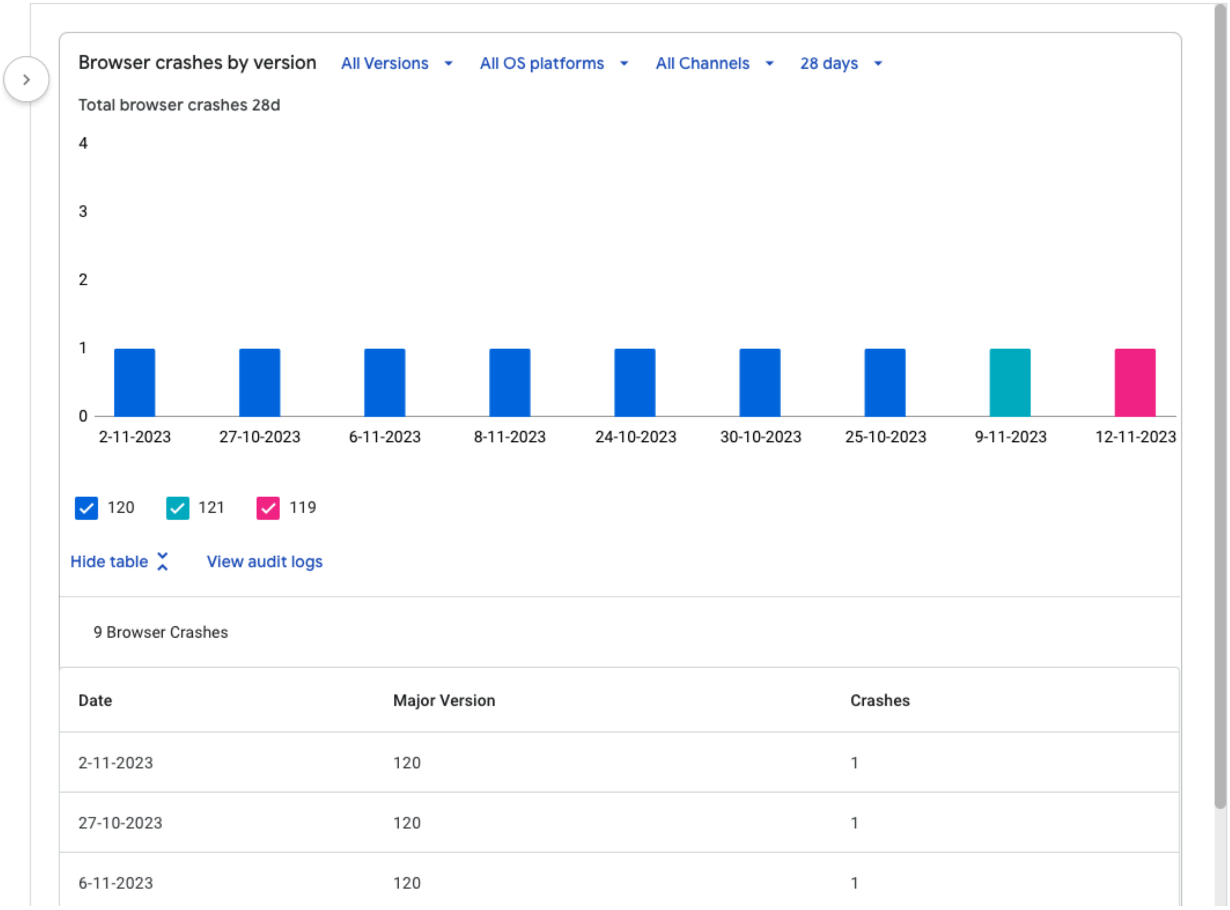
Privacy policy	-
Number of active users	0

Chrome crash report

As early as Chrome 122, 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 122 on Linux, MacOS, Windows: Feature rolls out

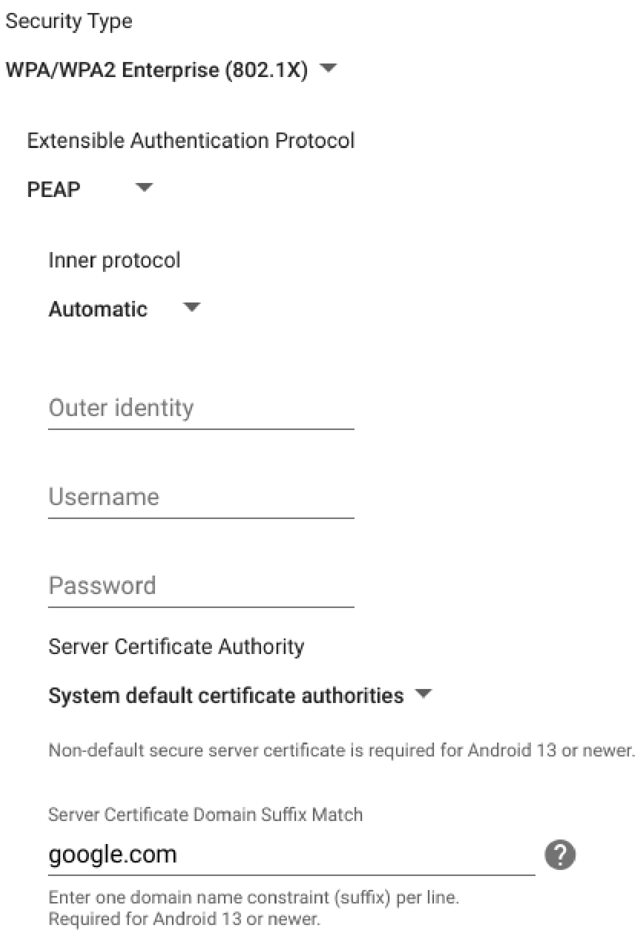


9 Browser Crashes

Date	Major Version	Crashes
2-11-2023	120	1
27-10-2023	120	1
6-11-2023	120	1

Fix for certain Android WiFi certificates (early Feb 2024)

Required as of Android 13, for certain WiFi configurations using enterprise authentication (802.1X), a new required field, called `DomainSuffixMatch`, was added for additional security. Before updating your fleet to Android 13, you need to edit the new field of that network's settings, **Server Certificate Authority**, to add at least one **Server Certificate Domain Suffix Match**. The device will only connect to the WiFi network if the server certificate presented by the remote end has a Subject CommonName or DNS Name SubjectAlternativeName (SAN) that matches the provided suffix.



Security Type

WPA/WPA2 Enterprise (802.1X)

Extensible Authentication Protocol

PEAP

Inner protocol

Automatic

Outer identity

Username

Password

Server Certificate Authority

System default certificate authorities

Non-default secure server certificate is required for Android 13 or newer.

Server Certificate Domain Suffix Match

google.com

Enter one domain name constraint (suffix) per line.
Required for Android 13 or newer.

New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
AllowChromeDataInBackups	User & Browser	Chrome (iOS)	Other Settings
OopPrintDriversAllowed	User & Browser	Chrome (Linux, MacOS, Windows)	Printing

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

Default Search Engine choice screen

Starting Chrome 120, enterprise end-users might be prompted to choose their default search engine within Chrome.
As part of our building for DMA compliance, some users will be prompted to choose their default search engine for Chrome. This prompt controls the default search engine setting, currently available at `chrome://settings/search`. The enterprise policies, DefaultSearchProviderEnabled and DefaultSearchProviderSearchUrl, will continue to control this setting as it does today, if it is set by the IT admin. Read more on this policy and the related atomic group.

- Chrome 120 on iOS, Chrome OS, LaCrOS, Linux, MacOS, Windows: 1% users might start getting the choice screen with Chrome 120.
- **Chrome 122 on iOS, Chrome OS, LaCrOS, Linux, MacOS, Windows: full roll-out for applicable users.**

Simplified sign-in and sync experience

Starting in Chrome 122, existing users with Chrome sync turned on will experience a simplified and consolidated version of sign-in and sync in Chrome. Chrome sync will no longer be shown as a separate feature in settings or elsewhere. Instead, users can sign in to Chrome to use and save information like passwords, bookmarks and more in their Google Account, subject to the relevant enterprise policies.

As before, the functionality previously part of Chrome sync that saves and accesses Chrome data in the Google Account can be 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: sunset Chrome sync for users who didn't have Chrome sync enabled at the time.
- **Chrome 122: sunset Chrome sync for users with Chrome sync enabled by migrating them to an equivalent state.**

Permissions prompt for Web MIDI API

There have been several reported problems around Web MIDI API's drive-by access to client MIDI devices (bugs). To address this problem, the Audio WG decided to place an explicit permission on the general MIDI API access. Originally, the explicit permission was only required for advanced MIDI usage (System Exclusive (SysEx) messages) in Chrome, with gated access behind a permissions prompt. We plan to expand the scope of the permission to regular MIDI API usage.

Today the use of SysEx messages with the Web MIDI API requires an explicit user permission. With this implementation, even access to the Web MIDI API without SysEx support will require a user permission. Three new policies—**DefaultMidiSetting, MidiAllowedForUrls and MidiBlockedForUrls**—will be available to allow administrators to pre-configure user access to the API.

- ○ **Chrome 122 on Windows, MacOS, Linux, Android**

SharedImages for PPAPI Video Decode

Chrome 119 introduces a new PPAPISharedImagesForVideoDecoderAllowed policy to control the recent refactor for VideoDecoder APIs in PPAPI plugin.

- Chrome 119 on ChromeOS, LaCrOS: Introduces escape hatch policy.

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

V8 security setting

Add a setting on `chrome://settings/security` to disable the V8 JIT optimizers, in order to reduce the attack surface of Chrome. 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 setting rolls out in Chrome 122. The enterprise policies have been available since Chrome 93.

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

Read aloud

Read aloud will allow users of Chrome on Android to listen to web pages via text to speech technology. Users will be able to access this feature via the overflow menu and control playback via audio controls.

Read aloud will send the page URL to Google servers to power playback, and users who use it will 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 will be enabled.

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

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 122 on Windows:** Network Service sandboxed on Windows

Removal of enterprise policy ChromeAppsWebViewPermissiveBehaviorAllowed

In Chrome 116, Chrome Apps webview usage have the following restrictions:
Using the webview NewWindow event to attach to a webview element in another App window causes the window reference returned by the window.open call in the originating webview to be invalidated. A temporary enterprise policy ChromeAppsWebViewPermissiveBehaviorAllowed was made available to give enterprises time to address possible breakage related to these changes. This policy will be removed in Chrome 122.

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

Asynchronous server-side Safe Browsing check

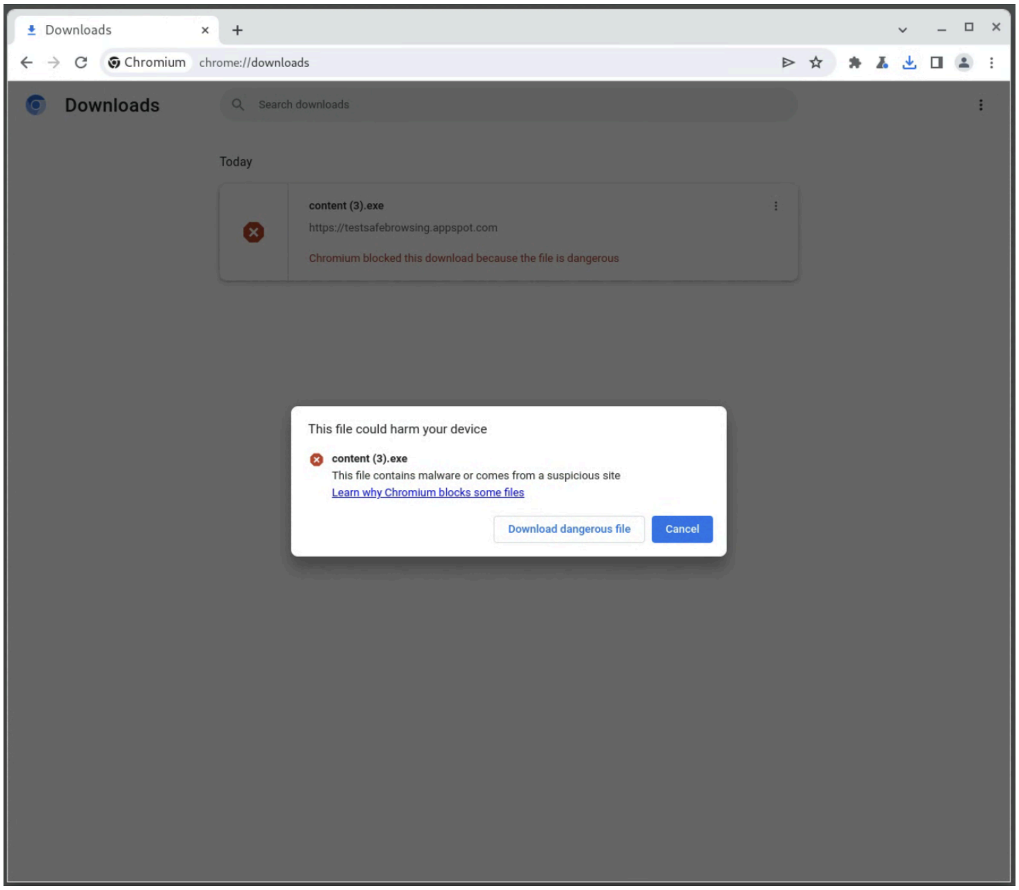
Today Safe Browsing checks are on the blocking path of page loads, meaning that the user cannot see the page until the checks are completed. To improve Chrome's loading speed, checks with the server-side Safe Browsing list will no longer block page loads after Chrome 122.
We have evaluated the risk and put mitigations in place:
1) To protect against direct exploits against the browser, local list checks will still be conducted in a synchronous manner so that malicious payloads cannot run until the local list check is completed.

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 (e.g. typed a password) by the time we show the 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.

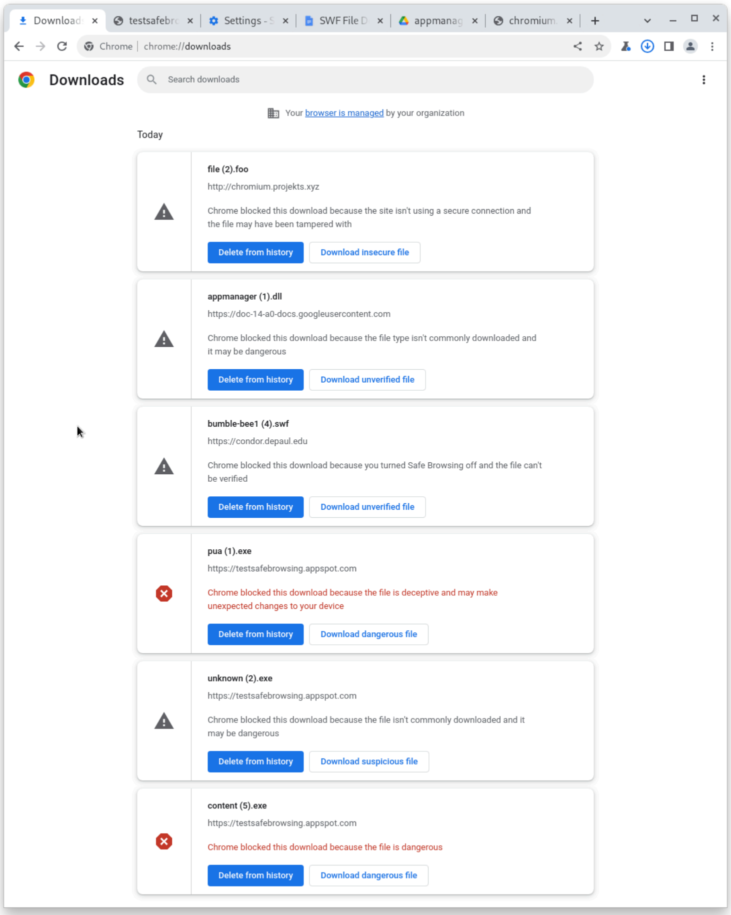
- **Chrome 122 on ChromeOS, LaCrOS, Linux, MacOS, Windows, Fuchsia:** Feature launches



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

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

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, Chrome OS, 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 Chrome OS, 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.

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:** ThrottleNonVisibleCrossOriginIframesAllowed 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 disabled 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

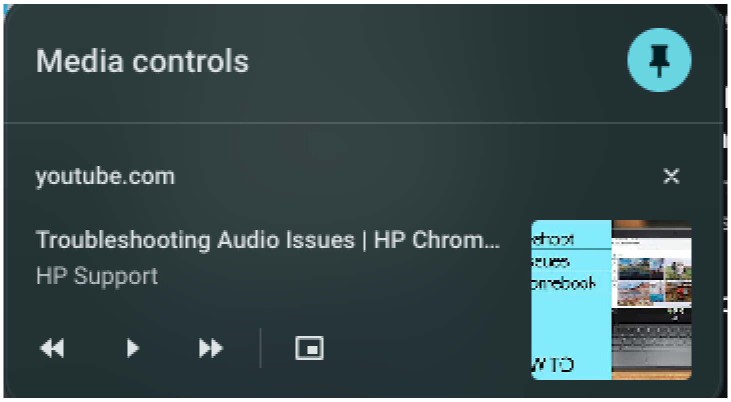
ChromeOS Flex Bluetooth Migration

ChromeOS Flex will be upgrading to the Floss bluetooth stack in ChromeOS 122. As part of this upgrade the following devices will 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

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.



App disablement by Admin in MGS

Up until now, Managed Guest Sessions (MGS) include a set of applications (Explore, Gallery, and Terminal apps) that are available to the user. With the SystemFeaturesDisableList policy, Admins will soon be able to disable these apps, blocking and hiding them from users across your enterprise.

Battery Saver

As early as ChromeOS 122, **Battery Saver** will be 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 will help when they need that last couple minutes to finish a task and don't have a charger handy. The feature will automatically be enabled when the user's battery level reaches 20%.

Upcoming Admin Console changes

Inactive browser deletion in Chrome Browser Cloud Management

As early as Chrome 124, 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.

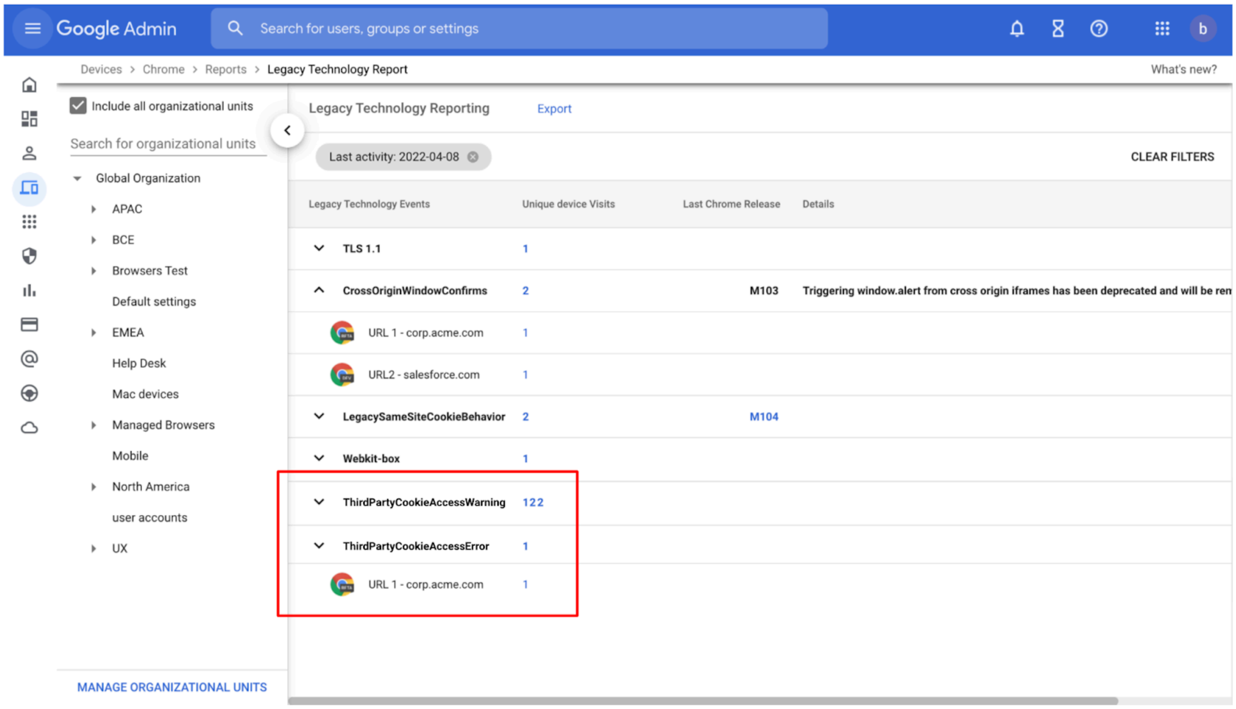
- **As early as Chrome 122:** The Inactive period for browser deletion policy UI will be available for early access in the Admin console. For IT admins who find the 18 month default inadequate, this will allow them to explicitly set a policy value (inactivity period of time) a few weeks before the actual deletion starts.

Legacy Technology report

As early as Chrome 122, 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 122 on Linux, MacOS, Windows**



☑ Include all organizational units

Legacy Technology Reporting

Last activity: 2022-04-08

Legacy Technology Events	Unique device Visits	Last Chrome Release	Details
TLS 1.1	1		
CrossOriginWindowConfirms	2	M103	Triggering window.alert from cross origin iframes has been deprecated and will be ren
URL 1 - corp.acme.com	1		
URL2 - salesforce.com	1		
LegacySameSiteCookieBehavior	2	M104	
Webkit-box	1		
ThirdPartyCookieAccessWarning	122		
ThirdPartyCookieAccessError	1		
URL 1 - corp.acme.com	1		

Previous release notes

Chrome version & targeted Stable channel release date	PDF
Chrome 120: November 29, 2023	PDF
Chrome 119: October 25, 2023	PDF
Chrome 118: October 04, 2023	PDF
Chrome 117: September 08, 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