chrome enterprise

Chrome 105 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 August 30, 2022.

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

Chrome 105 release summary

Chrome browser updates	Security/ Privacy	User productivity /Apps	Management
Chrome apps no longer supported on Windows, Mac, and Linux: Chrome 105 shows warning message		✓	✓
Launch Renderer AppContainer	✓		✓
Chrome maintains its own default root store	✓		
Web SQL deprecation in non-secure contexts	✓		
Chrome sync ends support for Chrome 73 and earlier	✓		
Policies on Mac distinguished between user and machine			✓
Add Set-Cookie as forbidden header name for Fetch	✓		
Disabling Chrome Variations no longer disables the Chrome Cleanup Tool			✓
Internal certificate viewer for server certificates on Mac and Windows	✓		
Privacy Sandbox updates on FLEDGE on Android	✓		
WebAuthn: prompt users for Bluetooth permissions on macOS	✓		
Syntax changes to markup based Client Hints delegation	✓		
About this page (Android)		✓	
Enhanced Safe Browsing Google accounts integration on desktop	✓		
ForceBrowserSignIn policy requires EnableExperimentalPolicies on Linux			✓
Browser Extension Telemetry	✓		
New and updated policies in Chrome browser			✓

ChromeOS updates	Security/ Privacy	User productivity /Apps	Management
Adaptive charging to extend battery life		✓	
Close a desk and its windows in one click		✓	
Admin console updates	**Security/ Privacy**	**User productivity /Apps**	**Management**
Group-based policy for managed apps & extensions			✓
Configure alerts for extension requests			✓
Browser Details: Installed apps & extensions UX changes		✓	✓
New policies in the Admin console			✓
Upcoming Chrome browser changes	**Security/ Privacy**	**User productivity /Apps**	**Management**
Support for Encrypted Client Hello (ECH)	✓		
Changes to chrome.runtime	✓		
Persistent quota deprecation launch			✓
Chrome will show Journeys on the History page on Android		✓	
Incognito lock on Android	✓		
Incognito downloads prompt on Android		✓	
Network Service on Windows will be sandboxed	✓		
Removal of window.webkitStorageInfo			✓
Removal of master_preferences			✓
User-Agent reduction Phase 5	✓		
Automated password changes on Desktop	✓		

	Security/ Privacy	User productivity /Apps	Management
Chrome sends Private Network Access preflights for subresources	✓		
Marshmallow deprecation for Chrome on Android	✓		
Upcoming ChromeOS changes	**Security/ Privacy**	**User productivity /Apps**	**Management**
Chrome OS Accessibility settings improvements		✓	
Photos integrations		✓	
Cursive pre-installed for Enterprise and Education accounts		✓	
Long-press diacritics		✓	
Fast Pair		✓	
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.

Chrome browser updates

Chrome apps no longer supported on Windows, Mac, and Linux: Chrome 105 shows warning message

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 109 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 109, 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

Launch Renderer AppContainer

As early as Chrome 105, a further sandbox security mitigation applies to renderer processes. They are placed inside an additional App Container on top of the existing sandbox. This prevents malicious code from having any network privileges by subverting kernel APIs from within the renderer process.

While we do not expect any incompatibilities with this new mitigation, some security products might react adversely to this.

A new policy RendererAppContainerEnabled allows selective disabling of this security mitigation while these issues are resolved. You can set this policy to *Disabled* to force disable the mitigation, otherwise it is enabled by default.

Chrome maintains its own default root store

As early as Chrome 105, to improve user security and provide a consistent experience across different platforms, Chrome maintains its own default root store and built-in certificate verifier. Chrome continues to use custom local roots installed to the operating system's trust store. See our article about the Chrome Root Program for more information.

We do not anticipate any changes to how enterprises currently manage their fleet and trusted enterprise CAs, such as through group policy, macOS Keychain Access, or system management tools like Puppet.

A new policy, called **ChromeRootStoreEnabled**, allows selective disabling of the Chrome Root Store in favor of the platform root store. You can set this policy to *Disabled* to force the use of the platform root store, otherwise it is enabled by default. The policy will be available until Chrome 111.

Web SQL deprecation in non-secure contexts

The non-standard Web SQL API is rarely used and requires frequent security fixes. At this point, only Chromium-based browsers support it. Web developers have been discouraged from using it for years. We are engaging in a careful process to seek out and warn partners who may still be using Web SQL, with the goal of removing it from Chrome entirely in 2023. Meanwhile, we're working on a replacement using WebAssembly.

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 introduce a deprecation warning in DevTools. In early 2023, we plan to remove support in third-party contexts.

An enterprise policy, **WebSQLNonSecureContextEnabled**, is available when support ends, to allow Web SQL API to function in non-secure contexts if needed. The policy will expire in alignment with the API's non-secure context removal schedule.

Chrome sync ends support for Chrome 73 and earlier
As early as Chrome 105, Chrome sync no longer supports Chrome 73 and earlier. You need to upgrade to a more recent version of Chrome if you want to continue using Chrome sync.

Policies on Mac distinguished between user and machine

Chrome 105 on Mac adheres to the same policy precedence as other platforms. As of 105, machine-level policies, for example, set via Chrome Browser Cloud Management token management, take precedence over user-level policies. Previously, all policies were set as machine-level, regardless of their origin. If this change has any unexpected effects on your users, you can temporarily use the PolicyScopeDetection enterprise policy to revert to the previous behavior.

Add Set-Cookie as forbidden header name for Fetch

Set-Cookie headers are semantically response headers, so they cannot just be combined and require more complex handling in the Headers object. Starting with Chrome 105, the Set-Cookie header is forbidden as a request header to avoid leaking this complexity into requests, as it is not useful for requests anyway. You can read more about this change on Github.

Disabling Chrome Variations no longer disables the Chrome Cleanup Tool

Starting in Chrome 105, turning off variations no longer affects whether the Chrome Cleanup Tool runs. This means that enterprises that already have Chrome Variations turned off might notice that the Chrome Cleanup Tool starts running once per week in Chrome 105 on Windows.

To disable it, you can still set the ChromeCleanupEnabled enterprise policy to *Disabled*.

Internal certificate viewer for server certificates on Mac and Windows

In Chrome 105 on Mac and Windows, the certificate viewer accessed from the page info bubble switches from using the platform provided viewer to one that is provided by Chrome. The Chrome certificate viewer is already used on Linux and ChromeOS.

Privacy Sandbox updates on FLEDGE on Android

In Chrome 105, the Privacy Sandbox provides controls for the new Topics & Interest Group APIs on Android. This follows the launch of these APIs on Desktop in Chrome 104. It also introduces a one-time dialog for Android users that explains Privacy Sandbox to users and allows them to manage their preferences. Guest users or managed EDU users do not see this dialog.

Some users may see this opt-in consent dialog:

Help us build a more private web

Chrome is exploring new features that allow sites to deliver the same browsing experience using less of your info

Limited sharing between sites

We're exploring ways to restrict tracking while enabling sites to stop ad spam and fraud.

More control over the ads you see

You can see and remove topics of interest sites use to show you ads. Chrome estimates your interests based on your recent browsing history.

Learn more about ad personalization in Chrome   ⌄

You can change your mind at any time in Chrome settings. The trials run alongside the current way ads get served, so you won't see changes right away.

No thanks   Yes, I'm in

Other users may see this dialog:
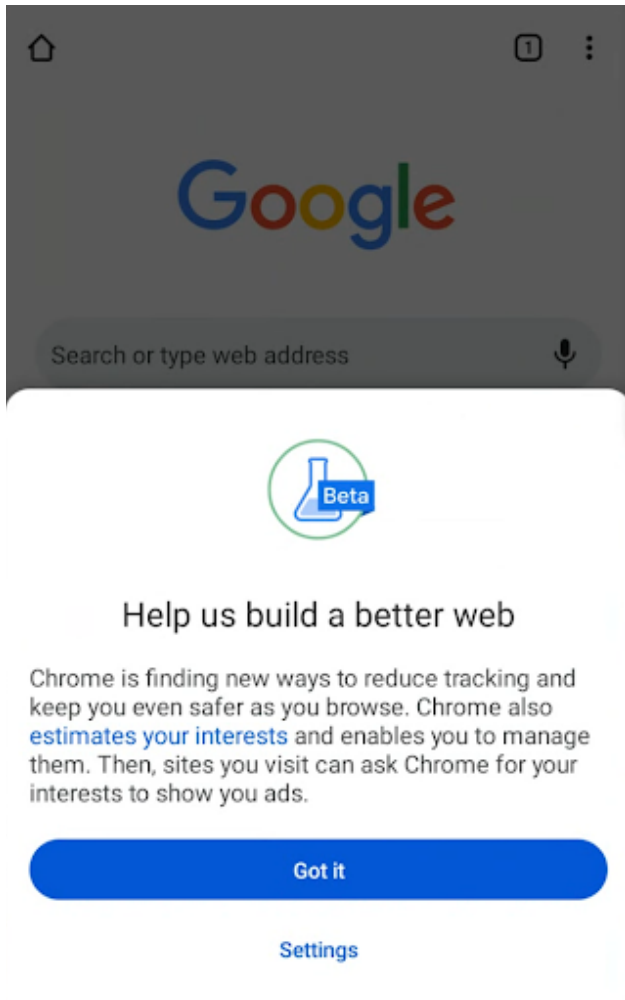
Admins can prevent the dialog from appearing for their managed users by controlling third party cookies explicitly via policy:

- To allow third-party cookies and Privacy Sandbox features, set BlockThirdPartyCookies to disabled.
- To disallow third-party cookies and Privacy Sandbox features, set BlockThirdPartyCookies to enabled. This might cause some sites to stop working.

Any of the above settings will prevent the dialog from showing. Privacy Sandbox features are also disabled, and no dialog shown, if DefaultCookiesSetting is set to *Do not allow any site to set local data*.

WebAuthn: prompt users for Bluetooth permissions on macOS

When a user attempts to use a phone as a security key on macOS, and Chrome does not have Bluetooth permission, and macOS doesn't show a permission prompt itself, Chrome now prompts the user to open System Preferences to grant the required permission. This is not enabled for macOS 13 because, as of current macOS betas, it's not yet possible to have the new System Settings open to the correct location.

Syntax changes to markup based Client Hints delegation

We're switching from syntax close to HTTP Permissions-Policy to use syntax closer to the iframe allow attribute at the request of developers.

There is existing HTML syntax to delegate client hints to third-party content which requires client information lost by user agent reduction. This syntax was introduced in Chrome 100 and is being removed in Chrome 105, for example:

```
<meta name="accept-ch" value="sec-ch-dpr=(https://foo.bar
https://baz.qux), sec-ch-width=(https://foo.bar)">
```

The replacement for this introduced in Chrome 105 is formatted as follows:

```
<meta http-equiv="delegate-ch" value="sec-ch-dpr
https://foo.bar https://baz.qux; sec-ch-width
https://foo.bar">
```

About this page on Android

We are improving the **From the web** feature in the site info UI. It is now called **About this page** and opens a website with multiple pieces of information regarding the source and topic of a website.

This feature is only enabled when **Make searches and browsing better** is enabled in **Settings > Sync and Google sServices>Other Google services.** You can control this setting with the UrlKeyedAnonymizedDataCollectionEnabled policy.
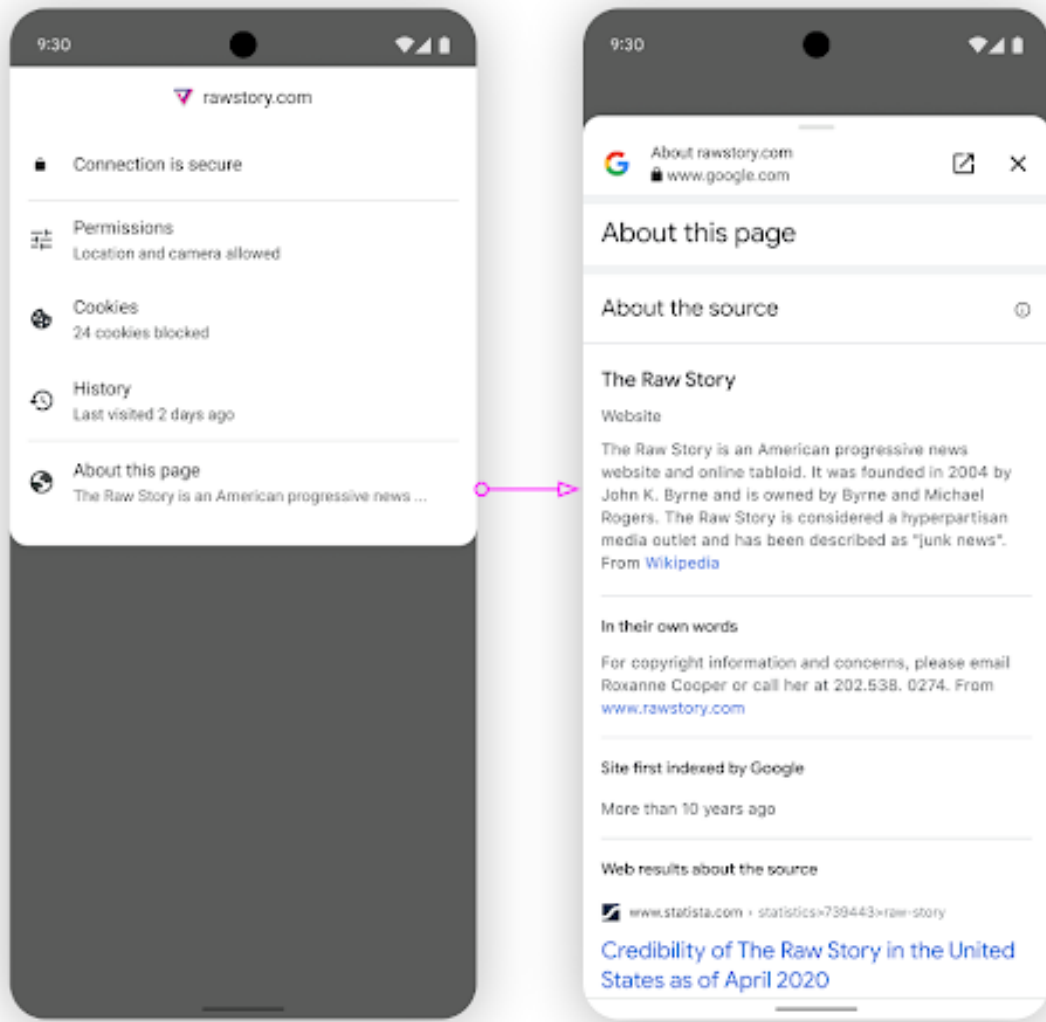
Enhanced Safe Browsing Google accounts integration on desktop

For Chrome on desktop where the Safe Browsing protection level is not controlled by the SafeBrowsingProtectionLevel policy, users who are signed in and syncing, and have enabled **Safe Browsing > Enhanced protection** on their Google Account are notified that **Enhanced protection** is also enabled on their Chrome profile. Similarly, when a user disables **Safe Browsing > Enhanced protection** on their Google Account, it is disabled for their Chrome profile too.

ForceBrowserSignIn policy requires EnableExperimentalPolicies on Linux

Starting in Chrome 105, you can only enable ForceBrowserSignIn on Linux if you also set EnableExperimentalPolicies to true.

ForceBrowserSignIn has never been officially supported on Linux, as per its documentation. However, prior to Chrome 105, it was possible to set it on Linux. This update is part of an ongoing effort to reduce Chrome's binary size and to more strictly adhere to Chrome's documented behavior.

A future release of Chrome will add **Force users to sign-in to use the browser** support to the BrowserSignIn policy on Linux. Once this is complete, ForceBrowserSignIn will not function on Linux, even when EnableExperimentalPolicies is enabled.

Browser Extension Telemetry

When you enable **Safe Browsing > Enhanced protection**, Chrome now collects telemetry information about installed extensions. It also monitors certain activities such as APIs executed and remote hosts contacted. These activities are analyzed on Google servers and further improve the detection of malicious and policy violating extensions. This improvement allows better protection for all Chrome extension users.

New and updated policies in Chrome browser

Policy	Description
PolicyAtomicGroupsEnabled	Enables the concept of policy atomic groups.
PolicyListMultipleSourceMergeList	Allow merging list policies from different sources (now also available on iOS).
PolicyDictionaryMultipleSourceMergeList	Allow merging dictionary policies from different sources (now available on Android and iOS).
PolicyScopeDetection	Allow policy scope detection on macOS.

ChromeRootStoreEnabled	Determines whether the Chrome Root Store and built-in certificate verifier will be used to verify server certificates.
ComponentUpdatesEnabled	Enable component updates in Google Chrome (now available on Android and iOS).
CloudUserPolicyOverridesCloudMachinePolicy	Allow user cloud policies to override Chrome Browser Cloud Management policies (now available on iOS).
EventPathEnabled	Re-enable the Event.path API (available until Chrome 115).
WebSQLNonSecureContextEnabled	Force WebSQL in non-secure contexts to be enabled (available until Chrome 110).
EnterpriseAuthenticationAppLinkPolicy	External authentication app launch URLs (Android Webview).
EncryptedClientHelloEnabled	Enable TLS Encrypted ClientHello.

ChromeOS updates

Adaptive charging to extend battery life

Adaptive charging helps to extend your battery's lifespan by understanding how you use your device and optimizing charging accordingly. This new feature analyzes your device usage patterns and keeps your battery working in the optimal charge range to avoid overcharging thereby delaying battery deterioration.

Close a desk and its windows in one click

Create a desk for each project or task and when you're done, close the desk and all its tabs and windows with a single click. Access this feature by hovering over a desk in the deskbar and selecting **Close desk and windows**.

Admin console updates

Group-based policy for apps & extensions

Admins can configure app & extension permissions for their organizations using Google groups in addition to organizational units. If you want to install an app for a small number of users–who might belong to different organizational units–you can now add those users to a group instead of moving them into a different organizational unit. Note that apps & extensions policies for groups take precedence over those set for organizational units, so if a user belongs to both a group and an organizational unit where you have a policy set, they follow the permissions set for their group rather than their organizational unit. Also note that you are only able to add users to Google groups at this time. Learn more.
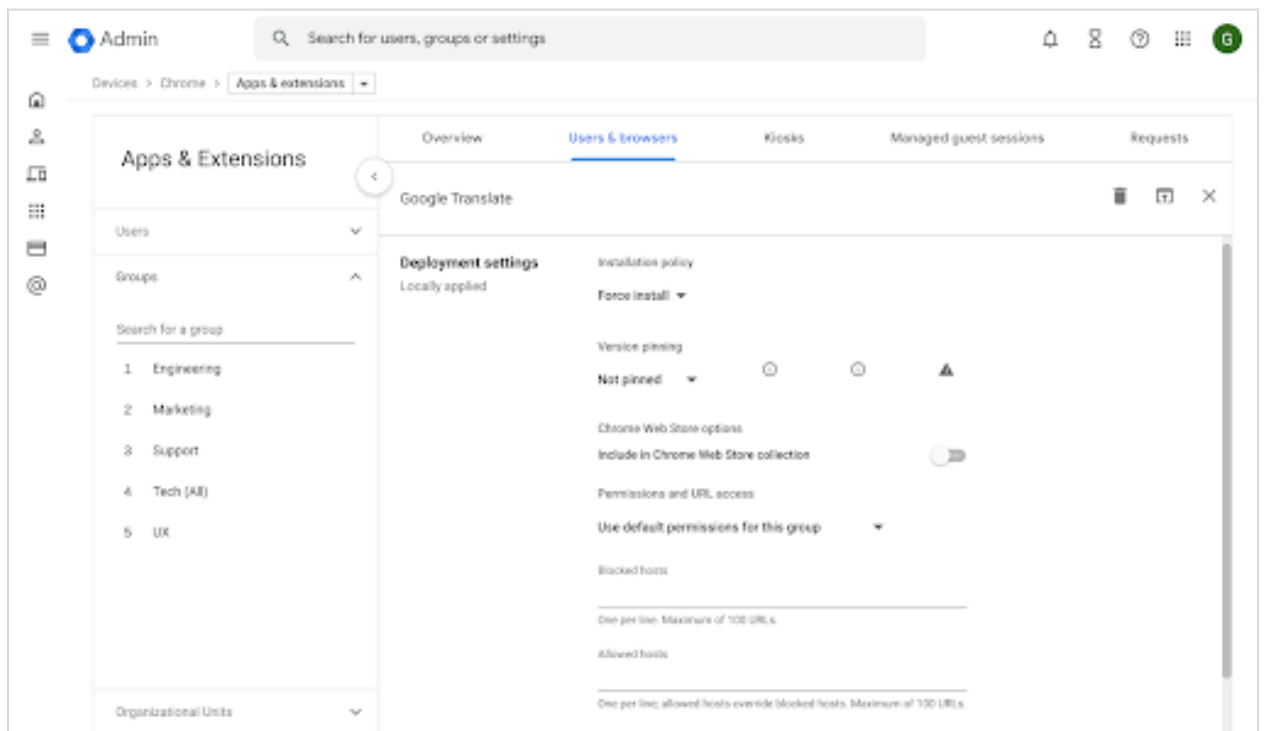
Configure alerts for extension requests

You can now configure alerts for extension requests by creating reporting or activity Rules. Follow the steps listed in this help center article.

Browser Details: Installed apps & extensions UX changes

In the Browser Details page, there is an **Installed apps & extensions** card. When the user clicks on an app, a new page opens up—the App Details page. Previously, an overflow menu allowed admins to take a limited set of actions and now admins can set policy in the App Details page.

Browser Details:

App Details:

New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
RendererAppContainerEnabled	User & Browser Settings	Chrome	Security > Renderer App Container
UnthrottledNestedTimeoutEnabled	User & Browser Settings; Managed Guest Session	Chrome ChromeOS Android	Content > Javascript setTimeout() clamping
ChromeAppsEnabled	Additional App Settings	Chrome	Additional application settings > Extend support for Chrome Apps

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

Support for Encrypted Client Hello (ECH)

As early as Chrome 106, Chrome will start rolling out support for ECH on sites that opt-in, as a continuation of our network related efforts to improve our users' privacy and safety on the web, for example, Secure DNS. There is an enterprise policy available to disable ECH, also available in Chrome 105.

If your organization's infrastructure relies on the ability to inspect SNI, for example, filtering, logging, and so on, you should test it with Chrome 106. If you encounter any

incompatibilities, you will be able to use the [EncryptedClientHelloEnabled](#) enterprise policy to disable support for ECH.

Changes to chrome.runtime

Chrome 106 will include a change that causes `chrome.runtime` to no longer be defined unconditionally on all sites. In contexts where there is no connectable extension, websites should never expect `chrome.runtime` to be defined.

Over the past couple of months, we have taken steps to remove Chrome's legacy U2F security API. This API was implemented in an internal Chrome extension called CryptoToken, which by design was externally connectable from all URLs. The presence of this extension meant that `chrome.runtime` was effectively always defined on any web origin, because there was always at least one extension to connect to, even if the user installed no other connectable extensions. As part of the U2F removal process, Chrome 106 stops loading CryptoToken by default, which means that `chrome.runtime` will now be undefined in contexts where there is no other connectable extension.

Websites should never assume that `chrome.runtime` is defined unconditionally. As a temporary workaround, the effects of this change can be reversed by enabling the `chrome://flags/#load-cryptotoken-extension` flag or an upcoming enterprise policy named **LoadCryptoTokenExtension**.

Persistent quota deprecation launch

In Chrome 106, [window.PERSISTENT](#) quota type in `webkitRequestFileSystem` will no longer be supported. `webkitRequestFileSystem` will still accept a `type` parameter and use of the PERSISTENT and TEMPORARY types will create file systems with separate roots, but the PERSISTENT type will no longer grant access to a persistent file system.

**Chrome will show Journeys on the History page on Android**

Chrome 96 started clustering local browsing activity on the History page into Journeys to make it easier to find prior activity and continue it with related search suggestions. This feature will also become available on Android as early as Chrome 106. For keywords typed into the Omnibox that match a cluster, an action chip displays for seamless access to the Journeys view. Users can delete clusters and disable Journeys, if desired. Additionally, admins will have the option to disable this feature using the HistoryClustersVisible policy.

Incognito lock on Android

Chrome 106 will introduce an option for users on Android 11 and later to require authentication when resuming an Incognito session. The feature will be OFF by default. It can be turned ON using the new **Lock Incognito tabs when you leave Chrome** toggle under **Settings > Privacy & Security**. This feature will not be available on managed devices where the IncognitoModeAvailability enterprise policy is set to *Disabled*.

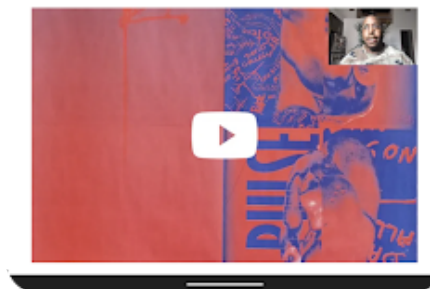**Incognito downloads prompt on Android**

When a user initiates a download while browsing on an Incognito tab, they will see a new informative prompt. Users have the option to dismiss the prompt or tap **Download** to go ahead and save the file. Files downloaded on Incognito will continue to be accessible through the download manager.
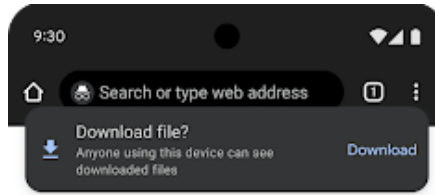
Network Service on Windows will be sandboxed

As early as Chrome 107, 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.

Removal of window.webkitStorageInfo

As early as Chrome 107, `window.webkitStorageInfo API` will be removed. This legacy quota API has been deprecated since 2013, and has been replaced by the now standardized StorageManager API.

Removal of master_preferences

master_preferences and initial_preferences are ways of setting default preferences for a Chrome install. The historical name of the file is *master_preferences*, but it was renamed to *initial_preferences* in Chrome 91. To make the transition easy for IT admins, from Chrome 91 to Chrome 106, naming the file either *initial_preferences* or *master_preferences* has the same effect. In Chrome 107, if you name the file *master_preferences*, it will not work by default. You should rename the file *initial_preferences*.

Alternatively, you will be able to use the **CompatibleInitialPreferences** enterprise policy to extend support for the *master_preferences* naming. This policy is not currently available..

User-Agent reduction Phase 5

As of Chrome 107, some portions of the User-Agent string will be reduced on desktop. As previously detailed in the Chromium blog, we intend to proceed with Phase 5 of the User-Agent reduction plan. The `<platform>` and `<oscpu>` tokens, parts of the User-Agent string, are reduced to the relevant `<unifiedPlatform>` token values, and will no longer be updated. Additionally, the values for `navigator.platform` are frozen on desktop platforms (see this Chromium update).

The UserAgentReduction policy will allow for opting out of these changes.

Automated password changes on Desktop

Chrome 107 will use the Google Assistant to help users change passwords that have been compromised. This reduces friction in updating passwords to help keep users safe. A policy will be available to control the Google Assistant directly, allowing you to enable password leak detection without the Google Assistant assisting in changing passwords.

Chrome sends Private Network Access preflights for subresources

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 (more details here).

In Chrome 107 at the earliest, the warnings will turn into errors and affected requests will fail. 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.

Marshmallow deprecation for Chrome on Android

Chrome 106 is the last version that will support Android 6.0 Marshmallow. From Chrome 107 and onwards, the minimum version supported is Android 7.0 Nougat.

Upcoming ChromeOS changes

ChromeOS Accessibility settings improvements

As early as ChromeOS 106, we will include new improvements to our accessibility settings, including improved search results, easier to understand feature descriptions, and improved layout for better discoverability of accessibility features.

Photos integrations

As early as ChromeOS 106, Chromebook users will get access to enhanced video editing features from Google Photos. The experience is optimized for a larger screen, and will seamlessly integrate with the built-in Gallery app and your Chromebook files – so you can use local images and clips recorded on your Chromebook camera or stored in your Files app to build your movie. While movie editing typically comes with a steep learning curve, the revamped movie creation tools in Google Photos help you make high-quality movies with just a few taps using your video clips and photos. You'll be able to create beautiful movies from suggested themes, or put yourself in the director's seat and start from scratch, right on your Chromebook.

Cursive pre-installed for Enterprise and Education accounts
As early as ChromeOS 106, [Cursive](#) is a stylus-first notes app for Chromebooks. In an upcoming release, it will be pre-installed for all Enterprise and Education accounts on stylus-enabled Chromebooks.

Long-press diacritics

The Essential Inputs team is planning to launch improvements to diacritic typing by including a key press functionality that showcases a new accent menu. This accent menu reveals diacritical marks associated with characters when the user presses and holds a key down on

key characters with diacritics. Users will then have the option to select and insert a diacritic character or close the menu without selection. Look out for this upcoming feature in ChromeOS 106.

Fast Pair

Fast Pair makes Bluetooth pairing easier on ChromeOS devices and Android phones. When you turn on your Fast Pair-enabled accessory, it automatically detects and pairs with your ChromeOS device or Android phone in a single tap. Fast Pair also associates 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 108.

Passpoint: Seamless, secure connection to Wi-Fi networks

Starting as early as ChromeOS 108, 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 104: August 2, 2022	PDF
Chrome 103: June 21, 2022	PDF
Chrome 102: May 26, 2022	PDF
Chrome 101: April 26, 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 and features planned for upcoming releases.

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.