Chrome 107 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 October 25, 2022.

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

Chrome 107 release summary

Chrome browser updates	Security/ Privacy	User productivity /Apps	Management
Support for Encrypted Client Hello (ECH)	✓		
User-Agent reduction Phase 5	✓		
Marshmallow deprecation for Chrome on Android	✓		
BuiltinCertificateVerifierEnabled removed on Mac			✓
Updates to Incognito Mode		✓	
A redesign for browser downloads		✓	
Password import for Chrome Desktop			✓
Sync after sign-in intercept	✓		✓
Updated Media picker on Android		✓	
Automatic revocation of disruptive notifications		✓	
DisplayCapturePermissionsPolicyEnabled policy removed			✓
New and updated policies in Chrome browser			✓
ChromeOS updates	**Security/ Privacy**	**User productivity /Apps**	**Management**
Camera Framing		✓	
Files app: Improved filtering in Recent tab		✓	
Lock device on lid close		✓	
3P Identity Provider: Autofill username	✓	✓	
Deprecate Assistant stylus features		✓	

Saved desks		✓	
Close a desk and its windows in one click		✓	
Photos integrations		✓	
Long-press to add accents		✓	
ChromeOS Accessibility settings improvements		✓	✓
Multi-touch virtual keyboard		✓	
Admin console updates	**Security/ Privacy**	**User productivity /Apps**	**Management**
Managed browser list: CSV export limit increased to 150,000 records			✓
Admin console: Extension request card			✓
Text action buttons instead of icons in Device and Browser lists			✓
New policies in the Admin console			✓
Upcoming Chrome browser changes	**Security/ Privacy**	**User productivity /Apps**	**Management**
Change Async methods to Sync in FileSystemSyncAccessHandle		✓	✓
As early as Chrome 108, Chrome will change the UI for some download warnings.	✓	✓	
Password Manager: Updates on iOS	✓		
Password Manager: Notes for Passwords	✓		
Windows: Pin to taskbar during install		✓	
Removal of master_preferences			✓
Device token deletion			✓
Rolling out GPU changes to NaCL Swapchain and	✓		

video decoding			
Strict MIME type checks for Worker scripts	✓		
Chrome sends Private Network Access preflights for subresources	✓		
Default to origin-keyed agent clustering in Chrome 109	✓		
Intent to deprecate and remove: Event.path	✓		
MetricsReportingEnabled policy will be available on Android in Chrome			✓
Windows 10 minimum required version in Chrome 110			✓
Network Service on Windows will be sandboxed	✓		
Chrome apps no longer supported on Windows, Mac, and Linux		✓	✓
Deprecation of Web SQL and other old storage features	✓		
Extensions must be updated to use Manifest V3	✓		
Upcoming ChromeOS changes	**Security/ Privacy**	**User productivity /Apps**	**Management**
Fast Pair		✓	
Passpoint: Seamless, secure connection to Wi-Fi networks	✓	✓	
ChromeOS Camera App: Document scanning improvements		✓	
Cursive pre-installed for Enterprise and Education accounts		✓	
Super Resolution Audio for Bluetooth headset microphones		✓	
Channel labeling on ChromeOS		✓	

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

Support for Encrypted Client Hello (ECH)

Chrome 107 starts 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.

If your organization's infrastructure relies on the ability to inspect SNI, for example, filtering, logging, and so on, you should test it. You can enable the new behavior by navigating to `chrome://flags` and enabling the `#encrypted-client-hello` flag. On Windows and Linux, you also need to enable Secure DNS for the flag to have an effect.

If you encounter any incompatibilities, you can use the EncryptedClientHelloEnabled enterprise policy to disable support for ECH.

User-Agent reduction Phase 5

User-Agent (UA) reduction describes the effort to minimize the identifying information shared in the User-Agent string which might be used for passive fingerprinting. Beginning in Chrome 107, Chrome reduces some portions of the User-Agent string on desktop devices. 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 are no longer updated. Additionally, the values for `navigator.platform` are frozen on desktop platforms. For more details, see this reference page and Chromium update.

The UserAgentReduction policy allows for opting out of these changes.

**Marshmallow deprecation for Chrome on Android**

Chrome 106 is the last version that supports Android 6.0 Marshmallow. From Chrome 107, the minimum version supported is Android 7.0 Nougat.

BuiltinCertificateVerifierEnabled removed on Mac

In Chrome 107, we have removed the BuiltinCertificateVerifierEnabled policy on Mac. This policy was used to control the use of the built-in certificate verifier while using the platform provided root store. Since Chrome 105, a new implementation is available that uses the built-in certificate verifier with the Chrome Root Store. You can control the new implementation using the ChromeRootStoreEnabled policy.

Updates to Incognito mode on iOS

Users can configure Chrome to open external links in Incognito using **Settings** > **Privacy and Security** > **Ask to open links from other apps in Incognito**. If you use the IncognitoModeAvailability policy to disable or to force Incognito mode, the policy setting takes precedence, and this user setting won't be available.
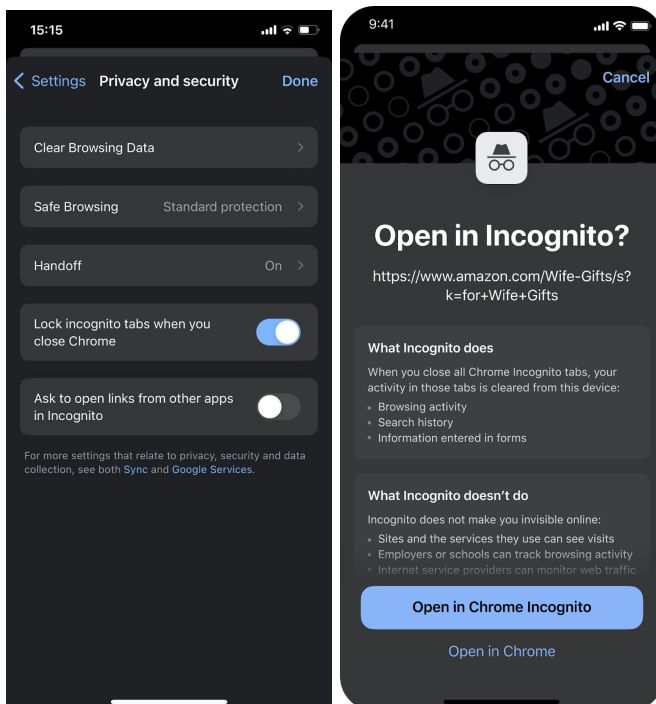
A redesign for browser downloads

In Chrome 107, remaining users now see a redesigned downloads experience for desktop that moves downloads into a secondary UI surface, following an initial rollout in Chrome 102. The new download tray stems from the trusted UX of Chrome and allows for more effective warnings to better protect users. If you need extra time to adjust to this change, the DownloadBubbleEnabled enterprise policy will be available to temporarily keep the old behavior.
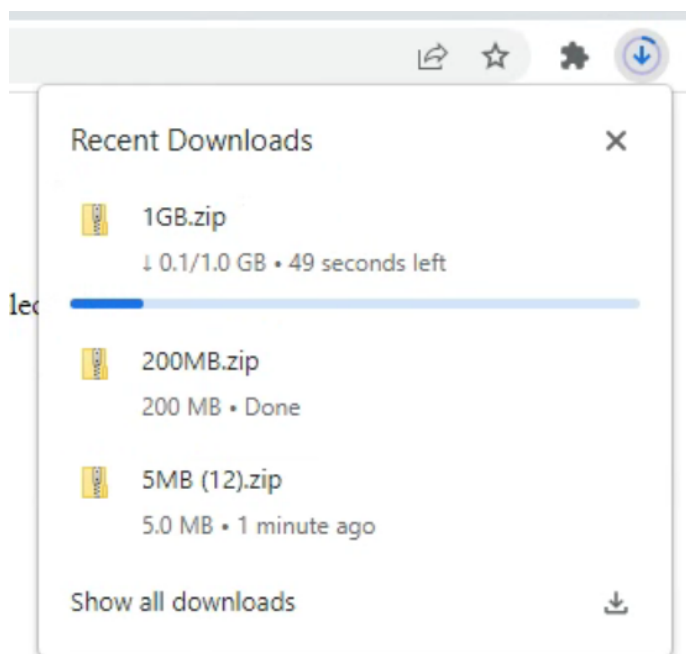

Password import for Chrome Desktop

Starting in Chrome 107 Desktop users can import their passwords using Chrome browser. Previously, users were only able to import via `passwords.google.com`. They can now upload a CSV file of passwords to add them to their saved passwords in Google **Password Manager**. If the user has sync enabled, their passwords are available across their devices, where they are signed in with the same account.

Sync after sign-in intercept

To provide a more consistent experience, Chrome now shows a new welcome screen after the user creates a new profile through the sign-in intercept. The user can optionally enable sync as well as modify the new profile name and theme color. The sign-in intercept bubble now contains an enterprise disclaimer if a new profile is to be managed by an organization. This also modifies the signed-out profile creation experience for consistency with other flows.

Enterprise administrators can disable the welcome dialog by setting the PromotionalTabsEnabled policy to false.
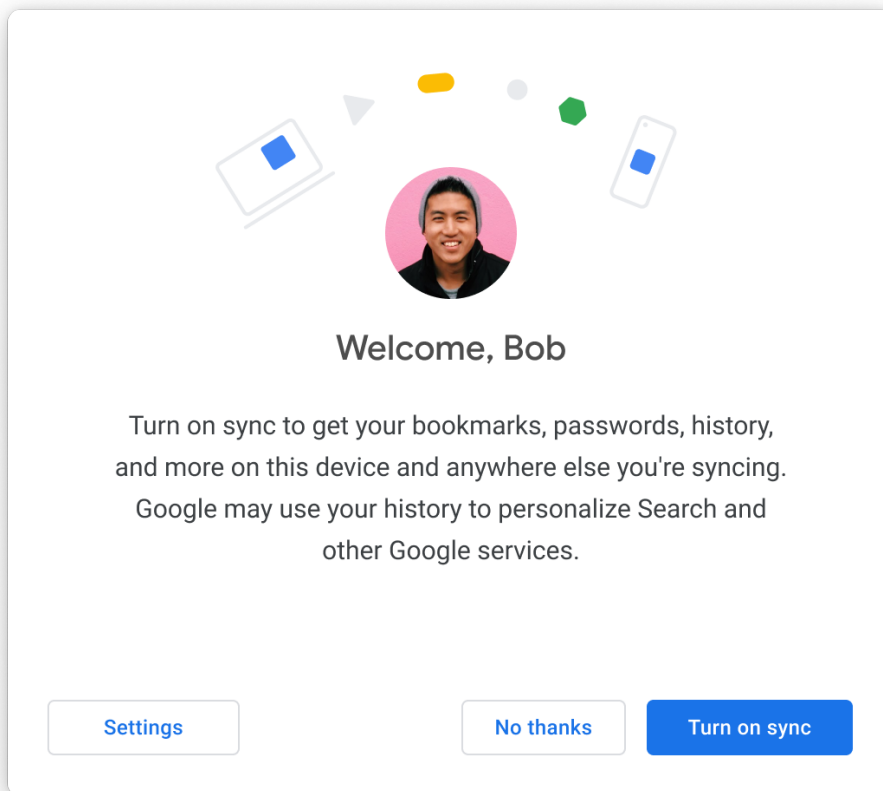
Updated Media picker on Android

Some users see the new Android Media Picker instead of Chrome's native Media Picker, when uploading photos and videos to the web.
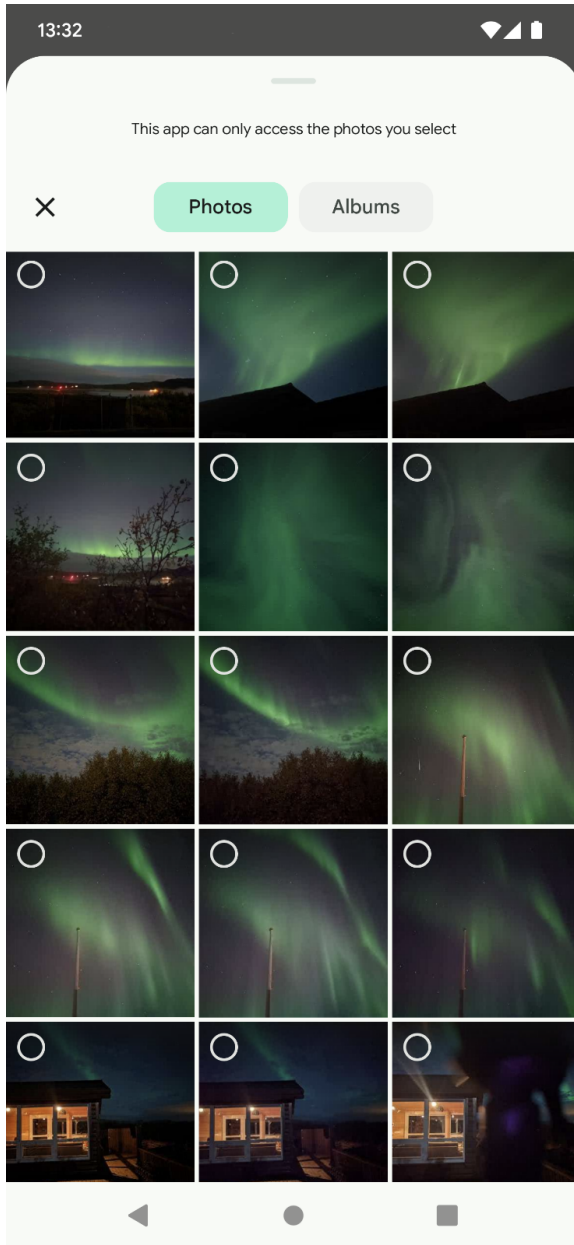
Automatic revocation of disruptive notifications

Some notification prompts and messages are increasingly disruptive for users. Chrome automatically removes the notification grant for sites that send such notifications to users, as these sites are violating Google's Developer Terms of Service. These sites also have subsequent notification prompts muted.

Any sites listed in the [NotificationsAllowedForUrls](#) enterprise policy do not have their notification permissions revoked.

DisplayCapturePermissionsPolicyEnabled policy removed

The display-capture permissions-policy controls access to the `getDisplayMedia()` method, in accordance with the [Screen Capture W3 specification](#).

In Chrome 94, we introduced `display-capture` as well as the enterprise policy, [DisplayCapturePermissionsPolicyEnabled](#), for bypassing it. Chrome 107 removes this enterprise policy, so it is no longer possible to bypass the `display-capture` permissions-policy.

New and updated policies in Chrome browser

Policy	Description
[HistoryClustersVisible](#)	Show Journeys on the Chrome history page, available on Android.
[AssistantWebEnabled](#)	Allow using Google Assistant on the web, for example, to enable changing passwords automatically.
[StrictMimetypeCheckForWorkerScriptsEnabled](#)	Enable strict MIME type checking for worker scripts.
ShoppingListEnabled	This policy controls the availability of the shopping list feature.

ChromeOS updates

Camera Framing

Camera Framing provides automatic zooming and centering of the user's face for video conference calls or taking selfies. If the device or camera supports Camera Framing, there's a prompt and an option in Quick Settings to enable or disable the feature. To center yourself again, simply toggle the feature off and back on.

Files app: Recent tab improvements

It's now faster and easier to find your recently used files. The **Recent** tab in the **Files** app has been split into time periods, and has a new *Document* filter.

Lock device on lid close

Settings now supports locking a device when the lid closes without suspending. This can be helpful if you have background tasks such as an SSH connection and don't want them to be paused. The existing settings for **Show lock screen when waking from sleep** now also apply to lock the screen when closing the lid.

On an enterprise level, admins can set **Action on lid close** to *Do nothing*, by setting the [LidCloseAction](#) policy to *3 = Do nothing*, and set **Lock screen on sleep or lid close**, by setting the [ChromeOsLockOnIdleSuspend](#) policy to true. With these settings, devices lock when the lid is closed except if they are docked and using an external monitor. In such a case, the device does not lock when the lid closes, but it locks if the external monitor is removed and the lid is still closed.

After locking, the device sleeps if configured to do so after an idle timeout, determined by the [PowerManagementIdleSettings](#) policy. If wake locks are allowed and an application holds a wake lock, with the [AllowWakeLocks](#) policy, the device does not sleep, which significantly affects battery consumption.

3P Identity Provider: Autofill username

With ChromeOS 107, we improve the online login flow for Chrome Enterprise and Education users that authenticate with Azure AD or Okta. Admins can activate the [DeviceAutofillSAMLUsername](#) policy to ensure that users no longer have to re-enter their username when authenticating with a third-party identity provider (3P IdP).

Deprecate Assistant stylus features

ChromeOS 107 deprecates stylus features on Pixelbooks related to the Assistant *what's on my screen* query. The Assistant option is no longer available on the stylus palette tool and stylus long press actions no longer trigger the Assistant screen selection mode.

Saved desks

You can now save and close an entire virtual desk, including all its app windows and their layout — perfect for when you want to switch gears or focus on a different task. When you're ready to get back to it, you can open your saved desk and all its windows and tabs with a single click.

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. To access this feature, hover the cursor over a desk in the deskbar and select **Close desk and windows**.

Photos integrations

As early as Oct 3rd, Chromebook users get access to enhanced video editing features from Google Photos. The experience is optimized for a larger screen, and seamlessly integrates 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. Starting in Q4 2022, you can create beautiful movies from suggested themes, or put yourself in the director's seat and start from scratch, right on your Chromebook.

Long-press to add accents

In ChromeOS 107, users with an English (en) hardware keyboard can hold a key to type an accented version or variant of that letter. For example, hold the **e** key to see a list of accents, such as **è** in *caffè* or **é** in *déjà vu*.

ChromeOS Accessibility settings improvements

Starting in ChromeOS 107, we include improvements to our accessibility settings, including improved search results, easier to understand feature descriptions, and improved layout for better discoverability of accessibility features.

Multi-touch virtual keyboard

We've made some under-the-hood improvements to the virtual keyboard to allow for better handling of multiple fingers simultaneously tapping keys. It is now faster to type on, especially for touch typists.

Admin console updates

**Managed browser list: CSV export limit increased to 150,000 records**

The CSV export limit on the Managed browser list increases from 5,000 records to 150,000. This means that you can now download the data of a maximum of 150,000 browsers in one CSV file.

Admin console: Extension request card

As early as Chrome 107, the list of extension requests that were previously shown in the right panel sidebar are now shown in a card in the **App Details** page.

Text action buttons instead of icons in devices and browsers lists

Chrome devices and browsers lists now show text actions instead of icons.
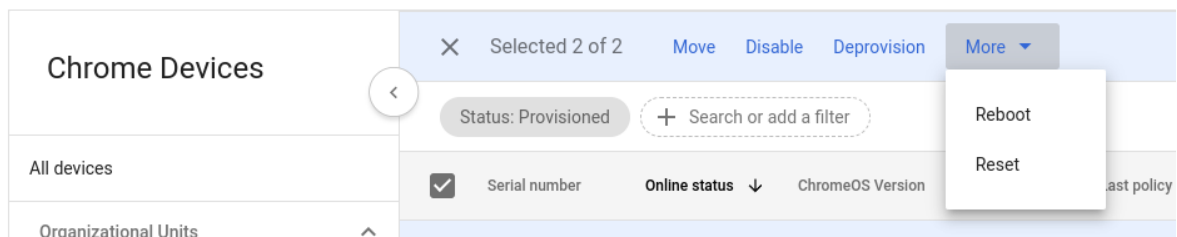
New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
[BlocklistedHexSSIDs](#)	Networks Settings	ChromeOS	General settings > Block SSIDs
[PasswordDismissCompromisedAlertEnabled](#)	User & Browser Settings	Chrome ChromeOS	Security > Compromised password alerts
[WebAuthnFactors](#)	User & Browser Settings	ChromeOS	Security > WebAuthn
[DeviceAutoUpdateP2PEnabled](#)	Device Settings	ChromeOS	Device updates > Auto-update settings > Allow peer to peer auto update downloads

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

### Change Async methods to Sync in FileSystemSyncAccessHandle Launch

In Chrome 108, `getSize()`, `truncate()`, `flush()` and `close()` async methods in `FileSystemSyncAccessHandle` primitive in the File System Access API will be converted to synchronous methods, in line with `read()` and `write()` methods.

This change supports a fully synchronous API for `FileSystemSyncAccessHandle`, enabling high performance for WebAssembly (WASM) based applications.

An enterprise policy, **FileSystemSyncAccessHandleAsyncInterfaceEnabled**, will be available until Chrome 110 to enable the async methods.

As early as Chrome 108, Chrome will change the UI for some download warnings

To protect users from malware, Chrome will start to show detailed context and customized UIs for some download warnings. For example, if Chrome detects a download to potentially steal user's information, the description will be changed 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 allowlist specific domains using SafeBrowsingAllowlistDomains.
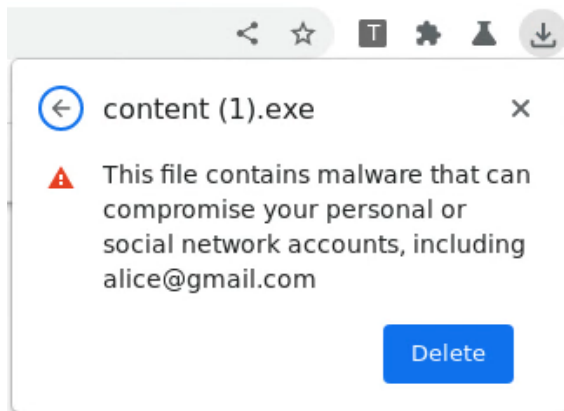

Password Manager: Updates on iOS

From Chrome on iOS 108, we will make it easier for users to access their passwords. The password list view will be simplified, to show users just their passwords. Password-related settings will be moved to their own screen, making it easier for users to see and manage their settings in one place. Existing features like adding or editing passwords and password checkup will remain available on the password list view.

Password Manager: Notes for Passwords

From Chrome for Desktop 108, you will be able to save a note for each saved credential in the password manager. Passwords (and notes) will move to a sub-page and will no longer be accessible from the eye icon on the Password List View, as part of this change. You will now need to re-authenticate before accessing the sub-page.

Windows: pin to taskbar during install

As early as Chrome 108, the Chrome installer will pin Chrome to the Windows taskbar for easier access to Chrome. You will be able to use the `do_not_create_desktop_shortcut` setting in [initial_preferences](#) to control this behavior.
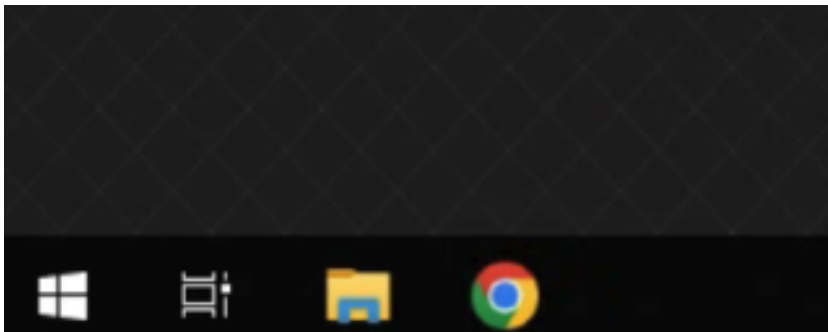
Removal of master_preferences

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 107, naming the file either *initial_preferences* or *master_preferences* has the same effect. In Chrome 108, 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.

Device token deletion

As early as Chrome 108, when deleting a browser from the managed browsers list in the Admin console, a new policy will allow Chrome Browser Cloud Management to delete the device token on the end-point devices. The default value will remain to invalidate the device token.

Rolling out GPU Changes to NaCL Swapchain and video decoding

As early as Chrome 109, 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.

Strict MIME type checks for Worker scripts

Starting with Chrome 109, 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 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. For more details, see this [blog post](#).

In Chrome 109 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.

Default to origin-keyed agent clustering in Chrome 109

As early as Chrome 109, 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.

Intent to deprecate and remove: Event.path

To improve web compatibility, we will stop supporting the non-standard API `Event.path` as early as Chrome 109. 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 will allow you to extend the lifetime of `Event.path` by an additional 6 milestones.

MetricsReportingEnabled policy will be available on Android in Chrome

As early as Chrome 109, 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.

Windows 10 as minimum required version in Chrome 110

Microsoft ends support for Windows 7 [ESU](#) and Windows 8.1 extended support on January 10, 2023. Chrome 110, tentatively scheduled for release on February 7, is the first version of Chrome which will have a minimum Windows version of Windows 10.

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 111 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 111, 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

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 are partnering with the SQLite team to create an evergreen cross-browser Web SQL replacement. The team is adding a web backend to SQLite, using Emscripten to compile it to WebAssembly and leveraging the new File System Access Handles API as a low-level virtual file interface. We expect this to be ready for use early in 2023. 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 early 2023. An enterprise policy, WebSQLNonSecureContextEnabled, will let Web SQL function in non-secure contexts for a few months past the removal date.

In early 2023, 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.

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 will cease running in Chrome. If your organization is running extensions that use Manifest V2, you must update them to leverage Manifest V3. If you need additional time to adjust to the Manifest V3 transition, you'll be able to extend Manifest V2 support in Chrome using an enterprise policy until 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.

Upcoming ChromeOS changes

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.

ChromeOS Camera App: Document scanning improvements

From M107, document scanning in the ChromeOS Camera App will be automatically downloaded when the user selects it, making it available to more devices including those with Apollo Lake and MT8173 processors. From M108, the document scanning feature will support taking multiple pages and combining them into a single PDF.

Cursive pre-installed for Enterprise and Education accounts

As early as ChromeOS 109, 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.

Super Resolution Audio for Bluetooth headset microphones

Starting in 109, 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.

Channel labeling on ChromeOS

Trying out the latest version of ChromeOS? For users on non-stable channels (Beta, Dev, Canary), starting in 109 you will see which channel you are on in the bottom right. Selecting the time to open quick settings will have a new UI with the device build as well as a button directly to submit feedback.

Previous release notes

Chrome version & targeted Stable channel release date	PDF
Chrome 106: September 27, 2022	PDF
Chrome 105: August 30, 2022	PDF
Chrome 104: August 2, 2022	PDF
Chrome 103: June 21, 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.