Chrome 111 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 March 1, 2023.

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

Chrome 111 release summary

Chrome browser updates	**Security/ Privacy**	**User productivity /Apps**	**Management**
Reminder of change in launch schedule			✓
Privacy Sandbox updates in Chrome 111	✓		
PPB_VideoDecoder(Dev) API removed		✓	
New Chrome sync dialog in Chrome for Desktop		✓	
Payment Handler API requires CSP connect-src	✓		
Out-of-process System DNS Resolution	✓		
Azure AD single sign-on (SSO)	✓		
Web speech recognition API on iOS		✓	
Chrome updater on Windows and Mac serves the most recent 12 versions of Chrome			✓
Policy name changes			✓
Chrome Browser Cloud Management subscription			✓
New and updated policies in Chrome browser			✓
Removed policies in Chrome browser			✓
ChromeOS updates	**Security/ Privacy**	**User productivity /Apps**	**Management**
Fast Pair		✓	
Keyboard shortcuts link in Text app		✓	
Print job origin identification for managed devices			✓
Admin console updates	**Security/ Privacy**	**User productivity**	**Management**

		/Apps	
Configure print server policies with Google groups		✓	
New policies in the Admin console			✓
Upcoming Chrome browser changes	**Security/ Privacy**	**User productivity /Apps**	**Management**
LegacySameSiteCookieBehaviorEnabledForDomainList policy extended			✓
Enable access to WebHID API from extension service workers in Chrome 112		✓	
Unused site permissions module in Safety Check	✓		
Default to origin-keyed agent clustering in Chrome 112	✓		
New Chrome Sync data types available in Takeout in Chrome 112	✓		
Chrome for Testing		✓	
Policy troubleshooting page available on Android		✓	
Risk Assessment card		✓	
Chrome apps no longer supported on Windows, Mac, and Linux		✓	
Auto upgrade mixed content to HTTPS	✓		
Deprecation trial for unpartitioned 3rd party Storage, Service Workers, and Communication APIs	✓		
Launching FastCheckout for Checkout experiences		✓	
Collect additional data for off-store extensions in telemetry reports			✓
Updated onboarding experience		✓	
Changes to phishing protection on Android as early as Chrome 113	✓		
Network Service on Windows will be sandboxed	✓		

Enable access to WebUSB API from extension service workers in Chrome 113		✓	
Extensions must be updated to leverage Manifest V3		✓	✓
First-Party Sets user controls	✓		
Removal ChromeRootStoreEnabled policy			✓
Full History sync		✓	
Removal of permissive Chrome Apps webview behaviors	✓		
Upcoming ChromeOS changes	**Security/ Privacy**	**User productivity /Apps**	**Management**
Cursive pre-installed for Enterprise and Education accounts		✓	
Screencast supports multi-language transcription in recordings		✓	
Passpoint: Seamless, secure connection to Wi-Fi networks	✓	✓	
Upcoming Admin console changes	**Security/ Privacy**	**User productivity /Apps**	**Management**
New Chrome browser insights		✓	✓

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

Reminder of change in launch schedule

Starting in Chrome 110, Chrome started rolling out to the Stable channel one week earlier than previously planned to a very small subset of users. For example, the Chrome 111 Stable release moves from March 7 to March 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 happens at a similar timeframe to the earlier communicated dates. This slower initial rollout leads to better stability and makes it easier for enterprises to stay on the latest and safest version of Chrome.

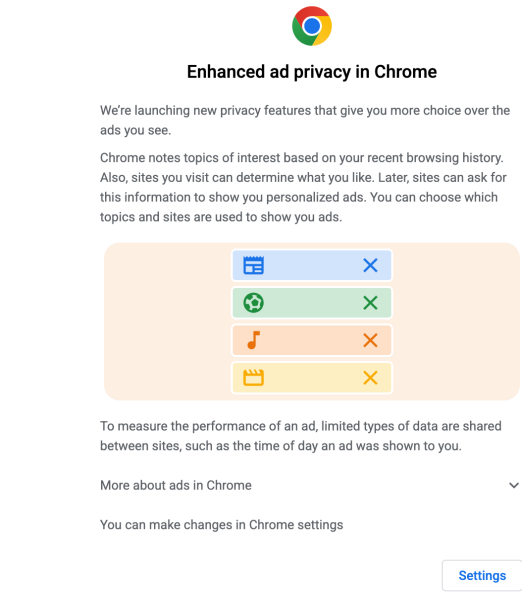
For more details, read about managing Chrome updates and check out the Chrome release schedule.

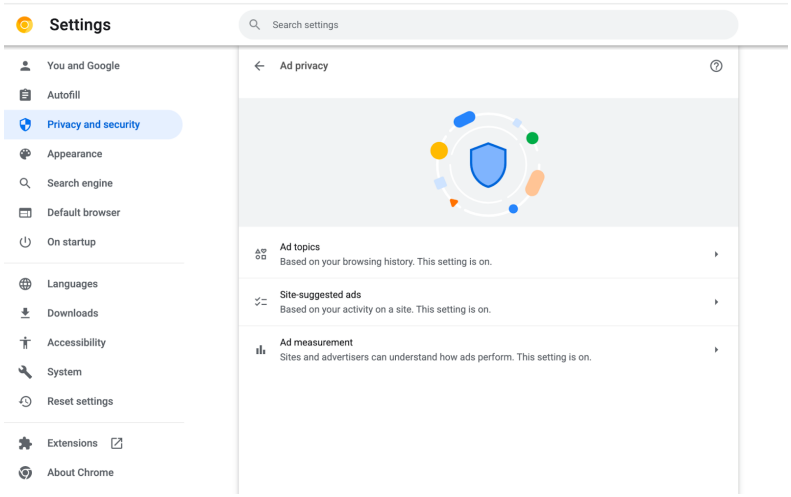
Privacy Sandbox updates in Chrome 111

Chrome 111 updates the user experience of the new ad privacy features related to the Privacy Sandbox project. As part of this, Chrome now shows users a confirmation dialog that introduces the new features to users, and directs them to the appropriate settings pages to allow 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.



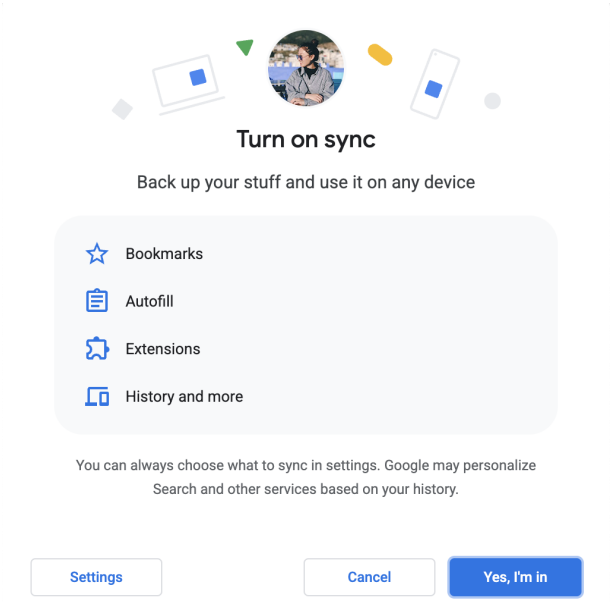


PPB_VideoDecoder(Dev) API removed

The PPB_VideoDecoder(Dev) API was introduced for Adobe Flash. Since Flash is no longer supported in Chrome, we are removing this API in Chrome 111. If you need any extra time to migrate legacy applications, you can use the ForceEnablePepperVideoDecoderDevAPI enterprise policy. This policy will only be supported through Chrome 114. If you need to use the policy after that, file a bug on crbug.com before May 5, 2023, explaining your use case.

New Chrome sync dialog in Chrome for Desktop

Some users now see a visually updated dialog to turn on Chrome Sync in Chrome 111. Relevant enterprise policies such as BrowserSignin, SyncDisabled, RestrictSigninToPattern and SyncTypesListDisabled continue to work as before to configure Chrome sync.



Payment Handler API requires CSP *connect-src*

If your organization uses the Web Payment API (Payment Handler and Payment Request) and also uses Content-Security-Policy (CSP) for better protection, then you need to add the domains of HTTP requests sent from the Web Payment API to the *connect-src* directive of the CSP. This is enforced in Chrome 111. For more information, see this developer blog post.

Out-of-process System DNS Resolution

Starting gradually in Chrome 111, as part of the Linux and Android network service sandboxes, system DNS resolution moves out of the network service and into the unsandboxed browser process, as system DNS resolution cannot run while sandboxed on these platforms. The Enterprise policy OutOfProcessSystemDnsResolutionEnabled is

available to control this feature. Setting this policy to false causes system DNS resolution to run in the network process rather than the browser process. This might force the network service sandbox to be disabled, degrading the security of Google Chrome.

Azure AD single sign-sn (SSO)

Chrome 111 now supports automatic sign-on into Microsoft identity providers using account information from Microsoft Windows. This feature is disabled by default and can be enabled using the CloudAPAuthEnabled policy.

Web speech recognition API on iOS

On Chrome 111 on iOS, websites can use the Web Speech API for speech recognition-based features. Speech-to-text conversion is performed by Apple servers.

Chrome updater on Windows and Mac serves the most recent 12 versions

The Chrome updater now supports serving versions of Chrome that reached 100% rollout, within the latest 12 releases on the Beta, Stable, and Extended Stable channels. If you're using the TargetVersionPrefix enterprise policy, ensure you are within 12 versions of the latest release. If you don't manually manage Chrome updates, no action is required.

Policy name changes

We've renamed the policies related to *Window Placement*, to better align with the underlying API and permissions, which have recently been renamed to *Window Management*. Starting in Chrome 111, DefaultWindowManagementSetting, WindowManagementAllowedForUrls, WindowManagementBlockedForUrls, WindowManagementSettings policies now supercede the DefaultWindowPlacementSetting, WindowPlacementAllowedForUrls, and WindowPlacementBlockedForUrls policies. The WindowPlacement variants will be removed in a future version. The WindowPlacementSettings atomic group has been renamed to WindowManagementSettings.

Chrome Browser Cloud Management subscription

As early as March 2023, the Chrome Browser Cloud Management (CBCM) subscription will be automatically added to all Admin console accounts who are using CBCM without the subscription. CBCM customers are now required to have the Chrome Browser Cloud Management subscription to use the service. This change adds no new cost to your existing account and there are no actions required.

New and updated policies in Chrome browser

Policy	Description
DomainReliabilityAllowed	Allow reporting of domain reliability related data.
MixedContentAutoupgradeEnabled	Enable mixed content auto upgrading on HTTPS sites.
DefaultWindowManagementSetting	Default Window Management permission setting.
WindowManagementAllowedForUrls	Allow Window Management permission on these sites.
WindowManagementBlockedForUrls	Block Window Management permission on these sites.
OutOfProcessSystemDnsResolutionEnabled	Enable system DNS resolution outside of the network service.
ForceEnablePepperVideoDecoderDevAPI	Enable support for the PPB_VideoDecoder(Dev) API.
CloudAPAuthEnabled	Allow automatic sign-in to Microsoft® cloud identity providers.
PrivacySandboxPromptEnabled	Choose whether the Privacy Sandbox prompt can be shown to your users.
PrivacySandboxAdMeasurementEnabled	Choose whether the Privacy Sandbox ad measurement setting can be disabled.
PrivacySandboxAdTopicsEnabled	Choose whether the Privacy Sandbox Ad topics setting can be disabled.

PrivacySandboxSiteEnabledAdsEnabled	Choose whether the Privacy Sandbox Site-suggested ads setting can be disabled.
GetDisplayMediaSetSelectAllScreensAllowedForUrls (now on Linux)	Enables auto-select for multi screen captures.

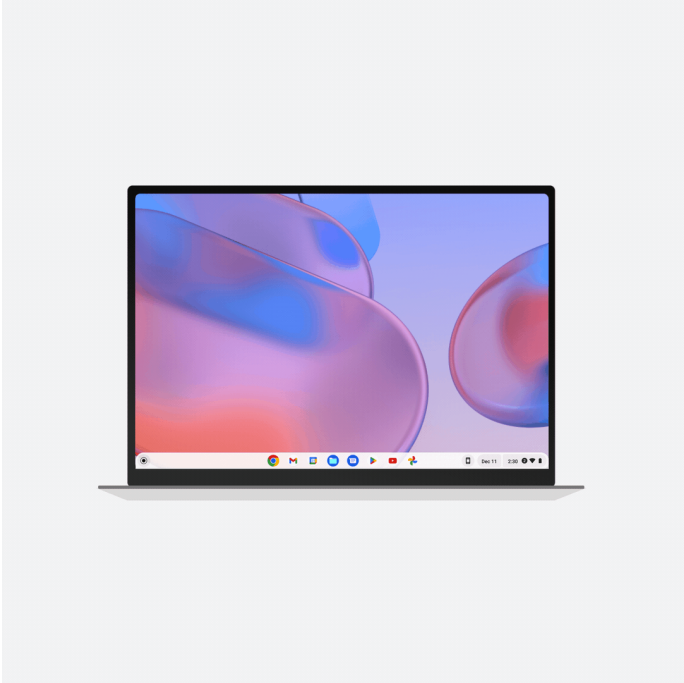
Removed policies in Chrome browser

Policy	Description
FileSystemSyncAccessHandleAsyncInterfaceEnabled	Re-enable the deprecated async interface for FileSystemSyncAccessHandle in File System Access API.

ChromeOS updates

Fast Pair

Fast Pair now 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.



Keyboard shortcuts link in Text app

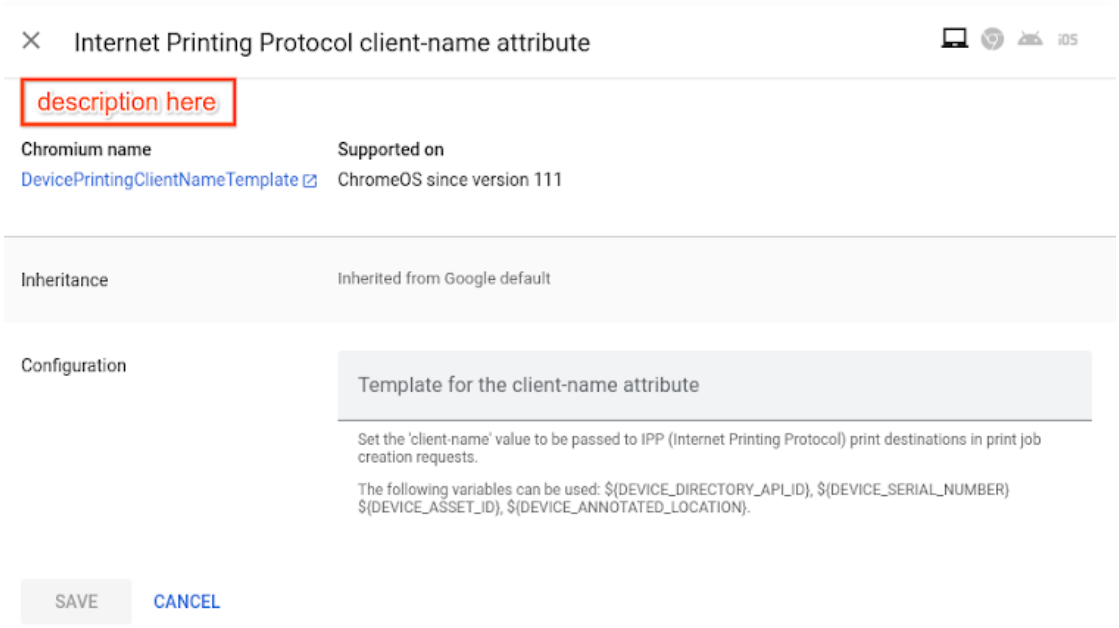
The ChromeOS **Text** app has a series of built-in keyboard shortcuts. ChromeOS 111 adds a link to the Help Center article from the **Text** app settings, to provide instructions on how to use these keyboard shortcuts.

Print job origin identification for managed devices

To improve support for specific advanced printing workflows in managed environments, mostly encountered in the Healthcare space, print jobs need to contain information about the device that they originated from. ChromeOS 111 introduces the *client-info* IPP attribute to populate an admin-specified value, which identifies a device used for downstream printing workflow or reporting activities.

Additionally, all print jobs now indicate *ChromeOS* together with the running release version.

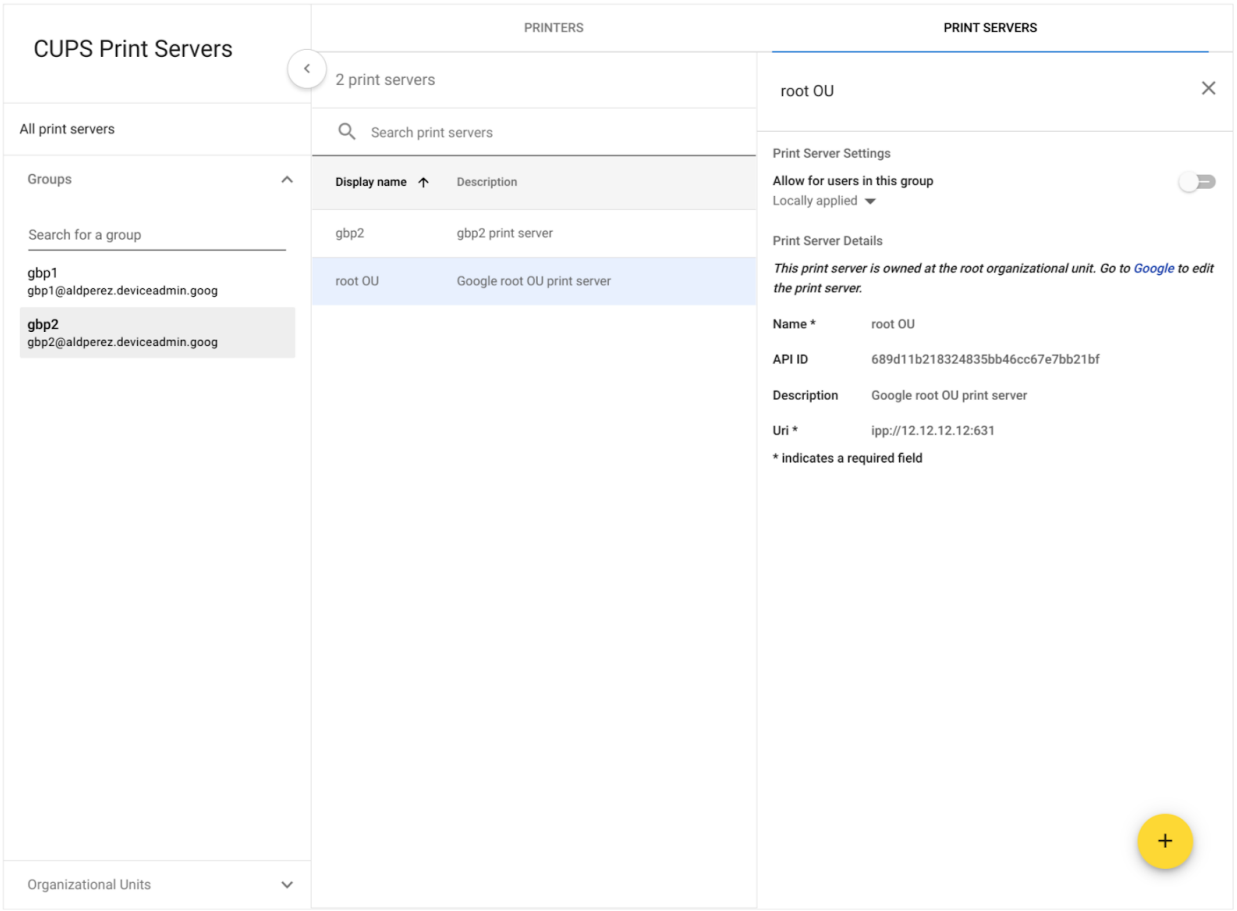
This new attribute in print jobs is only available for jobs originating from managed devices and controlled by a new admin policy.



Admin console updates

Configure print server policies with Google groups

Admins can now use new or existing Google groups to configure print servers for users in your organization. That means when you need to configure a print server for a specific set of users–who may or may not belong to different Organizational Units (OUs)–you can now use the flexibility of groups without needing to reconfigure your OUs. Note that configuration of print server policies for user groups works exactly the same as it does for printers.



New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
LensDesktopNTPSearchEnabled	User & Browser Settings; Managed Guest Session	Chrome ChromeOS	Startup > New Tab Google Lens button
SendMouseEventsDisabledFormControlsEnabled	User & Browser Settings; Managed Guest Session	Chrome ChromeOS Android	Legacy site compatibility > Disabled element MouseEvents
UserBorealisAllowed	User & Browser Settings; Managed Guest Session	ChromeOS	User experience > Allow Borealis on ChromeOS
OffsetParentNewSpecBehaviorEnabled	User & Browser Settings; Managed Guest Session	Chrome ChromeOS Android	Legacy site compatibility > Enable Legacy HTMLElement Offset behavior
AccessControlAllowMethodsInCORSPreflightSpecConformant	User & Browser Settings; Managed Guest Session	Chrome ChromeOS Android	Network > CORS Access Control Allow Methods Conformance

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

LegacySameSiteCookieBehaviorEnabledForDomainList policy extended

In Chrome 79, we introduced the LegacySameSiteCookieBehaviorEnabledForDomainList policy to revert the SameSite behavior of cookies (possibly on specific domains) to legacy behavior. LegacySameSiteCookieBehaviorEnabledForDomainList policy will continue to be supported up until Chrome 121.

Enable access to WebHID API from extension service workers in Chrome 112

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.

Unused site permissions module in Safety Check

In Chrome 112, Safety Check will be expanded to include auto-revocation of unused site permissions on Chrome. Chrome will reset permissions from sites that have low recent engagement. Chrome informs the user about auto-revocation of permissions and offers options to opt out or re-grant. Permissions granted by enterprise policies are not affected. This launch follows the first extension of safety check that introduced proactive notification of permission reminders.

Default to origin-keyed agent clustering in Chrome 112

In Chrome 112, 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. You can read more in the blog post.

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

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

New Chrome Sync data types available in Takeout in Chrome 112

There will be more Chrome data available to export in Takeout and Domain Wide Takeout (DWT). The following data types are available: AUTOFILL, PRIORITY_PREFERENCE, WEB_APP, DEVICE_INFO, TYPED_URL, ARC_PACKAGE, OS_PREFERENCE, OS_PRIORITY_PREFERENCE, PRINTER.

You can control which data types are synced to Chrome Sync using the SyncTypesListDisabled enterprise policy.

Chrome for Testing

In Chrome 112, Puppeteer, Chrome's browser automation library, will start using 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.

Policy troubleshooting page available on Android

`chrome://policy/logs` is a new page that admins will be able to use to help troubleshoot enterprise policies on Android.

Risk Assessment card

In Chrome 112, we're creating a new card in the **Extension details** page, which will show 3rd party risk scores, such as **CRXcavator.io** or **Spin.ai,** for public extensions.

Chrome apps no longer supported on Windows, Mac, and Linux

As previously announced, we are phasing out support for Chrome apps 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

Auto upgrade mixed content to HTTPS on iOS in Chrome 112

Chrome on iOS will start automatically upgrading passive mixed content (HTTP image, audio and video on HTTPS pages) to HTTPS when possible. The current behavior on iOS is to block passive mixed content. All other Chrome platforms already optimistically upgrade passive mixed content. An Enterprise policy MixedContentAutoupgradeEnabled is available to disable mixed content auto upgrading on HTTPS sites on iOS. The policy will be removed in 116.

Deprecation Trial for Unpartitioned 3rd party Storage, Service Workers, and Communication APIs

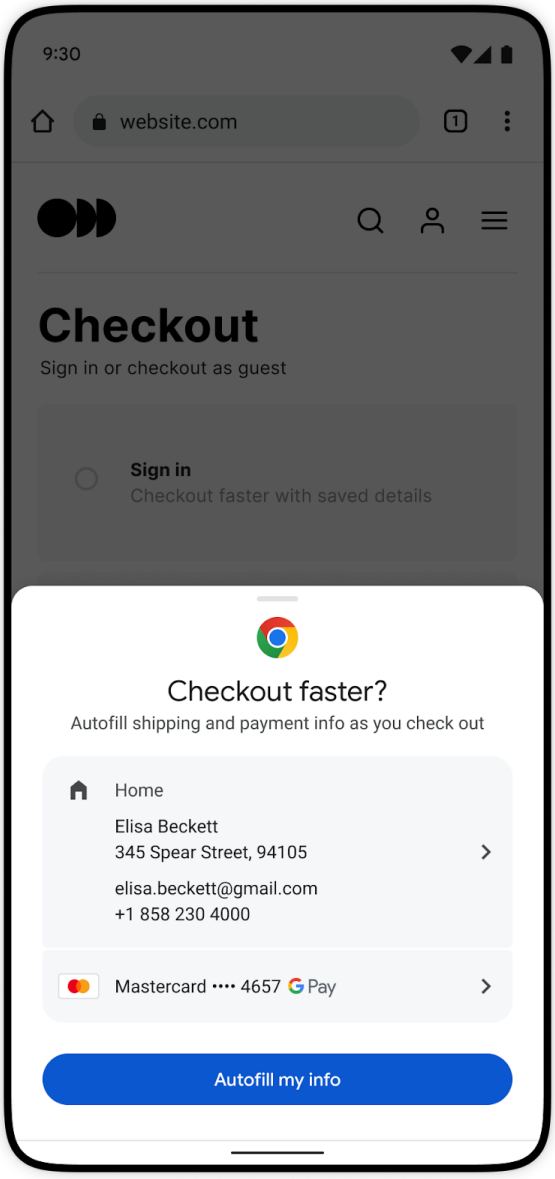
Beginning gradually in Chrome 113, storage, service workers, and communication APIs will be partitioned in third-party contexts. In addition to being isolated by the same-origin policy, the affected APIs used in third-party contexts would also be separated by the site of the top-level context. Sites that haven't had time to implement support for third-party storage partitioning can take part in a deprecation trial to temporarily **unpartition** (continue isolation by same-origin policy but remove isolation by top-level site) and restore prior behavior of storage, service workers, and communication APIs in content embedded on their site.

The following APIs will remain unpartitioned in third-party contexts should you enroll the top-level site in the **DisableThirdPartyStoragePartitioning** deprecation trial: Storage APIs (such as localStorage, sessionStorage, IndexedDB, Quota, and so on), Communication APIs (such as BroadcastChannel, SharedWorkers, and WebLocks), and ServiceWorker API.

Chrome 112 will also add the **ThirdPartyStoragePartitioningEnabled** enterprise policy, which will allow for unpartitioning all APIs in third-party contexts, to be supported for at least 12 milestones.

Launching FastCheckout for Checkout experiences

In Chrome 112, some users will see an updated Autofill UI targeting checkout pages on shopping websites. It can be disabled by either disabling policy AutofillAddressEnabled or AutofillCreditCardEnabled.

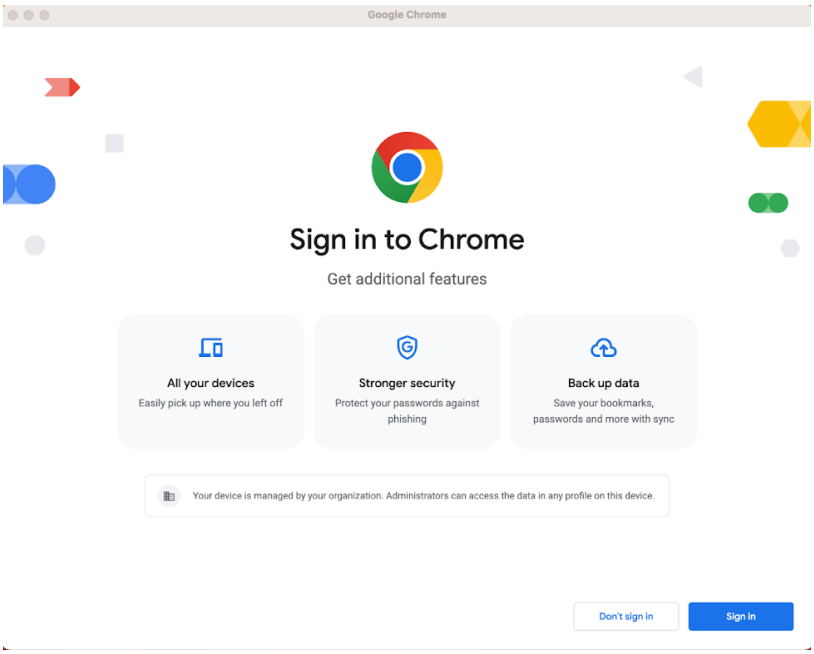


Collect additional data for off-store extensions in telemetry reports

When Enhanced Safe Browsing is enabled, Chrome 112 will start collecting additional telemetry on off-store extensions, such as file hashes and the manifest.json file. The data collected are analyzed on Google servers to detect malicious off-store extensions and improve protection for all Chrome extension users. This functionality along with the entire extension telemetry feature can be turned off by setting SafeBrowsingProtectionLevel to any value other than 2; this disables Enhanced Safe Browsing. Enterprise admins can use the SafeBrowsingProtectionLevel policy if they have any concerns about exposing this data.

Updated onboarding experience

In Chrome 112, some users may see a simplified onboarding experience with a more intuitive way to sign into Chrome. Enterprise policies like BrowserSignin, SyncDisabled, EnableSyncConsent, RestrictSigninToPattern and SyncTypesListDisabled will continue to be available as before to control whether the user can sign into Chrome and turn on sync. The PromotionalTabsEnabled policy can be used to skip the onboarding altogether.



Changes to phishing protection on Android as early as Chrome 113

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.

Network Service on Windows will be sandboxed

As early as Chrome 113, 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.

Enable access to WebUSB API from extension service workers in Chrome 113

As early as Chrome 113, 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.

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.

As mentioned earlier in our blog post, More details on the transition to Manifest V3, the Manifest V2 deprecation timelines are under review and the experiments scheduled for early 2023 are being postponed.

During the timeline review, existing Manifest V2 extensions can still be updated, and still run in Chrome. However, all new extensions submitted to the Chrome Web Store must implement 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.

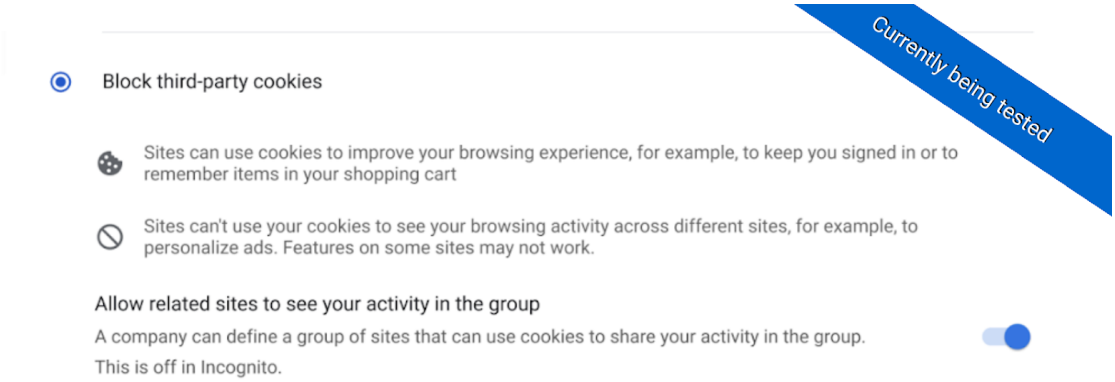
For more details, refer to the Manifest V2 support timeline.

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 113 will introduce user controls for these First-Party Sets. Two enterprise policies will be made available to manage First-Party sets: one to disable First-Party Sets and one to provide your own sets.



Removal ChromeRootStoreEnabled policy

In Chrome 105, we announced the launch of the Chrome Root Store on Windows and Mac. A new policy, called ChromeRootStoreEnabled, was introduced to allow selective disabling of the Chrome Root Store in favor of the platform root store. This policy will be removed from Windows and Mac on Chrome 113. Support for trusted leaf certificates and the Windows Trusted People store was added for Chrome 111. If you previously disabled the Chrome Root Store to work around either of these issues, please test again with Chrome 111. We are working on launching the Chrome Root Store for Android, Linux, and ChromeOS. As the Chrome Root Store launches on more platforms, we will continue to provide the policy on those platforms for six months after launch.

Full History sync

Starting with Chrome 112, Typed URLs will stop syncing for Enterprise users. Open Tabs will continue syncing as usual, unless disabled by existing SyncDisabled and SyncTypesListDisabled policies.

Removal of permissive Chrome Apps webview behaviors

In Chrome 113, Chrome Apps webview usage will have the following restrictions:

1. SSL errors within webview will show an error page that does not provide the user the option to unsafely proceed.

2. The use of the webview NewWindow event to attach to a webview element in another App window will cause the window reference returned by the window.open call in the originating webview to be invalidated.

In Chrome 112, you'll be able to test out this new behavior by navigating to `chrome://flags` and enabling the `chrome://flags/#enable-webview-tag-mparch-behavior`.

A temporary enterprise policy **ChromeAppsWebViewPermissiveBehaviorAllowed** will be available to give enterprises time to address possible breakage related to these changes.

Upcoming ChromeOS changes

Cursive pre-installed for Enterprise and Education accounts

As early as ChromeOS 112, 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*.

Screencast supports multi-language transcription in recordings

As early as ChromeOS 112, we plan to dramatically expand **Screencast** recording capabilities by including a wide range of languages by integrating with Google's **S3** transcription API.

The **Screencast** app for ChromeOS lets users record transcribed screencasts on their Chromebook. In previous versions, this feature was available in EN-US only, which meant that only English speaking users in the US could record screencasts. Soon, it will be possible to record and transcribe screencasts in a wide range of languages including Spanish, Japanese, French, Italian, and German.

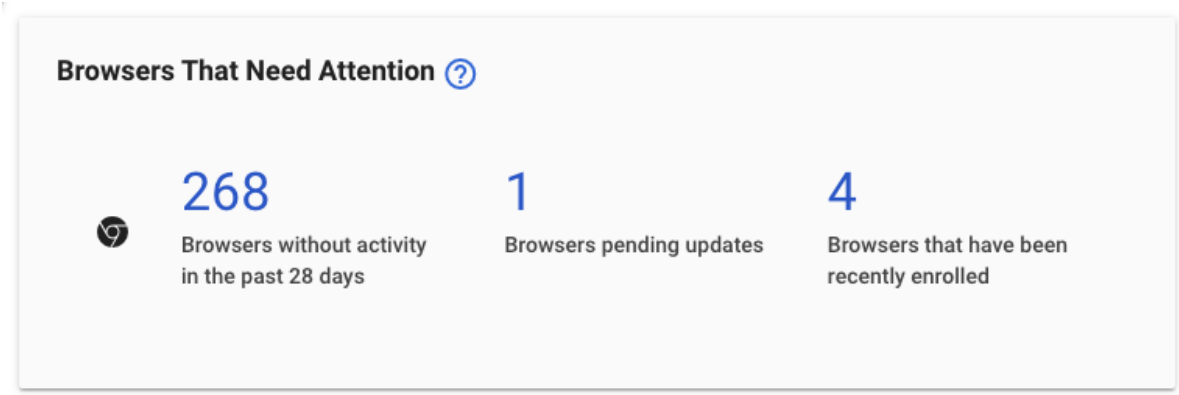
Passpoint: Seamless, secure connection to Wi-Fi networks

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.

Upcoming Admin console changes

New Chrome browser insights

As early as Chrome 112, a new **Browsers that need attention** insights card will allow IT admins to quickly identify browsers that have a pending Chrome update, browsers that are inactive and browsers that have recently enrolled.



Previous release notes

Chrome version & targeted Stable channel release date	PDF
Chrome 110: Feb 01, 2023	PDF
Chrome 109: Jan 10, 2023	PDF
Chrome 108: Nov 29, 2022	PDF
Chrome 107: October 25, 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.