chrome enterprise

Chrome 109 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 13, 2023.

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

Chrome 109 release summary

Chrome browser updates	**Security/ Privacy**	**User productivity /Apps**	**Management**
Confirmation permission chips in the address bar	✓		
About this page on Desktop	✓		
Chrome to change the UI for some download warnings	✓		
Changes to `HTMLElement.offsetParent`		✓	
Changes to mouse events on disabled form controls		✓	
Intent to deprecate and remove: `Event.path`		✓	
Release of Speculation Rules API for prerender in Android		✓	
Chrome handles *case* for matching in a different way		✓	
Lens image search in the Google *New tab* page search box		✓	
DNS queries to Cox resolvers automatically use SecureDNS if enabled	✓		
Chrome unpacks and scans 7z archives for malware	✓		
Measure usage of Web APIs			✓
Google Update internal upgrades			✓
New and updated policies in Chrome browser			✓
Removed policies in Chrome browser			✓
ChromeOS updates	**Security/ Privacy**	**User productivity /Apps**	**Management**
More robust logic for audio device selection		✓	

Ghost windows for ARC Apps launching		✓	
Device metrics and userID information now available to Telemetry API			✓
Color Picker improvements		✓	
Disable Trash in the Files app		✓	
Admin console updates	**Security/ Privacy**	**User productivity /Apps**	**Management**
New policies in the Admin console			✓
Upcoming Chrome browser changes	**Security/ Privacy**	**User productivity /Apps**	**Management**
Detailed translation settings in Chrome 110		✓	
Chrome for Testing		✓	
User-level Enhanced Safe Browsing on iOS in Chrome 110	✓		
MetricsReportingEnabled policy available on Android in Chrome			✓
Change in launch schedule starting in Chrome 110			✓
Content Analysis connector for local DLP agent integration	✓		
Windows 7/8/8.1 and Windows Server 2012/2012 R2 will be supported through Chrome 109			✓
Rolling out GPU Changes to NaCL Swapchain and video decoding		✓	
WebAuthn cannot be used on sites with TLS certificate errors	✓		
Default to origin-keyed agent clustering in Chrome 110		✓	
Password Change URLs		✓	
User-Agent Reduction Phase 6	✓		

Changes to phishing protection on Android	✓		
Privacy Sandbox updates	✓		
Strict MIME type checks for Worker scripts		✓	
Chrome Private Network Access preflights for subresources enforced in Chrome 113	✓	✓	
Enable access to WebHID API from extension service workers in Chrome 111		✓	
Enable access to WebUSB API from extension service workers		✓	
Deprecation of Web SQL and other old Storage features		✓	
Network Service on Windows will be sandboxed	✓		
Chrome apps no longer supported on Windows, Mac, and Linux			✓
Extensions must be updated to leverage Manifest V3		✓	
Payment Handler API will require CSP *connect-src*	✓		
First Party Sets user controls		✓	
Removal of ChromeRootStoreEnabled policy			✓
Upcoming ChromeOS changes	**Security/ Privacy**	**User productivity /Apps**	**Management**
Super Resolution Audio for Bluetooth headset microphones		✓	
Channel labeling on ChromeOS	✓		
Cursive pre-installed for Enterprise and Education accounts		✓	
Fast Pair		✓	
Updated emoji picker		✓	
Passpoint: Seamless, secure connection to Wi-Fi networks	✓	✓	

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.

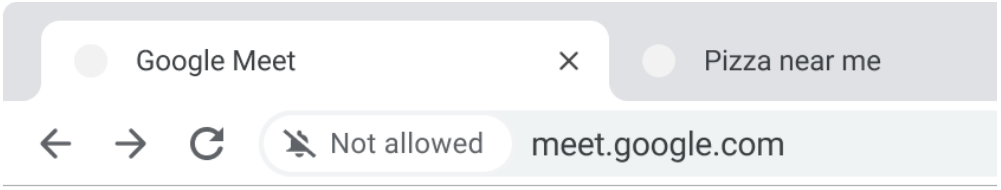
Current Chrome version release notes

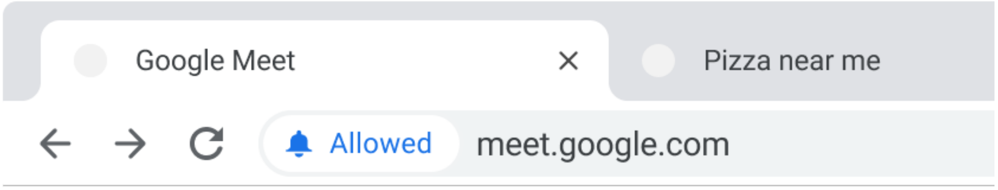
Chrome browser updates

Confirmation permission chips in the address bar

Chrome is consolidating permission prompts and indicators to make them more consistent and easier to understand. Some users now see a new permissions chip experience in the address bar, showing a chip after a user has made a decision on a permission prompt. It confirms the action a user has just taken and is shown for 4 seconds. If the user clicks on it, the page info bubble is shown, which allows users to manage their permission settings for the current site.

For some users, the lock icon in the address bar is hidden while a chip is displayed. Note that chips are only visible during certain permission requests and while a confirmation chip is displayed. As soon as the chip disappears, the lock icon becomes visible again.

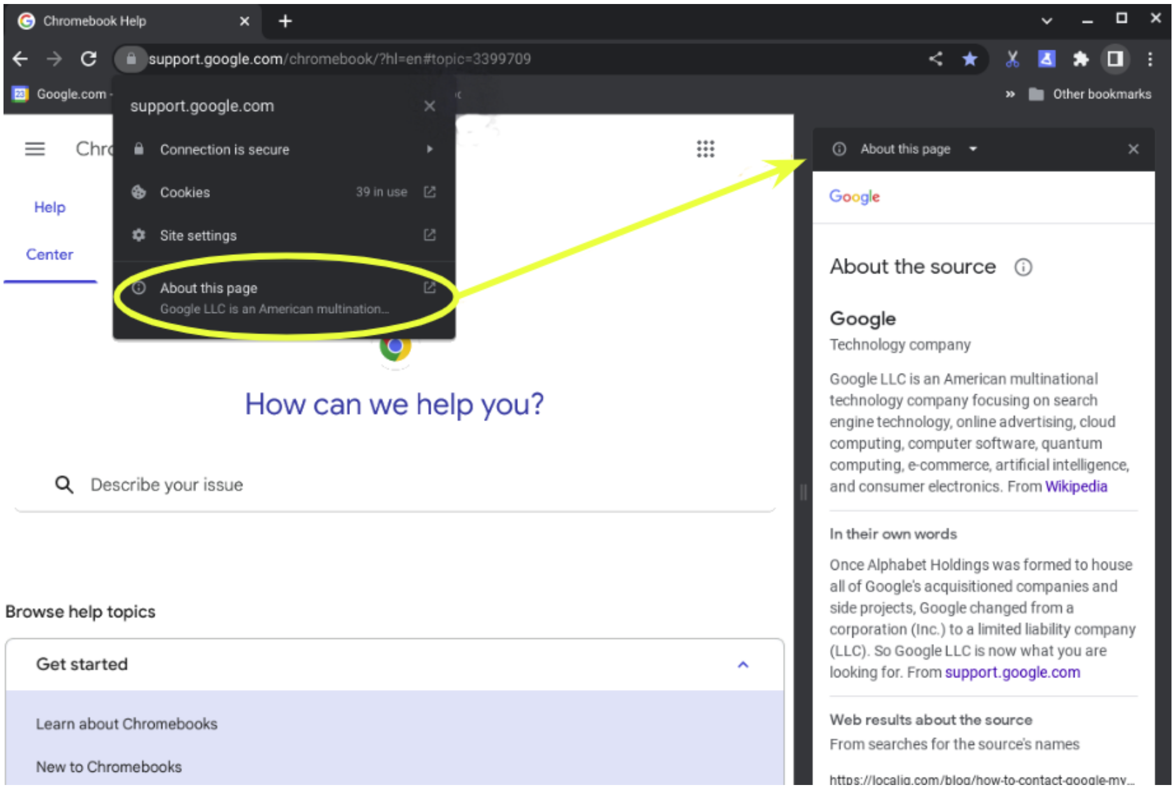




About this page on Desktop in Chrome 109

We are improving the **From the web** feature in the site info UI. It is now called **About this page** and it opens a website with multiple pieces of information regarding the source and topic of a website. Our goal is to empower users with the context to evaluate the trustworthiness of a webpage for themselves. You can learn more about helpful Search tools in this blog post.

This feature is only enabled when **Make searches and browsing better** is enabled in **Settings > Sync** and **Google Services > Other Google services**. You can control this setting with the UrlKeyedAnonymizedDataCollectionEnabled policy.



Google LLC is an American multinational technology company focusing on search engine technology, online advertising, cloud computing, computer software, quantum computing, e-commerce, artificial intelligence, and consumer electronics. From Wikipedia

In their own words

Once Alphabet Holdings was formed to house all of Google's acquisitioned companies and side projects, Google changed from a corporation (Inc.) to a limited liability company (LLC). So Google LLC is now what you are looking for. From support.google.com

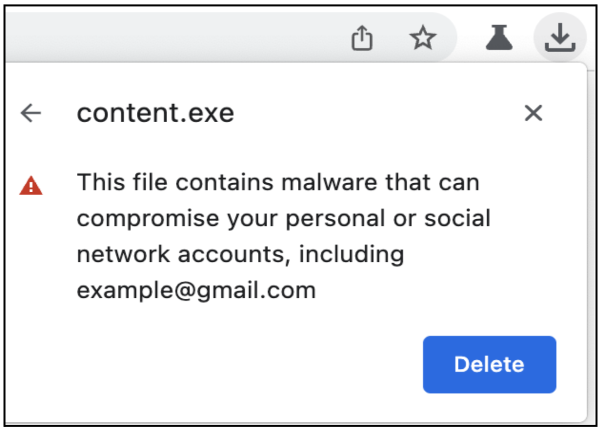
Web results about the source

From searches for the source's names

https://localiq.com/blog/how-to-contact-google-mv...

UI changes for some download warnings

As early as Chrome 109, to protect users from malware, Chrome shows detailed context and customized UIs for some download warnings. For example, if Chrome detects a download to potentially steal user's information, the description changes from *Chrome blocked this file because it is dangerous* to *This file contains malware that can compromise your personal or* *social network accounts*. You can disable download warnings by setting the SafeBrowsingProtectionLevel enterprise policy, or you can allowlist specific domains using SafeBrowsingAllowlistDomains.


content.exe

This file contains malware that can compromise your personal or social network accounts, including example@gmail.com

Changes to HTMLElement.offsetParent

In Chrome 109, the Javascript APIs HTMLElement.offsetParent, HTMLElement.offsetTop, and HTMLElement.offsetLeft are changed in an edge case involving ShadowDOM to match the behavior of Firefox and Safari. A new enterprise policy, OffsetParentNewSpecBehaviorEnabled, is available to disable the new behavior until Chrome 120. A polyfill was made to help migrate to the new behavior: https://github.com/josepharhar/offsetparent-polyfills.

Changes to mouse events on disabled form controls

In Chrome 109, some users see changes to the behavior of mouse events: clicking on form control elements with the disabled attribute triggers slightly different DOM events. Additional mouse events, including mousemove, mouseenter, mouseleave, mouseover, are fired on these elements. The ancestors of some types of form controls no longer receive click, mouseup, or mousedown events. A new enterprise policy, SendMouseEventsDisabledFormControlsEnabled, can disable the new behavior until at least Chrome 120.

Intent to deprecate and remove: Event.path

To improve web compatibility, Chrome 109 no longer supports the non-standard API `Event.path`. Websites should migrate to `Event.composedPath()`, which is a standard API that returns the same result. If you need additional time to adjust, a policy EventPathEnabled, available on Windows, Mac, Linux, ChromeOS, Android and WebView, allows you to extend the lifetime of `Event.path` by an additional 6 milestones.

Release of Speculation Rules API for prerender in Android

Chrome 103 introduced same-origin prerendering triggered by the Speculation Rules API. Chrome 109 expands coverage to also allow triggering same-site cross-origin pages. This allows web authors to suggest to Chrome which cross-origin pages that the user is likely to navigate to next. This prerendering is done with credentials and storage access, but such prerender targets must opt in by using the `Supports-Loading-Mode: credentialed-prerender` header. An enterprise policy, NetworkPredictionOptions, is available to block the usage of all prerendering activities which result in Chrome ignoring the hints provided using this API. See our article for more information.

Chrome handles *case* for matching in a different way

Previously, Chrome uppercased a request's method when matching with Access-Control-Allow-Methods response headers in CORS preflight. After this change, Chrome doesn't uppercase a request's method, except for those normalized in the specification. So, Chrome now requires exact case-sensitive matching.

For example, previously accepted, now rejected:

```
Request: fetch(url, {method: 'Foo'})

Response Header: Access-Control-Allow-Methods: FOO
```

Previously rejected, now accepted:

```
Request: fetch(url, {method: 'Foo'})
```

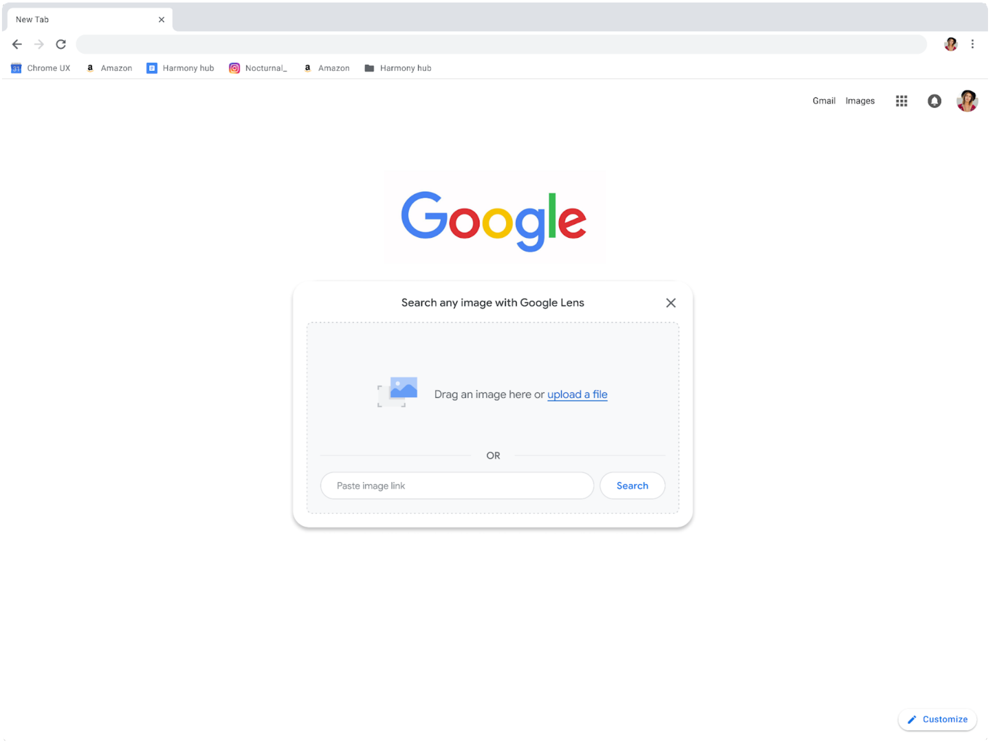
```
    Response Header: Access-Control-Allow-Methods: Foo
```

Namely, `post` and `put` are not affected because they are specified in `https://fetch.spec.whatwg.org/#concept-method-normalize`, while `patch` is affected.

An enterprise policy AccessControlAllowMethodsInCORSPreflightSpecConformant is available to control whether request methods are uppercased when matching with Access-Control-Allow-Methods response headers in CORS preflight.

Lens image search in the Google New Tab Page search box

In Chrome 109, some users see a camera icon in the search box when navigating to the Google **New tab** page. This feature allows users to search by image, by uploading a file from their computer or entering an image URL. This feature might only show on the Google **New tab** page. It does not show in Incognito, Guest User, or non-Google new tab pages. An enterprise policy, LensDesktopNTPSearchEnabled, is available to control this feature.



DNS queries to Cox resolvers automatically use SecureDNS if enabled

If SecureDNS is enabled via the DnsOverHttpsMode enterprise policy, insecure DNS requests to Cox DNS resolvers are upgraded to secure DNS requests without requiring a DnsOverHttpsTemplates enterprise policy.

Chrome unpacks and scans 7z archives for malware

In Chrome 109, Safe Browsing unpacks 7z archives locally to check for malware. This is similar to the previously-shipped local analysis of zip and rar archives. Chrome now reports contained files, hashes, and lengths to Safe Browsing. You can disable this by disabling Safe Browsing with the SafeBrowsingProtectionLevel policy.

Measure usage of Web APIs

As part of the Privacy Sandbox effort, Chrome continues to collect information about APIs commonly called by websites so that we can better understand their use as fingerprinting surfaces. You can disable this collection using the UrlKeyedAnonymizedDataCollectionEnabled enterprise policy.

Google Update internal upgrades

Over the coming weeks, Google introduces an overhauled version of **Google Update** that:

1. provides a cross-platform core for future development of update-related features.
2. improves its performance and reliability.

All existing enterprise policies and controls for managing Chrome's version will continue to work the same way. These changes first roll out to macOS and eventually to Windows.

Note: For customers that allowlist specific folders and binaries, there is a path change on Mac as follows:

- `Old: (~)/Library/Google/GoogleSoftwareUpdate`
- `New: (~)/Library/Google/GoogleUpdater`

New and updated policies in Chrome browser

Policy	Description
AssistantWebEnabled	Allow using Google Assistant on the web, for example, to enable changing passwords automatically.
ContextAwareAccessSignalsAllowlist	Enable the Chrome Enterprise Device Trust Connector attestation flow for a list of URLs.
SendMouseEventsDisabledFormControlsEnabled	Control the new behavior for event dispatching on disabled form controls.
RequireOnlineRevocationChecksForLocalAnchors	Require online OCSP or CRL checks for local trust anchors (now also available on iOS).
AccessControlAllowMethodsInCORSPreflightSpecConformant	Make `Access-Control-Allow-Methods` matching in CORS preflight spec conformant.

Removed policies in Chrome browser

Policy	Description
UrlParamFilterEnabled	Control the URL parameter filter feature

ChromeOS updates

More robust logic for audio device selection

ChromeOS now remembers multiple previously selected audio peripherals. This should reduce the need to change the audio input or output device when reconnecting a dock, monitor, hub, and so on.

Ghost windows for ARC Apps launching

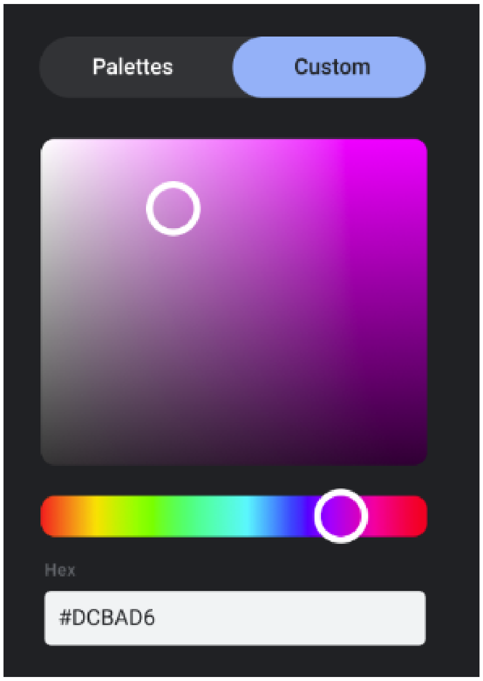
When users try to launch an Android Runtime for Chrome (ARC) app when ARC is still booting or the app is still loading, the shelf presents the App icon with a spinner above it to indicate the App is pending launch. With this feature, the ghost window pops up as an intermediate window state during the ARC booting time which improves perception and sets expectations of ARC apps by actively showing progress in the UI.

Device metrics and userID information now available to Telemetry API

The Telemetry API can provide valuable insights about users and devices in your enterprise. ChromeOS 109 now reports device activity status and userID data for the Telemetry API.

Color Picker Improvements

In ChromeOS Gallery, users can now choose between the **Palette** and **Custom** tabs within the color palette dialog. Tapping the **Custom** tab displays the freeform color select tool. Users can also enter a HEX code to choose a specific color.



Disable Trash in the Files app

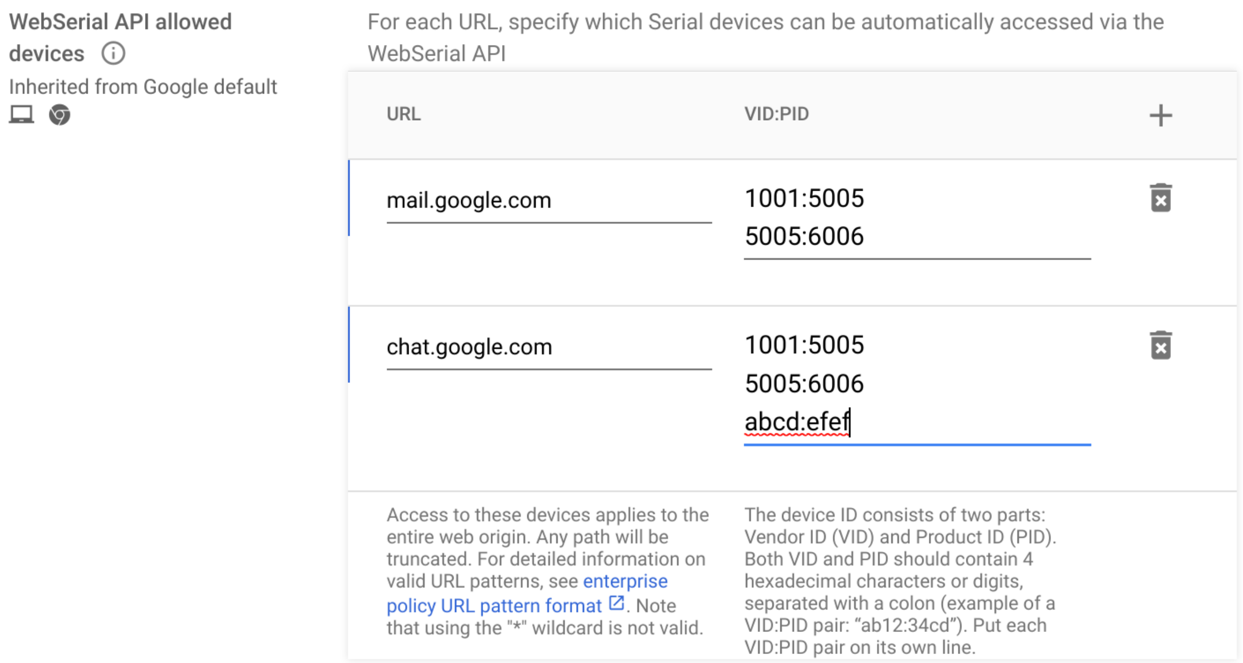
In ChromeOS 108, we introduced a new **Trash** section in the **Files** app, giving you 30 days to change your mind before files are permanently deleted. **Note:** This feature doesn't support Play, Linux, Windows file areas.

In ChromeOS 109, you can now disable the **Trash** section with the TrashEnabled policy.

Admin console updates

New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
SerialAllowUsbDevicesForUrls	User & Browser Settings; Managed Guest Session	Chrome ChromeOS Android	Hardware > WebSerial API allowed devices



WebSerial API allowed devices ⓘ

Inherited from Google default

For each URL, specify which Serial devices can be automatically accessed via the WebSerial API

URL	VID:PID
mail.google.com	1001:5005 5005:6006
chat.google.com	1001:5005 5005:6006 abcd:efef

Access to these devices applies to the entire web origin. Any path will be truncated. For detailed information on valid URL patterns, see enterprise policy URL pattern format. Note that using the "*" wildcard is not valid.

The device ID consists of two parts: Vendor ID (VID) and Product ID (PID). Both VID and PID should contain 4 hexadecimal characters or digits, separated with a colon (example of a VID:PID pair: “ab12:34cd”). Put each VID:PID pair on its own line.

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

Detailed translation settings in Chrome 110

New detailed translation settings will be added for controlling the current target language, never translate languages, and always translate languages. These settings were previously only editable from the Translate UI bubble but will now be permanently exposed under *chrome://settings/language*. Enterprise users may use the existing TranslateEnabled enterprise policy to globally enable or disable translation.

Chrome for Testing

As early as Chrome 110, Puppeteer, Chrome's browser automation library, will use the Chrome for Testing binary instead of a Chromium binary. In case you have the Chromium binary allowlisted, you might consider allowlisting the Chrome for Testing binary too.

Chrome for Testing is a dedicated Chrome flavor for the automated testing use case. It's not an end-user facing product, but rather a tool to be used by automation engineers through other projects such as Puppeteer. Chrome for Testing is a completely separate binary from *regular* Chrome.

User-level Enhanced Safe Browsing on iOS in Chrome 110

For Chrome on iOS where the Safe Browsing protection level is not controlled by SafeBrowsingProtectionLevel, users who are signed in and syncing, and have enabled Enhanced Safe Browsing on their Google Account, will be notified that Enhanced Safe Browsing has been enabled on their Chrome profile. Disabling Enhanced Safe Browsing on a synced Google Account will disable Enhanced Safe Browsing for their Chrome profile. Additionally, users that are signed-in and non-synced might be prompted to enable Chrome Enhanced Safe Browsing within 5 minutes of enabling Account Level Enhanced Safe Browsing.

MetricsReportingEnabled policy available on Android in Chrome

As early as Chrome 110, Chrome on Android will slightly modify the first run experience to support the MetricsReportingEnabled policy. If the admin disables metrics reporting, there will be no change to the first run experience. If the admin enables metrics, users will still be able to change the setting in Chrome settings. When enabled, the MetricsReportingEnabled policy allows anonymous reporting of usage and crash-related data about Chrome to Google.

Change in launch schedule starting in Chrome 110

Starting in Chrome 110, Chrome will be rolled out to the Stable channel one week earlier than previously communicated to a very small subset of users. For example, the Chrome 110 Stable release moves from February 7 to February 1, 2023.

You can also expect to see a much smaller rollout at a significantly reduced percentage of our user population for the first week of the published Stable release date. The wider rollout to most users will happen at a similar timeframe to the earlier communicated dates.

Content Analysis connector for local DLP agent integration

Some third party software, for example AV or DLP agents, injects code into Chrome. Though this practice is discouraged, it is still prevalent in the enterprise environment since there are few alternatives for these local agents.

Chrome 110 will provide secure, native integration that allows selected third party DLP agents to protect sensitive data transfers that happen within the browser.

Windows 7/8/8.1 and Windows Server 2012/2012 R2 will be supported through Chrome 109

Microsoft is ending support for most variants of Windows 7/8/8.1 in January 2023. As announced in a previous blog post, Chrome 109 will be the last supported version of Chrome for these operating systems.

Update: Chrome running on Windows Server 2012 and Windows Server 2012 R2 will not be updated beyond Chrome 109, as those OSes are based on Windows 8/8.1. However, critical security fixes will be issued to Chrome 109 on these two OS versions until October 10, 2023 to ease customer transitions. For the most up to date information, see this post in the Chrome Enterprise and Education help center.

Rolling out GPU changes to NaCL Swapchain and video decoding

As early as Chrome 110, we will refactor the implementation of the NaCL swapchain and the Pepper video decoding APIs. These changes are not intended to have any behavioral impact on users. However, it is possible that due to bugs they might result in visual artifacts, unacceptably slow performance when playing video, unacceptable increases in power, or crashes. Information about how to signal any problems will be available as these refactors roll out.

WebAuthn cannot be used on sites with TLS certificate errors

Starting on Chrome 110, Chrome will stop allowing WebAuthn requests on websites with TLS certificate errors. The criteria will be the same used for showing danger interstitials or a *Not secure* pill on the omnibox. This will prevent bad actors from generating valid assertions in a Man-in-the-Middle attack on users who may skip the interstitial.

Enterprises will be able to use the **AllowWebAuthnWithBrokenTlsCerts** policy if needed as a workaround.

Default to origin-keyed agent clustering in Chrome 110

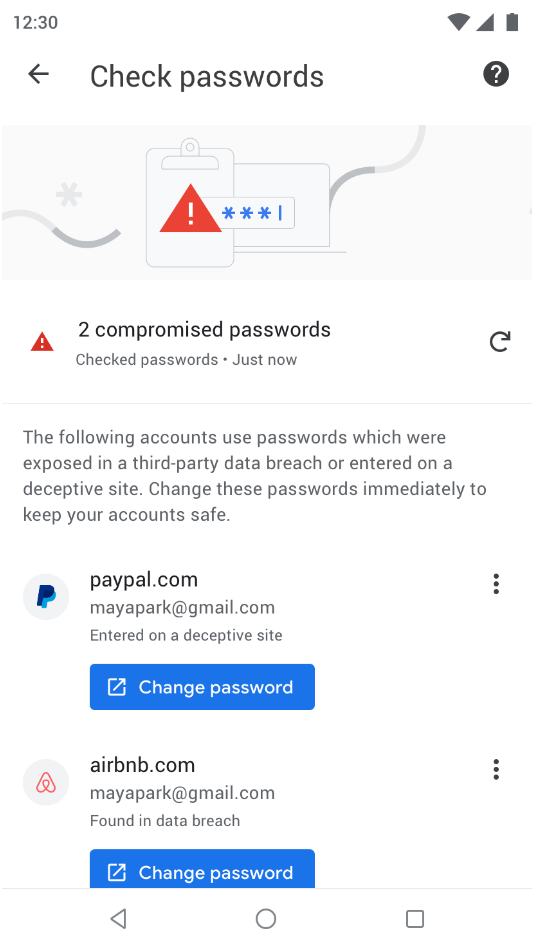
As early as Chrome 110, websites will be unable to set `document.domain`. Websites will need to use alternative approaches such as `postMessage()` or Channel Messaging API to communicate cross-origin. If a website relies on same-origin policy relaxation via `document.domain` to function correctly, it will need to send an `Origin-Agent-Cluster: ?0` header along with all documents that require that behavior.

Note: `document.domain` has no effect if only one document sets it.

The OriginAgentClusterDefaultEnabled enterprise policy will allow you to extend the current behavior.

Password Change URLs

The **Check passwords** tool, `chrome://settings/passwords/check`, and its analogues on other platforms, query change password URLs from the backend to facilitate fixing compromised passwords, for example, `https://example.com/settings/change_password.html`. This launch will extend the list of URLs available on the backend.



12:30

Check passwords

2 compromised passwords

Checked passwords • Just now

The following accounts use passwords which were exposed in a third-party data breach or entered on a deceptive site. Change these passwords immediately to keep your accounts safe.

paypal.com

mayapark@gmail.com

Entered on a deceptive site

Change password

airbnb.com

mayapark@gmail.com

Found in data breach

Change password

User-Agent Reduction Phase 6

As of Chrome 110, some portions of the User-Agent string will be reduced on Chrome for Android. As previously detailed in the Chromium blog, we intend to proceed with Phase 6 of the User-Agent Reduction plan. For more details, see this reference page and Chromium update. The UserAgentReduction policy allows for opting out of these changes.

Changes to phishing protection on Android as early as Chrome 111

When a user authenticates to Android with their Google password, for example during account setup, Chrome will be notified so the password can begin receiving phishing protection when surfing the Web with Chrome. In previous versions of Chrome on Android, users needed to explicitly provide their password within a Chrome tab, for example, sign in to Gmail, to receive phishing protection for their Google password.

You can disable warnings regarding password reuse by setting PasswordProtectionWarningTrigger to 0.

Privacy Sandbox updates in Chrome 111

Chrome 111 will update the user experience of the new ad privacy features related to the Privacy Sandbox project. As part of this, Chrome will show users a confirmation dialog that explains their options and allows them to set their preferences.

IT admins can disable Chrome's Privacy Sandbox settings via the **PrivacySandboxAdTopicsEnabled**, **PrivacySandboxSiteEnabledAdsEnabled**, and **PrivacySandboxAdMeasurementEnabled** enterprise policies, and suppress the user-facing prompt via the **PrivacySandboxPromptEnabled** policy.

For more information, see the developer documentation about Privacy Sandbox technologies in Chrome.

Strict MIME type checks for Worker scripts

As early as Chrome 111, Chrome will strictly check MIME types for Worker scripts, like Service Workers or Web Workers. Strict checking means that Chrome will only accept JavaScript resources for Workers with a MIME type of `text/javascript`. Currently, Chrome will also accept other MIME types, like `text/ascii`. This change is aimed at improving the security of web applications, by preventing inclusion of inappropriate resources as JavaScript files.

Disabling the StrictMimetypeCheckForWorkerScriptsEnabled policy allows you to keep the current behavior.

Chrome Private Network Access preflights for subresources enforced in Chrome 113

Chrome 104 started sending a CORS preflight request ahead of any private network requests for subresources, asking for explicit permission from the target server. This request carries a new `Access-Control-Request-Private-Network: true` header. In this initial phase, this request is sent, but no response is required from network devices. If no response is received, or it does not carry a matching `Access-Control-Allow-Private-Network: true` header, a warning is shown in DevTools. For more details, see this blog post.

As early as Chrome 111 on Android, the warnings will turn into errors and affected requests will fail, for sites not opted out via an Origin Trial. Remaining platforms will also have these warnings enforced in Chrome 113. You can disable Private Network Access checks using the InsecurePrivateNetworkRequestsAllowed and InsecurePrivateNetworkRequestsAllowedForUrls enterprise policies.

If you want to test this feature in advance, you can enable warnings using `chrome://flags/#private-network-access-send-preflights`. If you want to test how it behaves once warnings turn into errors, you can enable `chrome://flags/#private-network-access-respect-preflight-results`.

Chrome is making this change to protect users from cross-site request forgery (CSRF) attacks targeting routers and other devices on private networks. To learn more about mitigating this change proactively, see details on what to do if your site is affected. Read the whole blog post for a more general discussion and latest updates about Private Network Access preflights.

Enable access to WebHID API from extension service workers in Chrome 111

This launch will enable access to WebHID API from extension service workers as a migration path for manifest V2 extensions that currently access the API from a background page.

Enable access to WebUSB API from extension service workers

As early as Chrome 111, we will enable access to WebUSB API from extension service workers as a migration path for Manifest V2 extensions that currently access the API from a background page.

WebUSB policies can also be applied to extension origins to control this behavior. See DefaultWebUsbGuardSetting, WebUsbAskForUrls, WebUsbBlockedForUrls, and WebUsbAllowDevicesForUrls for more details.

Deprecation of Web SQL and other old Storage features

The Web SQL API is rarely used, and since its removal by Safari, only Chromium-based browsers have supported it. It requires frequent security fixes, and developers have been discouraged from using it for years. We're now engaging in an effort to seek out and warn anyone who may still be using Web SQL, with the goal of removing it entirely in 2023.

What you need to do depends on how you're using Web SQL:

- If you're just using Web SQL to detect whether a given browser is Chrome, that method will stop working when Web SQL is removed. Navigator.userAgentData is a better alternative.
- If you're using Web SQL to simply store a few data points, localStorage and sessionStorage provide easier ways to do this.
- However, if you're using Web SQL for more complex storage, you'll need to find a proper replacement.

Here are some migration options for more complex storage:

- If your storage needs don't require a relational database, IndexedDB is the standard solution for structured storage on the web. Large sites rely on IndexedDB, and all major browsers support it.
- For those who do need a relational database, we've partnered with the SQLite team to create an evergreen cross-browser Web SQL replacement. In November, SQLite released a web backend, using Emscripten to compile to WebAssembly and leveraging the new File System Access Handles API as a low-level virtual file

> interface. It's about as fast as Web SQL, and often it's faster. For more information, see our blog post Deprecating and removing Web SQL, which we'll update when noteworthy events occur.

We've already disabled Web SQL in third-party contexts. The next step is to remove support in non-secure contexts. In Chrome 105, we introduced a deprecation warning in DevTools. We'll remove this support in Chrome 110. An enterprise policy, WebSQLNonSecureContextEnabled, will let Web SQL function in non-secure contexts for a few months past the removal date.

In Chrome 110, we will also remove the window.webkitStorageInfo API. This legacy quota API has been deprecated since 2013, and has been replaced by the now standardized StorageManager API.

Network Service on Windows will be sandboxed

As early as Chrome 111, 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 apps no longer supported on Windows, Mac, and Linux

As previously announced, Chrome apps are being phased out in favor of Progressive Web Apps (PWAs) and web-standard technologies. The deprecation schedule was adjusted to provide enterprises who used Chrome apps additional time to transition to other technologies, and Chrome apps will now stop functioning in Chrome 112 or later on Windows, Mac, and Linux. If you need additional time to adjust, a policy ChromeAppsEnabled will be available to extend the lifetime of Chrome Apps an additional 2 milestones.

Starting in Chrome 105, if you're force-installing any Chrome apps, users are shown a message stating that the app is no longer supported. The installed Chrome Apps are still launchable.

Starting with Chrome 112, Chrome Apps on Windows, Mac and Linux will no longer work. To fix this, remove the extension ID from the force-install extension list, and if necessary, add the corresponding **install_url** to the web app force install list. For common Google apps, the **install_urls** are listed below:

Property	**Extension ID** (Chrome App)	**install_url** (PWA / Web App)
Gmail	pjkljhegncpnkpknbcohdijeoejaedia	https://mail.google.com/mail/installwebapp?usp=admin
Docs	aohghmighlieiainnegkcijnfilokake	https://docs.google.com/document/installwebapp?usp=admin
Drive	apdfllckaahabafndbhieahigkjlhalf	https://drive.google.com/drive/installwebapp?usp=admin
Sheets	felcaaldnbdncclmgdcncolpebgiejap	https://docs.google.com/spreadsheets/installwebapp?usp=admin
Slides	aapocclcgogkmnckokdopfmhonfmgoek	https://docs.google.com/presentation/installwebapp?usp=admin
Youtube	blpcfgokakmgnkcojhhkbfbldkacnbeo	https://www.youtube.com/s/notifications/manifest/cr_install.html

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.

All new extensions submitted to the Chrome Web Store already must implement Manifest V3, but existing Manifest V2 extensions can still be updated, and still run in Chrome. In 2023, extensions using Manifest V2 may cease running in Chrome. If your organization is running extensions that use Manifest V2, you must update them to leverage Manifest V3.

Starting with Chrome 110, an Enterprise policy ExtensionManifestV2Availability will be 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 until at least January 2024.

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.

For more details, refer to the Manifest V2 support timeline.

Payment Handler API will require CSP *connect-src*

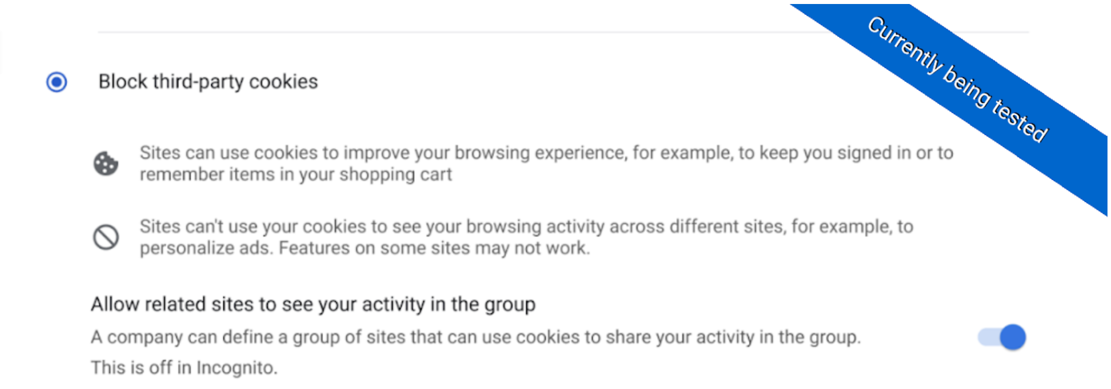
If your organization is using the Web Payment API (Payment Handler and Payment Request) and also uses Content-Security-Policy (CSP) for better protection, then you need to make sure the domains of HTTP requests sent from the Web Payment API are added to the *connect-src* directive of the CSP. For more information, see this developer blog post.

First-Party Sets user controls

First-Party Sets is an upcoming framework for developers to declare relationships between domains, such that the browser can make decisions regarding access based on the third party's relationship to the first party. A set may enjoy first party benefits, including continued access to their cookies when the top-level domain is in the same set.

First-Party Sets are part of Chrome's roadmap for a more privacy-focused web.

Chrome 111 introduces user controls for these First-Party Sets.



Currently being tested

● Block third-party cookies

Sites can use cookies to improve your browsing experience, for example, to keep you signed in or to remember items in your shopping cart

Sites can't use your cookies to see your browsing activity across different sites, for example, to personalize ads. Features on some sites may not work.

Allow related sites to see your activity in the group

A company can define a group of sites that can use cookies to share your activity in the group. This is off in Incognito.

Removal ChromeRootStoreEnabled policy

In Chrome 105 Chrome announced the launch of the Chrome Root Store. A new policy, called ChromeRootStoreEnabled, was introduced to allow selective disabling of the Chrome Root Store in favor of the platform root store. The policy will be removed in Chrome 113.

Upcoming ChromeOS changes

Super Resolution Audio for Bluetooth headset microphones

Starting in 110, your ChromeOS device will help you sound more natural in calls and conferences by reconstructing the high-frequency audio components that are not transmitted from Bluetooth headsets.

Cursive pre-installed for Enterprise and Education accounts

As early as ChromeOS 110, Cursive, a stylus-first notes app, will be available for Chromebooks. In an upcoming release, it will be pre-installed for all Enterprise and Education accounts on stylus-enabled Chromebooks. If you want to block access to the app, you can prevent Chromebooks in your enterprise from accessing *cursive.apps.chrome*.

Channel labeling on ChromeOS

Trying out the latest version of ChromeOS? For users on non-stable channels (Beta, Dev, Canary), starting in 110, you will see which channel you are on in the bottom right. You will be able to click the time to open quick settings, which will have a new UI showing the device build and a feedback button.

Fast Pair

Fast Pair will make Bluetooth pairing easier on ChromeOS devices and Android phones. When you turn on your Fast Pair-enabled accessory, it will automatically detect and pair with your ChromeOS device or Android phone in a single tap. Fast Pair will also associate your Bluetooth accessory with your Google account, making it incredibly simple to move between devices without missing a beat. This feature will be available as early as ChromeOS 111.

Updated emoji picker

The updated emoji picker will include commonly used symbols and characters, such as scientific notations and math operators. In addition, we will also include text-based emoticons (kaomoji) for even more expressive conversations. The new top-level navigation bar will help you find the high-level category quickly, ranging from emojis, symbols, and emoticons. The improved universal search will show possible matches from all categories.

Passpoint: Seamless, secure connection to Wi-Fi networks

Starting as early as ChromeOS 114, Passpoint will streamline Wi-Fi access and eliminate the need for users to find and authenticate a network each time they visit. Once a user accesses the Wi-Fi network offered at a location, the Passpoint-enabled client device will automatically connect upon subsequent visits.

Previous release notes

Chrome version & targeted Stable channel release date	PDF
Chrome 108: Nov 29, 2022	PDF
Chrome 107: October 25, 2022	PDF
Chrome 106: September 27, 2022	PDF
Chrome 105: August 30, 2022	PDF
Archived release notes	

Additional resources

- For emails about future releases, sign up here.
- To try out new features before they're released, sign up for the trusted tester program.
- Connect with other Chrome Enterprise IT admins through the Chrome Enterprise Customer Forum.
- How Chrome releases work—Chrome Release Cycle
- Chrome Browser downloads and Chrome Enterprise product overviews—Chrome Browser for enterprise
- Chrome version status and timelines—Chrome Platform Status | Google Update Server Viewer
- Announcements: Chrome Releases Blog | Chromium Blog
- Developers: Learn about changes to the web platform.

Still need help?

- Google Workspace, Cloud Identity customers (authorized access only)—Contact support
- Chrome Browser Enterprise Support—Sign up to contact a specialist
- Chrome Administrators Forum
- Chrome Enterprise Help Center

Google and related marks and logos are trademarks of Google LLC. All other company and product names are trademarks of the companies with which they are associated.