



Chrome 110 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 February 1, 2023.

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

[Chrome 110 release summary](#)

[Current Chrome version release notes](#)

[Chrome browser updates](#)

[ChromeOS updates](#)

[Admin console updates](#)

[Coming soon](#)

[Upcoming Chrome browser changes](#)

[Upcoming ChromeOS changes](#)

[Upcoming Admin console changes](#)

[Previous release notes](#)

[Additional resources](#)

[Still need help?](#)

Chrome 110 release summary

Chrome browser updates	Security/ Privacy	User productivity /Apps	Management
Windows 7/8/8.1 and Windows Server 2012/2012 R2 are no longer supported			✓
Detailed translation settings		✓	
Manual translation on iOS		✓	
Change in launch schedule			✓
Biometrics protection for passwords	✓		
App Store rating on iOS		✓	
Custom web app default network error page		✓	
User-level Enhanced Safe Browsing on iOS	✓		
Chrome Headless mode upgrades		✓	
MetricsReportingEnabled policy available on Android in Chrome			✓
WebAuthn cannot be used on sites with TLS certificate errors	✓		
Cookie information from extensions	✓		
Deprecation of WebSQL and other old Storage features		✓	
Easier password updates when a compromise is detected	✓		
Rolling out GPU changes to NaCL Swapchain and video decoding		✓	
WebView metrics moves app package name filtering to server-side			✓

User-Agent reduction Phase 6	✓		
Real time URL Allowlist now synced through component updaters on Android	✓		
Google Update internal upgrades			✓
New and updated policies in Chrome browser			✓
Removed policies in Chrome browser			✓
ChromeOS updates	Security/ Privacy	User productivity /Apps	Management
Super Resolution Audio for Bluetooth headset microphones		✓	
Channel labeling on ChromeOS	✓		
Search autocomplete redesign		✓	
ChromeOS 110 no longer supports Active Directory Management			✓
Select-to-Speak Improvements		✓	
Local website approvals for Family Link users	✓		
Low storage warning for ChromeOS Camera App			✓
Feedback tool refresh with inline assistive capabilities		✓	
Admin console updates	Security/ Privacy	User productivity /Apps	Management
Recent changes on Chrome Settings page	✓	✓	✓
Plugins section removed from the Browser details view		✓	✓
New policies in Admin console			✓
Upcoming Chrome browser changes	Security/	User	Management

	Privacy	productivity /Apps	
Azure AD Single Sign On (SSO)	✓		
Unused site permissions module in Safety Check	✓		
Web speech recognition API on iOS		✓	
Privacy Sandbox updates in Chrome 111	✓		
New Chrome Sync data types available in Takeout in Chrome 111	✓		
Chrome for Testing		✓	
Enable access to WebHID API from extension service workers in Chrome 111		✓	
PPB_VideoDecoder(Dev) API removed		✓	
New Chrome sync dialog in Chrome for Desktop		✓	
Strict MIME type checks for Worker scripts	✓		
Default to origin-keyed agent clustering in Chrome 112	✓		
Changes to phishing protection on Android as early as Chrome 112	✓		
Chrome apps no longer supported on Windows, Mac, and Linux		✓	
Network Service on Windows will be sandboxed	✓		
Enable access to WebUSB API from extension service workers in Chrome 112 or later		✓	
Extensions must be updated to leverage Manifest V3		✓	✓
Payment Handler API will require CSP connect-src	✓		
First-Party Sets user controls	✓		
Removal ChromeRootStoreEnabled policy			✓
Upcoming ChromeOS changes	Security/ Privacy	User productivity /Apps	Management

Fast Pair		✓	
Managed DoH (DNS over https) with user identification	✓		
Cursive pre-installed for Enterprise and Education accounts		✓	
Updated emoji picker		✓	
Passpoint: Seamless, secure connection to Wi-Fi networks	✓	✓	
Upcoming Admin console changes	Security/ Privacy	User productivity /Apps	Management
Configure print server policies with Google groups			✓
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.

Current Chrome version release notes

Chrome browser updates

Windows 7/8/8.1 and Windows Server 2012/2012 R2 are no longer supported

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

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

Detailed translation settings

Chrome 110 adds new detailed translation settings for controlling the current target language: **Never translate languages** and **Always translate languages**. These settings were previously only editable from the **Translate** UI bubble but now are permanently exposed under `chrome://settings/language`. Enterprise admins can use the existing [TranslateEnabled](#) policy to globally enable or disable translation.

Manual translation on iOS

In addition to detecting and translating languages automatically, Chrome on iOS allows the user to trigger translation manually, if the language was not detected automatically.

Change in launch schedule

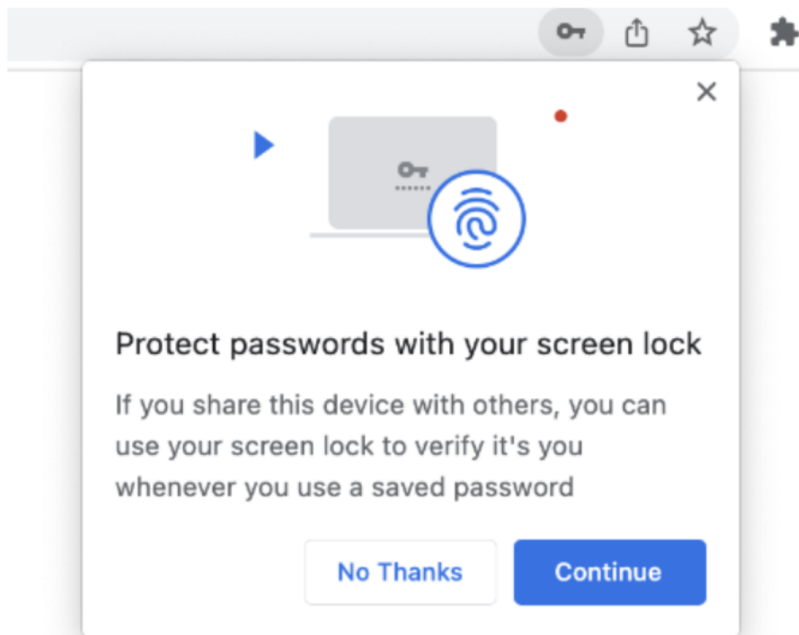
Starting in Chrome 110, Chrome rolls out to the Stable channel one week earlier than previously planned to a very small subset of users. For example, the Chrome 110 Stable release moves from February 7 to February 1, 2023.

You can also expect to see a much smaller rollout at a significantly reduced percentage of our user population for the first week of the published Stable release date. The wider rollout to most users 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](#).

Biometrics protection for passwords

For improved security, Chrome Desktop users can opt into requiring biometrics to autofill their passwords every time.

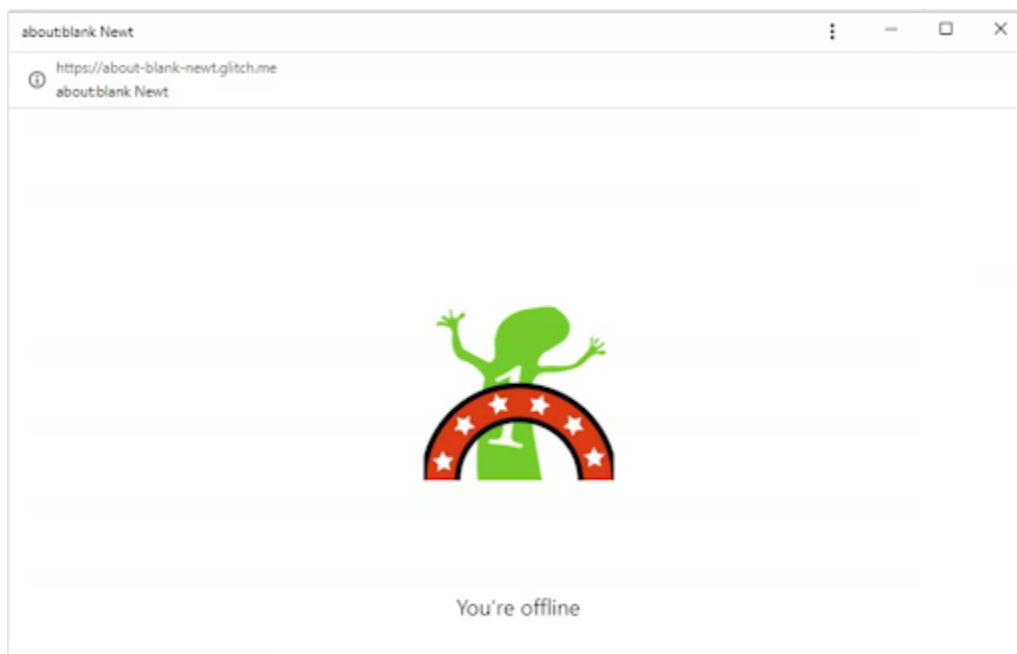


App Store rating on iOS

In Chrome 110, some iOS users might be presented with Apple's standardized App Store rating prompt at most once per year. The prompt gives users the option to rate the app or dismiss the prompt. An enterprise policy, [AppStoreRatingEnabled](#), is available to disable any appearance of the prompt.

Custom web app default network error page

Chrome provides a custom default network error page (when the network is down) for web apps that don't define their own custom offline experience.



User-level Enhanced Safe Browsing on iOS

For Chrome on iOS where the Safe Browsing protection level is not controlled by [SafeBrowsingProtectionLevel](#), users who are signed in and syncing, and have enabled Enhanced Safe Browsing on their Google Account, are now notified that Enhanced Safe Browsing has been enabled on their Chrome profile. Disabling Enhanced Safe Browsing on a synced Google Account disables Enhanced Safe Browsing for their Chrome profile.

Additionally, users that are signed-in and non-synced might be prompted to enable Chrome Enhanced Safe Browsing within 5 minutes of enabling Account Level Enhanced Safe Browsing.

Chrome Headless mode upgrades

Chrome's Headless mode provides a full Chrome browser to tooling vendors and developers that don't need to bring pixels to the screen. It's used for test automation, automation of workflow steps, for example, steps required when setting up a new machine in an enterprise or autofill-like behavior, scraping web content, web rendering services, and so on.

We've rebuilt Headless mode so that it's much closer to Chrome's regular mode. This provides more consistent experiences, including respecting enterprise policies when in Headless mode.

MetricsReportingEnabled policy available on Android in Chrome

As early as Chrome 110, Chrome on Android slightly modifies the first run experience to support the [MetricsReportingEnabled](#) policy. If the admin disables metrics reporting, there is no change to the first run experience. If the admin enables metrics, users can still change the setting in Chrome settings. When enabled, the [MetricsReportingEnabled](#) policy allows anonymous reporting of usage and crash-related data about Chrome to Google.

WebAuthn cannot be used on sites with TLS certificate errors

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

Enterprises can use the [AllowWebAuthnWithBrokenTlsCerts](#) policy if needed as a workaround.

Cookie information from extensions

When you enable Enhanced Safe Browsing, Chrome now collects telemetry information about the cookie information extensions request. 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.

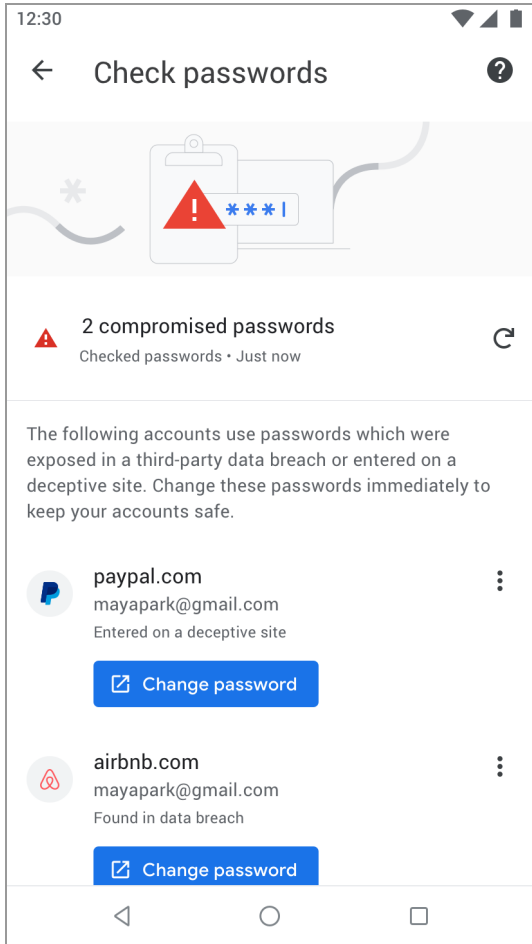
Deprecation of WebSQL and other old Storage features

In Chrome 110 removes the [window.webkitStorageInfo API](#). This legacy quota API has been deprecated since 2013, and has been replaced by the now standardized [StorageManager API](#). Admins can re-enable webkitStorageInfo until Chrome 112, using the enterprise policy, [PrefixedStorageInfoEnabled](#).

WebSQL in third-party contexts is already disabled, and it has had a warning in DevTools since Chrome 105. Chrome 110 removes support in non-secure contexts. An enterprise policy, [WebSQLNonSecureContextEnabled](#), allows Web SQL to function in non-secure contexts for a few months past the removal date.

Easier password updates when a compromise is detected

The **Check passwords** tool now has an expanded set of URLs pointing directly to a **Change password** form. This allows users to take action and fix compromised passwords. The **Check passwords** tool is only available if [PasswordManagerEnabled](#) is set to true or unset.



Rolling out GPU changes to NaCL Swapchain and video decoding

Chrome 110 refactors 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.

If your enterprise encounters any unexpected problems, you can use the [UseMojoVideoDecoderForPepperAllowed](#) and [PPAPISharedImagesSwapChainAllowed](#) enterprise policies to rollback to the previous behavior. If issues appear that are fixed by enabling those policies, please also file a bug at crbug.com before May 5 with the details.

WebView metrics moves app package name filtering to server-side

WebView metrics only store app package names for a limited set of *allowlisted* common apps, to preserve user privacy and anonymity. In Chrome 110, the filtering of these apps moves from the client to the server. Apps using WebView can [opt out of metrics collection](#) via the app manifest.

User-Agent reduction Phase 6

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

Real time URL Allowlist now synced through component updater on Android

In Chrome 110, Chrome on Android uses an allowlist synced through the component updater. This applies to Enhanced Safe Browsing and Make Browsing Better users who have **Safe Browsing URL real time checking** enabled. This allows faster rollout of updated allowlist versions. Since the new allowlist versions are served through the component updater, admins who choose to disable the component updater do not benefit from this feature. In these scenarios, Chrome uses a version of the allowlist that is updated less frequently.

Google Update internal upgrades

In Chrome 109, Google introduced an overhauled version of **Google Update** that:

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

This rollout is continuing gradually throughout the Chrome 110 timeframe. All [existing enterprise policies](#) and controls for managing Chrome's version continue to work the same way. These changes first roll out to macOS and eventually to Windows.

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

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

New and updated policies in Chrome browser

Policy	Description
ExtensionManifestV2Availability	Controls Manifest v2 extension availability.
AppStoreRatingEnabled	Allows users to be shown the iOS App Store Rating promo.
DnsOverHttpsSalt	Specifies a salt value to be used in DnsOverHttpsTemplatesWithIdentifiers when evaluating identify information.
DnsOverHttpsTemplatesWithIdentifiers	Specifies URI template of desired DNS-over-HTTPS resolver with identity information.
MetricsReportingEnabled (new on Android)	Enables reporting of usage and crash-related data.
PPAPISharedImagesSwapChainAllowed	Allows modern buffer allocation for Graphics3D APIs PPAPI plugin.
PdfLocalFileAccessAllowedForDomains	Allows local file access to file:// URLs on these sites in the PDF Viewer.
UseMojoVideoDecoderForPepperAllowed	Allows Pepper to use a new decoder for hardware accelerated video decoding.
AllowWebAuthnWithBrokenTlsCerts	Allows Web Authentication requests on sites with broken TLS certificates.
ShowCastSessionsStartedByOtherDevices	Shows media controls for Google Cast sessions started by other devices on the local network.
NewBaseUrlInheritanceBehaviorAllowed	Allows enabling the feature NewBaseUrlInheritanceBehavior.
ThrottleNonVisibleCrossOriginFramesAllowed	Allows enabling throttling of non-visible, cross-origin iframes.

Removed policies in Chrome browser

Policy	Description
SetTimeoutWithout1MsClampEnabled	Control Javascript setTimeout() function minimum timeout.
AssistantWebEnabled	Allow using Google Assistant on the web, for example, to enable changing passwords automatically

ChromeOS updates

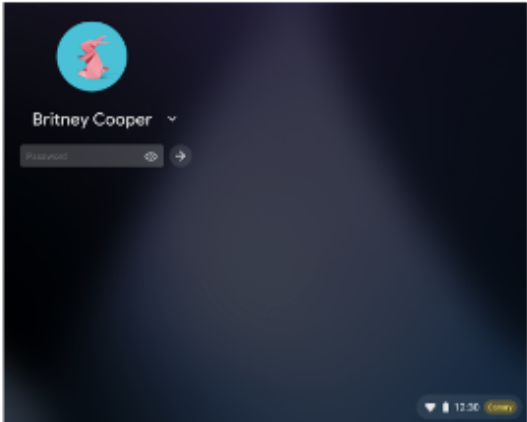
Super Resolution Audio for Bluetooth headset microphones

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

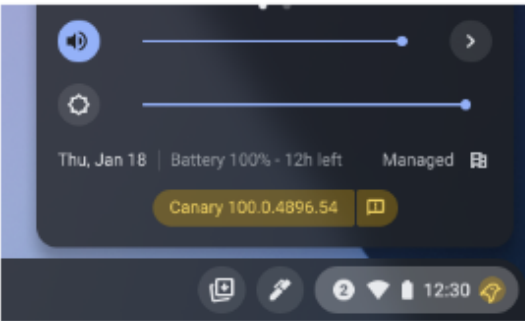
Channel labeling on ChromeOS

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

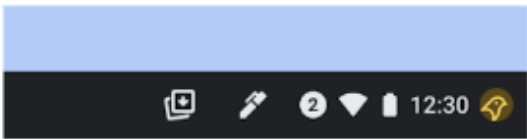
Channel label on the login screen:



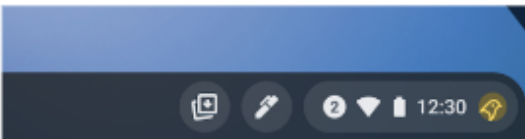
Channel label on Canary:



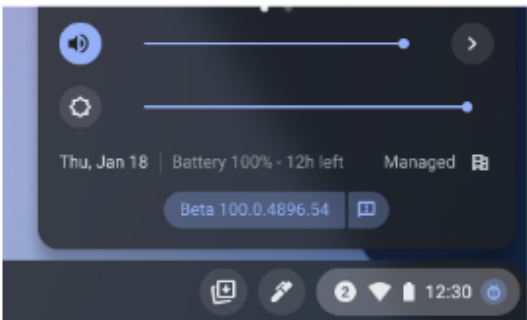
Channel label on tablet:



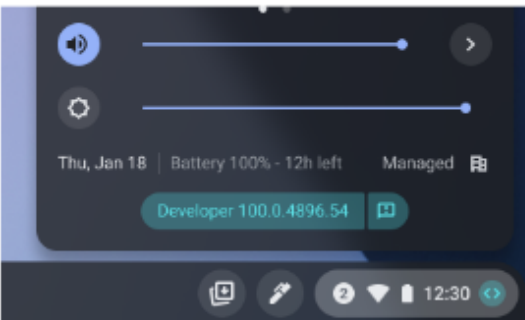
Channel label on clamshell:



Channel label on Beta channel:



Channel label on Developer channel:



Search autocomplete redesign

In ChromeOS Search, we've redesigned the Launcher Search autocomplete to help users shortcut their Search journey with robust autocompletion for mistyped and misspelled queries, clear search result categories for selected results, and intuitive keyboard navigation for result selection.

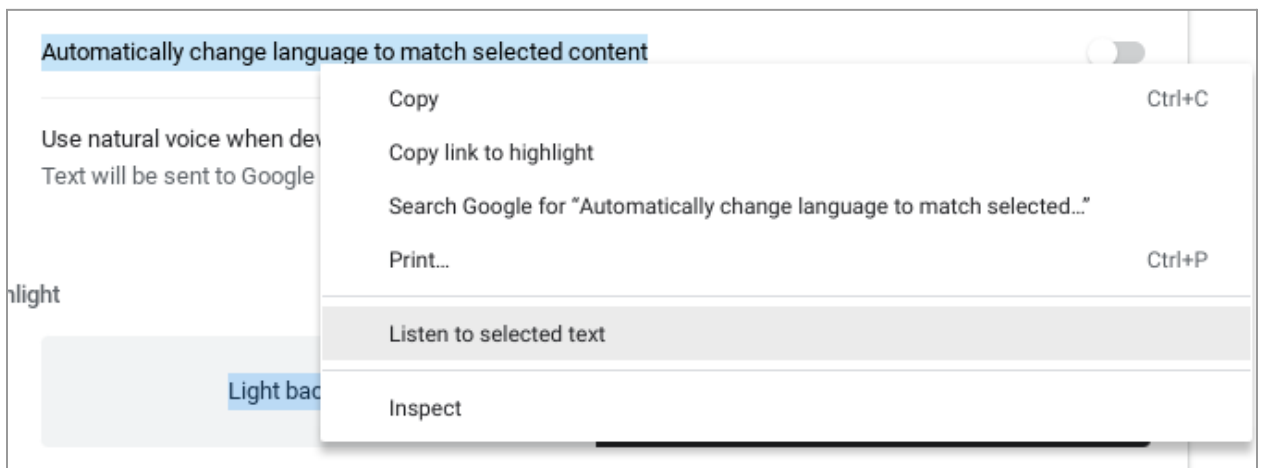
ChromeOS 110 no longer supports Active Directory Management

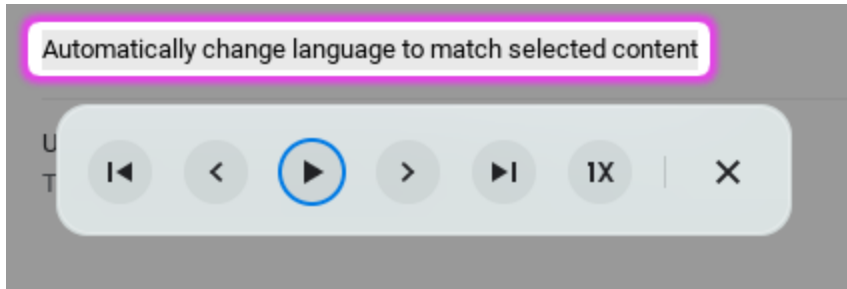
As previously announced, M110 no longer supports Active Directory Management for ChromeOS devices, and login to these devices is blocked.

If you are still [using Active Directory Management for ChromeOS devices](#), make sure to finalize your migration to Cloud Management before updating to M110. If you are not using Active Directory Management for ChromeOS devices, this feature update does not affect you.

Select-to-speak improvements

Chromebook users can now start Select-to-speak from the context menu (right-click menu) of the selected text. For users who continue to start Select-to-speak from the status-tray icon, we've updated the instructions shown when hovering over the icon.





Select-to-speak can now automatically switch language to match the content selected by the user, so that words are pronounced correctly in that language, without the user having to manually change the voice settings.

In addition, we've made setting up Select-to-speak easier, by moving the Select-to-speak settings to a ChromeOS settings page, rather than opening a separate browser tab.

Settings

Search settings

- Network
- Bluetooth
- Connected devices
- Accounts
- Device
- Personalization
- Search and Assistant
- Security and Privacy
- Apps
- Accessibility**
- Advanced
- About ChromeOS

Select-to-speak settings

Speech

Language: Device language

Voice: System voice

Voice preview: Hi there! I'm your text-to-speech voice. [Play](#)

System voice settings

Automatically change language to match selected content:

Use natural voice when device is online:
Text will be sent to Google for processing. [Learn more](#)

Highlight

Light background | Dark background

Highlight each word as it is spoken:

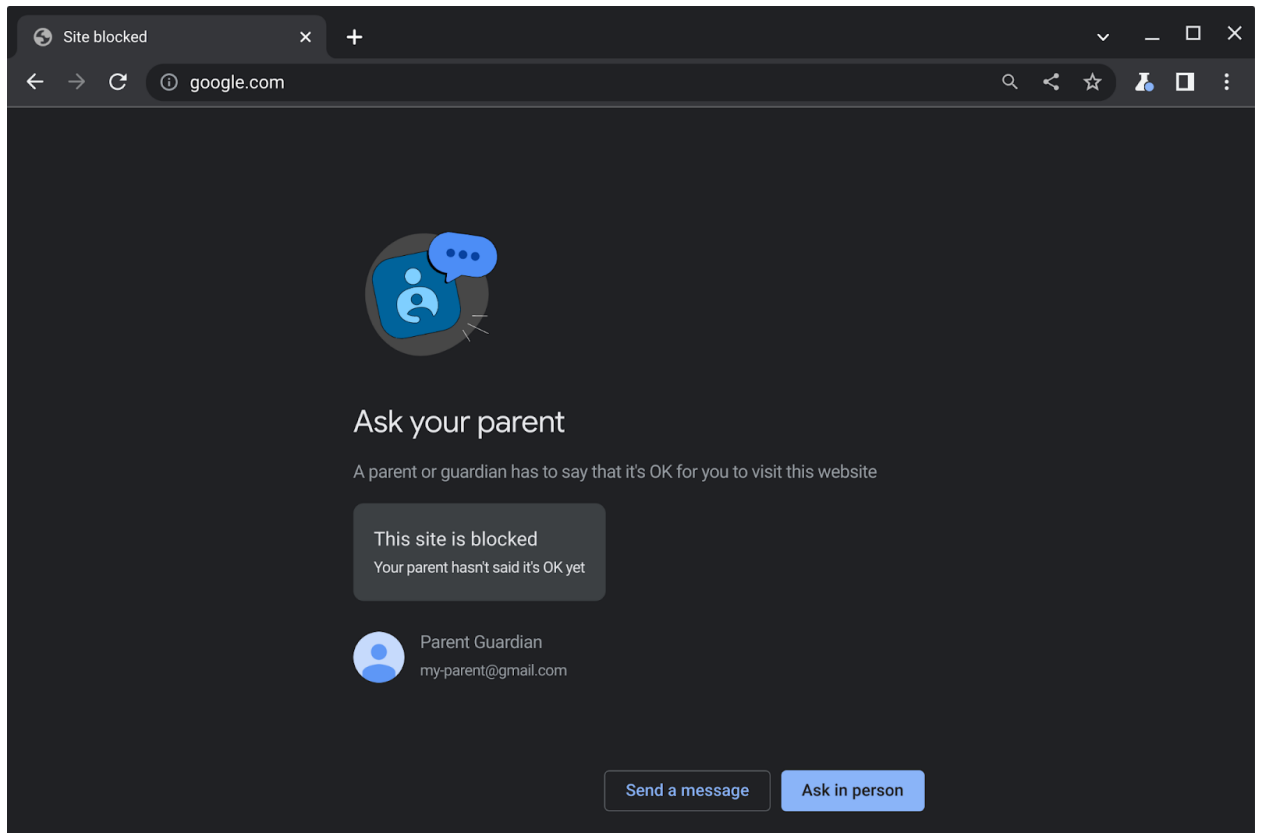
The quick brown fox jumped over the lazy dog.
The quick brown fox jumped over the lazy dog.
The quick brown fox jumped over the lazy dog.

Dim background content:

Navigation controls:
Provides controls to speed up, slow down, and pause the reading voice

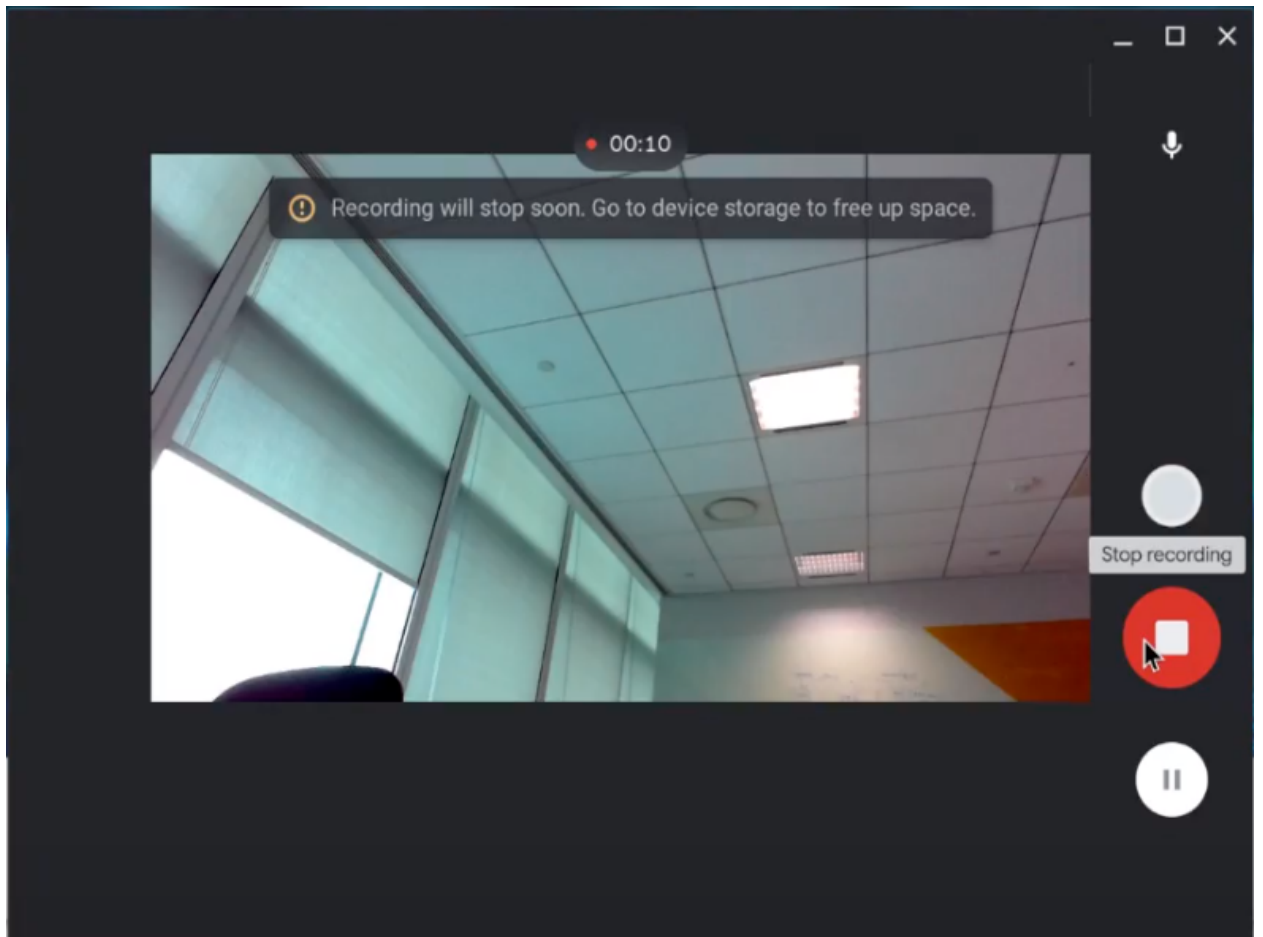
Local website approvals for Family Link users

Parents now have the option to quickly approve blocked websites directly on their child's Chromebook without the **Family Link** app. When blocked from accessing a website, children can now choose to **Ask in person** to allow parents to approve access. For details, see [Manage your child's account on Chromebook](#).




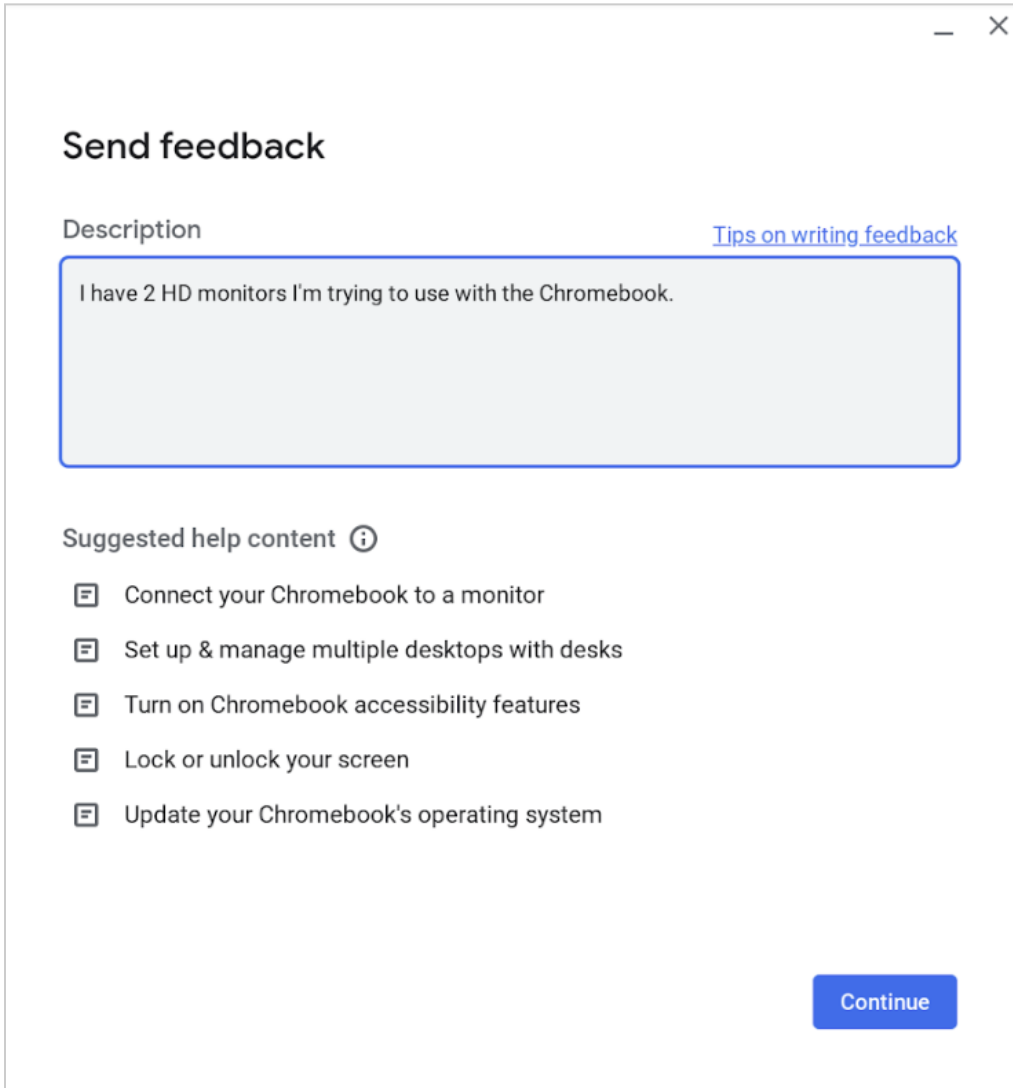
Low storage warning for ChromeOS Camera App

If ChromeOS Camera App detects that the system is running low on storage, it now shows a warning message, then stops recording before all storage is used up.



Feedback tool refresh with inline assistive capabilities


Users can [report a problem or share feedback with Google](#) with the Feedback  form. In ChromeOS 110, a refreshed Feedback form shows users several related help articles, to help them diagnose problems.



Send feedback

Description [Tips on writing feedback](#)

I have 2 HD monitors I'm trying to use with the Chromebook.

Suggested help content 

- Connect your Chromebook to a monitor
- Set up & manage multiple desktops with desks
- Turn on Chromebook accessibility features
- Lock or unlock your screen
- Update your Chromebook's operating system

[Continue](#)

View PPDs for installed printers

You can now view the PostScript Printer Description (PPD) information for any of the installed printers on your system. Select **Settings>Advanced>Print and scan>Printers>Edit printer**. To view the PPD for any of the saved printers, click **View printer PPD**.

Edit printer

Name
HP LaserJet MFP M29w

Address
npofsdhk2.local:631

Protocol
Internet Printing Protocol (IPP)

Queue
ipp/print

URI
ipps://npif03ee2.local:631/ipp/print

Manufacturer
HP

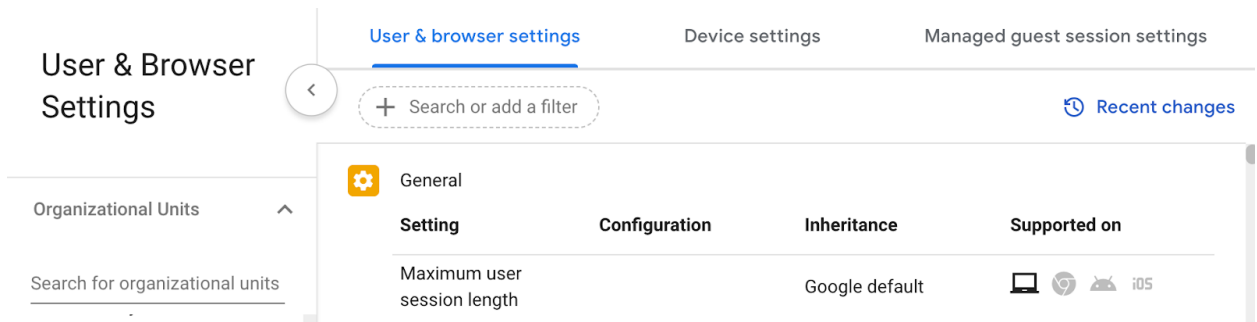
Model
HP Laserjet Mfp M28-M31

[View printer PPD](#) or select PPD. [Learn more](#)

Admin console updates

Recent changes on Chrome Settings page

Admins now see a new **Recent changes** option on the Chrome settings pages. With a single click, admins can access the audit log and see recent policy changes in their domains.



Plugins section removed from the Browser details view

Plugins have been integrated into Chrome; they are now updated and versioned in line with the browser. Chrome 110 removes the **Plugins** section of the Browser details page as it is no longer relevant.

New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
PdfLocalFileAccessAllowedForDomains	User & Browser Settings; Managed Guest Session	Chrome (Linux, Mac, Windows) ChromeOS	Content > Allow local file access to file:// URLs on these sites in the PDF Viewer
ThrottleNonVisibleCrossOriginframesAllowed	User & Browser Settings; Managed Guest Session	Chrome (Linux, Mac, Windows, Android) ChromeOS	Content > Allows enabling throttling of non-visible, cross-origin iframes

AllowWebAuthnWithBrokenTlsCerts	User & Browser Settings; Managed Guest Session	Chrome (Linux, Mac, Windows, Android) ChromeOS	Security > Allow Web Authentication requests on sites with broken TLS certificates.
---	--	--	---

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

Azure AD Single Sign On (SSO)

Chrome 111 will support automatic sign-on into Microsoft identity providers using account information from Microsoft Windows. This feature will be disabled by default.

Unused site permissions module in Safety Check

To better protect user security and privacy, Chrome 111 will automatically revoke the granted permissions that belong to unused websites (not used for 2 months). Chrome will also show the revoked permissions on settings so that users can review them. The revoked permission data will be wiped out 1 month after revocation happens. Permissions granted by enterprise policies are not affected.

Web speech recognition API on iOS

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

Privacy Sandbox updates in Chrome 111

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

IT admins will be able to 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](#).

New Chrome Sync data types available in Takeout in Chrome 111

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

As early as Chrome 111, [Puppeteer](#), Chrome's browser automation library, will use the **Chrome for Testing** binary instead of a Chromium binary. In case you have the Chromium binary allowlisted, you might consider allowlisting the **Chrome for Testing** binary too.

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

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

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

PPB_VideoDecoder(Dev) API removed

The PPB_VideoDecoder(Dev) API was introduced for Adobe Flash. Since Flash is no longer supported in Chrome, this API will be removed in Chrome 111. If you need any extra time to migrate legacy applications, you can use the **ForceEnablePepperVideoDecoderDevAPI** enterprise policy. **As this policy will only be supported through Chrome 114, please file a [bug on crbug.com](https://crbug.com) by May 5 at the absolute latest explaining your use case if you must use the policy.**

New Chrome sync dialog in Chrome for Desktop

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

Strict MIME type checks for Worker scripts

As early as Chrome 112, 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.

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.

Changes to phishing protection on Android as early as Chrome 112

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.

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

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

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

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

Property	Extension ID (Chrome App)	install_url (PWA / Web App)
Gmail	pjkljhegncpnkpnbcohdijeoejaedia	https://mail.google.com/mail/installwebapp?usp=admin
Docs	aohghmighlieiainnegkijnfilokake	https://docs.google.com/document/installwebapp?usp=admin
Drive	apdfllckaahabafndbhieahigkjhalf	https://drive.google.com/drive/installwebapp?usp=admin
Sheets	felcaaldnbdnccImgdncolpebgiejap	https://docs.google.com/spreadsheets/installwebapp?usp=admin
Slides	aapocclcgogkmnckokdopfmhonfmgoek	https://docs.google.com/presentation/installwebapp?usp=admin
Youtube	blpcfgokakmgnkcojhhkbfldkacnbeo	https://www.youtube.com/s/notifications/manifest/cr_install.html

Network Service on Windows will be sandboxed

As early as Chrome 112, 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 112 or later

As early as Chrome 112, 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](#).

Payment Handler API will require CSP *connect-src*

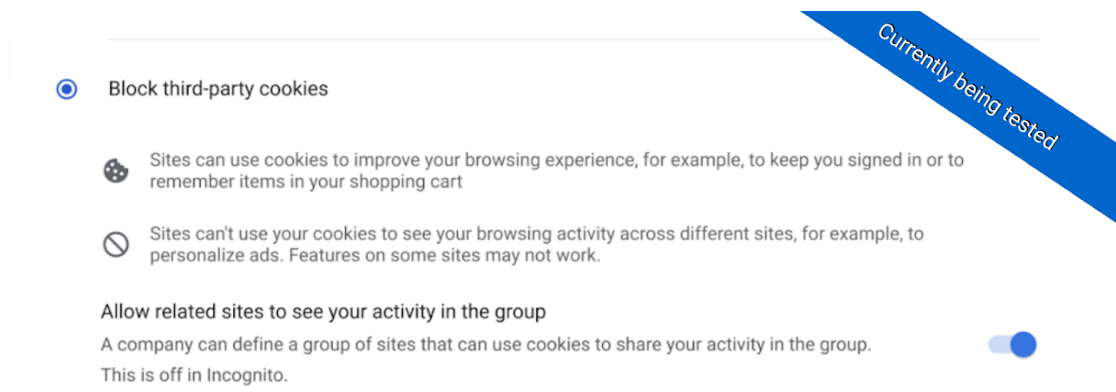
If your organization is using the Web Payment API (Payment Handler and Payment Request) and also uses Content-Security-Policy (CSP) for better protection, then you need to make sure the domains of HTTP requests sent from the Web Payment API are added to the *connect-src* directive of the CSP. This will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

First-Party Sets user controls

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

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

Chrome 112 introduces user controls for these First-Party Sets.



Removal ChromeRootStoreEnabled policy

In Chrome 105, we announced the launch of the [Chrome Root Store](#). A new policy, called [ChromeRootStoreEnabled](#), was introduced to allow selective disabling of the Chrome Root Store in favor of the platform root store. This policy will be removed in Chrome 113.

Upcoming ChromeOS changes

Fast Pair

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

Managed DoH (DNS over https) with user identification

As early as ChromeOS 111, admins will be able to specify secure DNS resolvers with URI templates that include identifying device or user information on supported DNS servers for managed network traffic solutions.

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*.

Updated emoji picker

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

Passpoint: Seamless, secure connection to Wi-Fi networks

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

Upcoming Admin console changes

Configure print server policies with Google groups

Admins will be able to 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 will be able to 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 Chrome browser insights

As early as Chrome 111, 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 109: Jan 10, 2023	PDF
Chrome 108: Nov 29, 2022	PDF
Chrome 107: October 25, 2022	PDF
Chrome 106: September 27, 2022	PDF
Previous 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.