# Chrome 117 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 September 8, 2023. Updated on September 14, 2023.*

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

# Chrome 117 release summary

| Chrome browser updates | Security/ Privacy | User productivity/Apps | Management |
|---|---|---|---|
| Skip unload events | | ✓ | |
| Chrome no longer supports macOS 10.13 and macOS 10.14 | | | ✓ |
| Update to lock icon | ✓ | | |
| Network service is sandboxed on Linux and ChromeOS | ✓ | | |
| TLS Encrypted Client Hello (ECH) | ✓ | | |
| User surveys related to SafeBrowsing warnings | | | ✓ |
| Simplified onboarding experience | | ✓ | |
| Warnings on insecure downloads | ✓ | | |
| Service Worker static routing API | | ✓ | |
| Chrome browser integration with Symantec Endpoint DLP | ✓ | | |
| Require X.509 key usage extension for RSA certificates chaining to local roots | ✓ | | |
| Simplified sign-in and sync experience | | ✓ | |
| Updates to Clear Browsing Data on Android | ✓ | | |
| Allow users to review and optionally remove potentially unsafe extensions | | | ✓ |
| New Chrome Desktop visual refresh in Chrome 117 | | ✓ | |
| Native Client support updates | | ✓ | |
| Deprecate and remove WebSQL | | ✓ | |

| | | | |
|---|---|---|---|
| Revamp permission usage or lockage indicators | | | |
| Price tracking | | ✓ | |
| Price insights on Chrome desktop | | ✓ | |
| Auth on entry to Password Manager on iOS | ✓ | | |
| Improved download warnings | | ✓ | |
| Storage Access API with prompts | | ✓ | |
| Chrome on Android trackpad support | | ✓ | |
| Port overflow check in URL setters | ✓ | | |
| Deprecate TLS SHA-1 server signatures | ✓ | | |
| URL standard-compatible IPv4 embedded IPv6 host parser | ✓ | | |
| Form-filler accessibility mode | | ✓ | |
| Clear client hints via Clear-Site-Data header | ✓ | | |
| Remove WebRTC getStats datachannelIdentifier -1 | ✓ | | |
| Remove WebRTC getStats encoderImplementation/decoderImplementation `unknown` | ✓ | | |
| Unship callback-based legacy getStats() in WebRTC | ✓ | | |
| New and updated policies in Chrome browser | | | ✓ |
| Removed policies in Chrome browser | | | ✓ |
| ChromeOS updates | Security/ Privacy | User productivity/Apps | Management |
| ChromeOS battery state sounds | | | ✓ |

| | | | |
|---|---|---|---|
| Avoid content control escapes on the login or lock screen | ✓ | | |
| Emoji Picker with GIF support | | ✓ | |
| ChromeOS gets a makeover | | ✓ | |
| ChromeOS Personalization App | | ✓ | |
| Color correction settings on ChromeOS | | ✓ | |
| Tabbed PWAs on ChromeOS | | | ✓ |
| System answer cards in Launcher search | | ✓ | |
| Nudge managed users towards enrolling non-ZTE devices | ✓ | | ✓ |
| Replacing the Bluetooth stack on ChromeOS | | | ✓ |
| Time-lapse recording | | ✓ | |
| Enhanced options in clipboard history | | ✓ | |
| ChromeVox dialog changes | | ✓ | |
| Steam enabled on all capable devices | | ✓ | |
| Up Next Calendar view with *Join video call* integration | | ✓ | |
| Adaptive Charging | | | ✓ |
| Admin console updates | Security/ Privacy | User productivity/Apps | Management |
| Printing reports now available in Chrome Management Reports API | | | ✓ |
| New policies in the Admin console | | | ✓ |
| Upcoming Chrome browser changes | Security/ Privacy | User productivity/Apps | Management |
| Chrome will introduce a `chrome://policy/test page` | | | ✓ |

| | | | |
|---|---|---|---|
| Network Service on Windows will be sandboxed | ✓ | | |
| RemoveForceMajorVersionToMinorPositionInUserAgent policy | | | ✓ |
| Remotely disable malicious off-store extensions | ✓ | | |
| Remove RendererCodeIntegrityEnabled policy | | | ✓ |
| Support for passkeys in iCloud Keychain on macOS | | ✓ | ✓ |
| Hash-prefix real-time lookups | ✓ | | |
| Red interstitial facelift | ✓ | ✓ | |
| Form controls support vertical writing mode | | ✓ | |
| Block all cookies set via JavaScript that contain control characters | ✓ | | |
| Clearer Safe Browsing protection level settings text and images | ✓ | | |
| WebUSB in Extension Service Workers | ✓ | | |
| Include chrome.tabs API calls in extension telemetry reports | ✓ | | |
| Remove non-standard appearance keywords | | ✓ | |
| Chrome release schedule changes | | | ✓ |
| Permissions prompt for Web MIDI API | ✓ | | |
| Migrate away from data URLs in SVG <use> element | ✓ | ✓ | |
| Chrome Browser Cloud Management: Crash report | | | ✓ |
| IP protection Phase 0 for Chrome | ✓ | | |
| Display banner to allow resume last tab from other devices | | ✓ | |

| | | | |
|---|---|---|---|
| Remove Sanitizer API | ✓ | | |
| Tab groups can be saved, recalled, and synced | | ✓ | |
| Chrome profile separation: new policies | | | ✓ |
| Chrome on Android will no longer support Android Nougat | | | ✓ |
| Replace dangling markup in target name to *_blank* | ✓ | | |
| Private Network Access restrictions for automotive | ✓ | | |
| Deprecate non-standard `shadowroot` attribute for declarative shadow DOM | ✓ | | |
| Chrome Third-Party Cookie Deprecation (3PCD) | ✓ | | |
| Remove LegacySameSiteCookieBehaviorEnabledForDomainList policy | | | ✓ |
| Intent to deprecate: Mutation events | | ✓ | |
| Extensions must be updated to leverage Manifest V3 | ✓ | ✓ | ✓ |
| Upcoming ChromeOS changes | Security/ Privacy | User productivity/Apps | Management |
| Privacy Hub | | | ✓ |
| ChromeOS Admin templates | | | ✓ |
| Upcoming Admin console changes | Security/ Privacy | User productivity/Apps | Management |
| URL-keyed anonymized data collection in Kiosk mode | ✓ | | |

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

### Skip unload events

The presence of unload event listeners is a primary blocker for back/forward cache on Chromium based browsers and for Firefox on desktop platforms. On the other hand, for mobile platforms, almost all browsers prioritize the bfcache by not firing unload events in most cases. To improve the situation, we've been working with lots of partners and successfully reduced the use of unload event listeners over the last few years. To further accelerate this migration, we propose to have Chrome for desktop gradually skip unload events. In case you need more time to migrate away from unload events, we'll offer temporary opt-outs in the form of an API and a group policy, which will allow you to selectively keep the behavior unchanged.

- **Chrome 117 on Chrome OS, Linux, Mac, Windows:** Dev Trial

### Chrome no longer supports macOS 10.13 and macOS 10.14

Chrome will no longer support macOS 10.13 and macOS 10.14, which are already outside of their support window with Apple. Users have to update their operating systems in order to continue running Chrome browser. Running on a supported operating system is essential to maintaining security. If run on macOS 10.13 or 10.14, Chrome continues to show an infobar that reminds users that Chrome 117 will no longer support macOS 10.13 and macOS 10.14.

- **Chrome 117 on Mac:** Chrome no longer supports macOS 10.13 and macOS 10.14

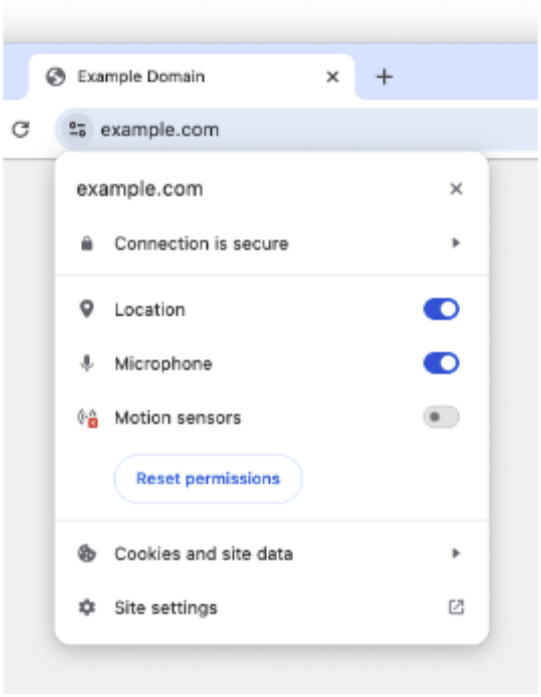
**Update to lock icon**

We plan to replace the lock icon with a variant of the tune icon, which is commonly used to indicate controls and settings. Replacing the lock icon with a neutral indicator prevents the misunderstanding that the lock icon is associated with the trustworthiness of a page, and emphasizes that security should be the default state in Chrome. Our research has also shown that many users never understood that clicking the lock icon showed important information and controls. We think the new icon helps make permission controls and additional security information more accessible, while avoiding the misunderstandings that plague the lock icon.

The new icon is scheduled to launch as part of a general design refresh for desktop platforms. Chrome will continue to alert users when their connection is not secure. You can enable the tune icon pre-release in Chrome for Desktop if you enable Chrome Refresh 2023 at chrome://flags#chrome-refresh-2023, but keep in mind this flag enables work that is still actively in-progress and under development, and does not represent a final product.

We will also replace the icon on Android. On iOS, the lock icon is not tappable, so we will be removing the icon. You can read more in this blog post.

- **Chrome 117 on Linux, Mac, Windows:** The new icon is scheduled to launch in Chrome 117.




**Network service is sandboxed on Linux and ChromeOS**

The network service is sandboxed on Linux and ChromeOS to improve security. On Linux, it's possible that third party software (likely data loss prevention or antivirus software) is injecting code into Chrome's processes and will be blocked by this change. This may result in Chrome crashing for your users.

If this happens, you should work with the vendor of the third party software to stop it from injecting code into Chrome's processes. In the meantime, you will be able to use the NetworkServiceSandboxEnabled policy to defer the sandboxing. This is a temporary measure intended to help enterprises surprised by the change; the policy will be removed in a future version of Chrome.

- **Chrome 117 on Chrome OS, Linux:** The network service sandboxed on Linux and ChromeOS to improve security.

**TLS Encrypted Client Hello (ECH)**

The TLS Encrypted ClientHello (ECH) extension enables clients to encrypt ClientHello messages, which are normally sent in cleartext, under a server's public key. This allows websites to opt-in to avoid leaking sensitive fields, like the server name, to the network by hosting a special HTTPS RR DNS record. (Earlier iterations of this extension were called Encrypted Server Name Indication, or ESNI.) 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 notice any incompatibilities, you can use the EncryptedClientHelloEnabled enterprise policy to disable support for ECH.

**Chrome 117 on Chrome OS, Linux, Mac, Windows**

**User surveys related to SafeBrowsing warnings**

After a user adheres to or bypasses a SafeBrowsing warning, Chrome may ask them about their satisfaction with the experience. You can control this with the SafeBrowsingSurveysEnabled policy.

- **Chrome 117 on Chrome OS, Linux, Mac, Windows**

**Simplified onboarding experience**

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

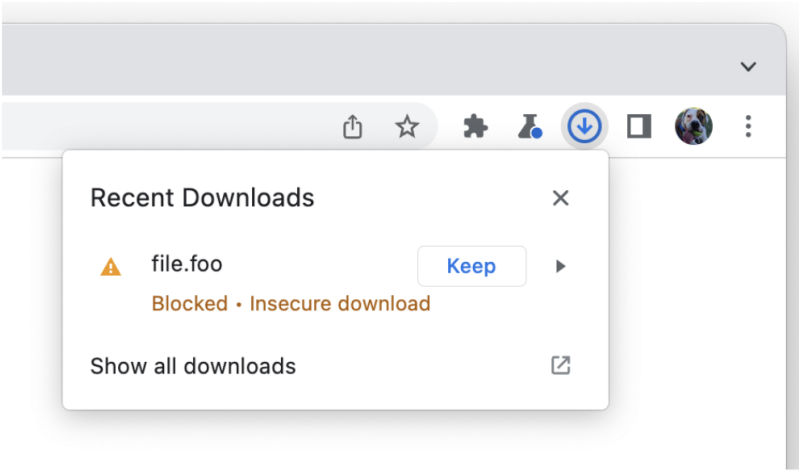
control whether the user can sign into Chrome and turn on sync. The PromotionalTabsEnabled policy can be used to skip the onboarding altogether. DefaultBrowserSettingEnabled is respected in the same way as before.

- **Chrome 117 on Linux, Mac, Windows**

**Warnings on insecure downloads**

Chrome will begin showing warnings on some downloads if those files were downloaded over an insecure (i.e. not HTTPS) connection. These warnings do not prevent downloading and can be bypassed by the user. Enterprises can test their downloads by enabling warnings via chrome://flags/#insecure-download-warnings . Enterprises can also disable warnings for sites that can not deliver files securely by adding the downloading site to InsecureContentAllowedForUrls.

- **Chrome 117 on Android, Chrome OS, LaCrOS, Linux, Mac, Windows, Fuchsia:** Chrome shows warnings on some downloads.



**Service Worker static routing API**

Chrome releases the Service Worker static routing API; it enables developers to optimize how Service Workers are loaded. Specifically, it allows developers to configure the routing, and allows them to offload simple things ServiceWorkers do. If the condition matches, the navigation happens without starting ServiceWorkers or executing JavaScript, which allows web pages to avoid performance penalties due to ServiceWorker interceptions.

- Chrome 116 on Android, Chrome OS, Linux, Mac, Windows: Origin Trial for Service Worker static routing API
- **Chrome 117 on Android, Chrome OS, Linux, Mac, Windows:** Release of the Service Worker static routing API

**Chrome browser integration with Symantec Endpoint DLP**

This feature provides a secure native integration that transfers content (file or text) between Chrome and Broadcom's Symantec DLP agent without the need for deploying an extension. When a CBCM or CDM managed user performs an action that sends data via Chrome, Symantec Endpoint DLP can monitor for data exfiltration and apply allow/block controls based on customer's DLP policies.

- **Chrome 117 on Windows**

**Require X.509 key usage extension for RSA certificates chaining to local roots**

X.509 certificates used for HTTPS should contain a key usage extension that declares how the key in a certificate may be used. Such instructions ensure certificates are not used in an unintended context, which protects against a class of cross-protocol attacks on HTTPS and other protocols. For this to work, HTTPS clients must check that server certificates match the connection's TLS parameters, specifically that the key usage flag for “digitalSignature” and possibly “keyEncipherment” (depending on TLS ciphers in use) are asserted when using RSA.

Chrome 117 will begin enforcing that the key usage extension is set properly on RSA certificates chaining to local roots. Key usage is already required for ECDSA certificates, and for publicly trusted certificates. Enterprises can test and temporarily disable key usage enforcement using the RSAKeyUsageForLocalAnchorsEnabled policy (available in Chrome 116).

- Chrome 116 on Android, Chrome OS, Linux, Mac, Windows: The RSAKeyUsageForLocalAnchorsEnabled policy is added
- **Chrome 117 on Android, Chrome OS, Linux, Mac, Windows:** Chrome begins enforcing that the key usage extension is set properly on RSA certificates chaining to local roots. Key usage is already required for ECDSA certificates, and for publicly trusted certificates.

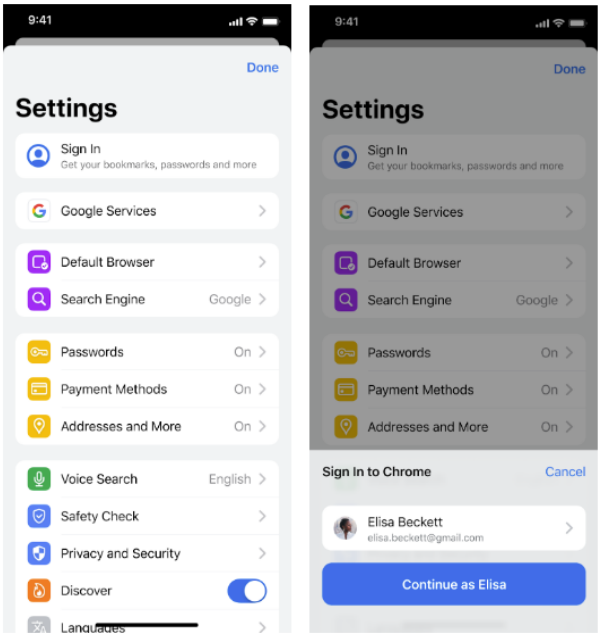
**Simplified sign-in and sync experience**

Chrome launches a simplified and consolidated version of sign-in and sync in Chrome. Chrome sync will no longer be shown as a separate feature in settings or elsewhere. Instead, users can sign in to Chrome to use and save information like passwords, bookmarks and more in their Google Account, subject to the relevant enterprise policies.

As before, the functionality previously part of Chrome sync that saves and accesses Chrome data in the Google Account can be turned off fully (via SyncDisabled) or partially (via SyncTypesListDisabled). Sign-in to Chrome can be required or disabled via BrowserSignin as before.

Note that the changes do not affect users' ability to sign in to Google services on the web (like Gmail) without signing in to Chrome, their ability to stay signed out of Chrome, or their ability to control what information is synced with their Google Account.

- **Chrome 117 on iOS:** Simplified sign-in and sync experience launches on iOS




**Updates to *Clear browsing data* on Android**

Chrome enhances the browser data deletion controls by making it easier and quicker for users to complete their ‘Clear browsing data’ journeys, while maintaining the granular controls for advanced data deletion needs.

- **Chrome 117 on Android**

**Allow users to review and optionally remove potentially unsafe extensions**

A new review panel will be added in chrome://extensions, which appears whenever there are potentially unsafe extensions that need the user's attention, such as extensions that are malware, policy violating or are no longer available in the Chrome Web Store. The user can choose to remove or keep these extensions.

There is also a count of risky extensions needing review that is presented in the Chrome Privacy & Security settings page. As an administrator, you can preemptively control the availability of potentially unsafe extensions using the ExtensionUnpublishedAvailability policy.

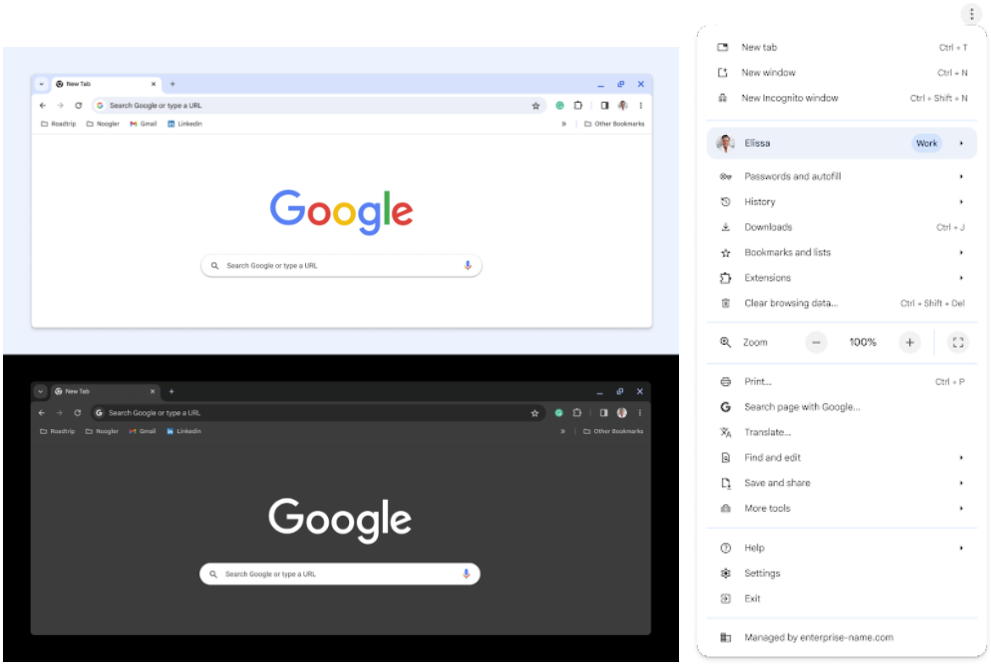
- **Chrome 117 on Chrome OS, Linux, Mac, Windows**

**New Chrome Desktop visual refresh in Chrome 117**

With Google’s design platform moving to Google Material 3, we have an opportunity to modernize our desktop browser across OS’s, leveraging updated UI elements or styling, enhancing personalization through a new dynamic color system, and improving accessibility. The first wave of UI updates will roll out in Chrome 117.

The three dot Chrome menu will also be refreshed, providing a foundation to scale personalization and customization experiences in Chrome by enabling customers proximate access to tools and actions.. The menu will be updated in phases starting in Chrome 117.

- **Chrome 117 on Linux, Mac, Windows:** Rollout starts for all users




**Native Client support updates**

We will remove Native Client NaCl support from extensions on Windows, macOS, Linux. An enterprise policy will be available, NativeClientForceAllowed, which will allow Native Client to continue to be used.

- **Chrome 117 on Linux, Mac, Windows:** Removal of Native Client NaCl support from extensions on Windows, macOS, Linux.
- Chrome 119 on Linux, Mac, Windows: Removal of NativeClientForceAllowed policy

**Deprecate and remove WebSQL**

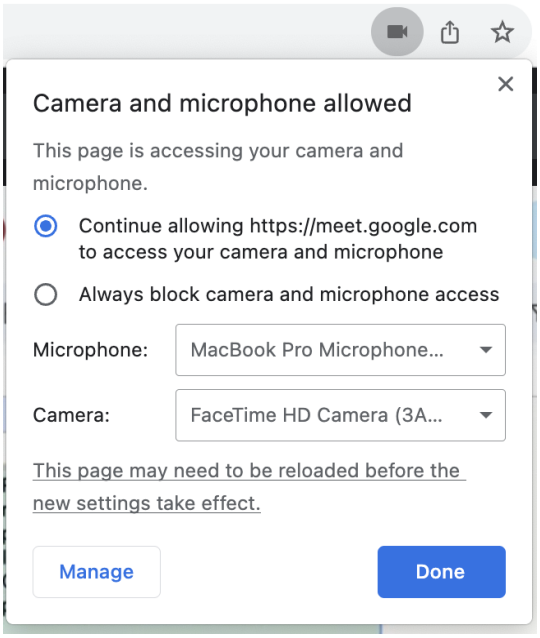
The Web SQL Database standard was first proposed in April 2009 and abandoned in November 2010. Gecko never implemented this feature and WebKit deprecated this feature in 2019. The W3C encouraged those needing web databases to adopt Web Storage or Indexed Database. Ever since its release, it has made it incredibly difficult to keep our users secure. SQLite was not initially designed to run malicious SQL statements, and yet with WebsQL we have to do exactly this. Having to react to a flow of stability and security issues is an unpredictable cost to the storage team. With SQLite over WASM as its official replacement, we want to remove WebSQL entirely.

- Chrome 115: Deprecation message added to console.
- **Chrome 117:** In Chrome 117 the WebSQL Deprecation Trial starts. The trial ends in Chrome 123. During the trial period, a policy, WebSQLAccess, is needed for the feature to be available.
- Chrome 119: Starting Chrome 119, WebSQL is no longer available. Access to the feature is available until Chrome 123 using the WebSQLAccess policy.

**Revamp permission usage or blockage indicators**

In-use activity indicators are visual cues that let users know that an origin is actively using a permission-gated feature. They can be used to indicate things like whether geolocation is accessed, or video and audio are being captured. Chrome is changing the life cycle of the activity indicators, updating how long they appear in the address bar.

- **Chrome 117 on Chrome OS, Linux, Mac, Windows**

- 


**Price tracking**

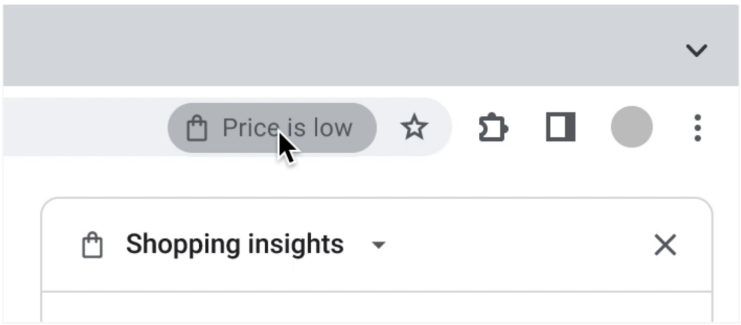
Starting in Chrome 117, when users bookmark a price-trackable product, price tracking will be enabled by default when available. Users will be able to disable price tracking per item, and administrators can disable the feature entirely with the ShoppingListEnabled policy.

- **Chrome 117 on Chrome OS, Linux, Mac, Windows**

**Price insights on Chrome desktop**

Some users will see a chip in the address bar which enables them to see price information about a product they're shopping for.

- **Chrome 117 on Chrome OS, Linux, Mac, Windows**




**Auth on entry to Password Manager on iOS**

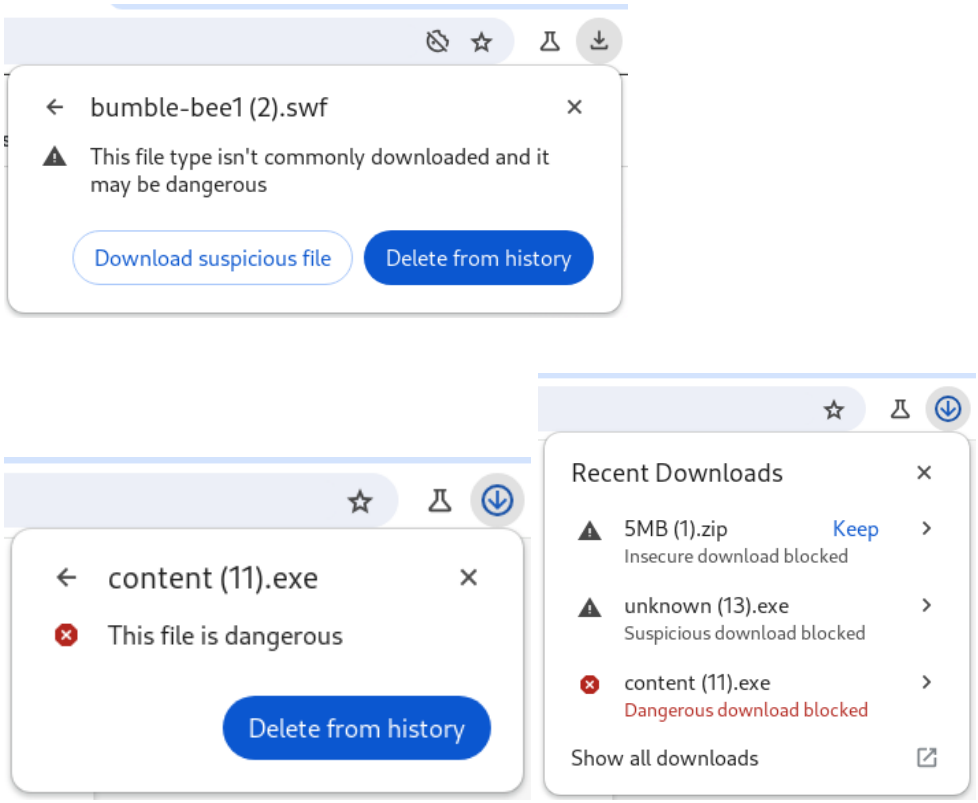
To improve security, re-auth is now required when entering Google Password Manager on Chrome on iOS. Previously, re-auth was required only when viewing password details or notes. The device unlock method will be offered, i.e. FaceID, TouchID, or Passcode. If a Passcode is not set-up, the user will be prompted to do so.

- **Chrome 117 on iOS:** Re-auth required anytime when entering Google Password Manager on Chrome on iOS

**Improved download warnings**

To help reduce cookie theft and other consequences of downloading malware, we're cleaning up desktop download warning strings and patterns to be clear and consistent.

- **Chrome 117 on LaCrOS, Linux, Mac, Windows:** Strings, icons, and colors, as well as warning messages for some downloads, will be updated.




**Storage Access API with prompts**

Allow frames to request access to third-party cookies through the Storage Access API (SAA) when third-party cookies are blocked.

- **Chrome 117 on Chrome OS, LaCrOS, Linux, Mac, Windows:** Support the Storage Access API by implementing all the behaviors listed in the specification, i.e. with user prompts, and additionally having its own user-agent-specific behaviors.

**Chrome on Android trackpad support**

Chrome on Android will have advanced keyboard and trackpad/mouse support, similar to desktop Chrome.

- **Chrome 117 on Android:** Enabled shortcuts for web content edit, cursor movements and media.

**Port overflow check in URL setters**

The port value will be checked when setting url.port. All the values that overflow the 16-bit numeric limit will be no longer valid. For instance the following script behave differently after the change: ``` u = new URL("http://test.com"); u.port = 65536; console.log(u.port); ``` Before the change the output is 65536. After the change the output will be 80.

- **Chrome 117 on Windows, Mac, Linux, Android**

**Deprecate TLS SHA-1 server signatures**

Chrome is removing support for signature algorithms using SHA-1 for server signatures during the TLS handshake. This does not affect SHA-1 support in server certificates, which was already removed, or in client certificates, which continues to be supported. SHA-1 can be temporarily re-enabled via the temporary InsecureHashesInTLSHandshakesEnabled enterprise policy. This policy will be removed in Chrome 123.

- **Chrome 117 on Windows, Mac, Linux, Android**

**URL standard-compatible IPv4 embedded IPv6 host parser**

The behavior of parsing IPv4 embedded IPv6 host parser will be updated to strictly follow the web URL standard: https://url.spec.whatwg.org/#concept-ipv6-parser The introduced restrictions on the IPv6 address are: * The embedded IPv4 address shall always consist of 4 parts. Addresses with less than 4 parts like http://[::1.2] will be no longer valid. The feature is a part of the URL interop 2023.

- **Chrome 117 on Windows, Mac, Linux, Android**

**Form-Filler Accessibility Mode**

This feature improves performance by providing a subset of the full accessibility API to form-filler apps.

- **Chrome 117 on Android:** A subset of the full accessibility API is provided to form-filler apps.

**Clear client hints via `Clear-Site-Data` header**

Websites will now be able to clear the client hints cache using `` `Clear-Site-Data: "clientHints"` ``. Client hints will also now be cleared when `cookies`, `cache`, or `*` are targeted by the same header. This is because if the user clears cookies in the UI client hints are already cleared as well, the client hints cache is a cache, and to be consistent with wildcard targets respectively.

- **Chrome 117 on Windows, Mac, Linux, Android**

**Remove WebRTC getStats datachannelIdentifier -1**

The WebRTC getStats API exposes a dataChannelIdentifier property. It will no longer provide the value "-1" in cases where statistics are queried before the datachannel connection is established. Instead, the dictionary member will be omitted. This follows the general pattern not to return meaningless information described in this article.

- **Chrome 117 on Windows, Mac, Linux, Android**

**RemoveWebRTC getStats encoderImplementation or decoderImplementation *unknown***

The WebRTC getStats API exposes the encoder and decoder implementation names for outbound and inbound video:

`https://w3c.github.io/webrtc-stats/#dom-rtcoutboundrtpstreamstats-encoderimplementation`

It will no longer provide the value *unknown* in cases where statistics are queried before a video frame was encoded or decoded. Instead, the dictionary member will be omitted. This follows the general pattern not to return meaningless information described in this article.

- **Chrome 117 on Windows, Mac, Linux, Android**

**Unship callback-based legacy getStats() for WebRTC**

RTCPeerConnection has two versions of `getStats()`, one that is spec-compliant returning the report via resolving a promise, and one that is non-standard returning a very different report via a callback as the first argument. The callback-based one will soon be removed. Removal target: Chrome 117. A deprecation trial is available Chrome 113- Chrome 121 for apps that need more time. In the Chrome 114+ the method will throw an exception in Canary/Beta unless using the trial.

- **Chrome 117 on Windows, Mac, Linux, Android**

**New and updated policies in Chrome browser**

| Policy | Description |
|---|---|
| NetworkServiceSandboxEnabled | Enable the network service sandbox (now available on Linux). |
| BeforeunloadEventCancelByPreventDefaultEnabled | Control new behavior for the cancel dialog produced by the `beforeunload` event. |
| ForcePermissionPolicyUnloadDefaultEnabled | Controls whether unload event handlers can be disabled. |
| AccessibilityPerformanceFilteringAllowed | Allow accessibility performance filtering. |
| SafeBrowsingSurveysEnabled | Allow Safe Browsing surveys. |

### Removed policies in Chrome browser

| Policy | Description |
| --- | --- |
| DeviceTargetVersionSelector | Allow devices to select a specific target version of Google ChromeOS they will update to |

## ChromeOS updates

### ChromeOS battery state sounds

In Chrome 117, audible sounds now indicate battery status. Users can turn on and off these sounds and Admins can control them using the DeviceLowBatterySoundEnabled policy.

When the device is not plugged in, you hear warning sounds if:

- Battery level goes down to 15 minutes of charge time left, and another one when there is 5 minutes left.

When the device is plugged in, you hear an information beep when:

- Battery level - 0-15% (low)
- Battery level - 16-79% (med)
- Battery level - 80-100% (high)

In the case where the device is connected to a low power charger, you'll hear warnings when the battery goes down to 10%, then again at 5%.

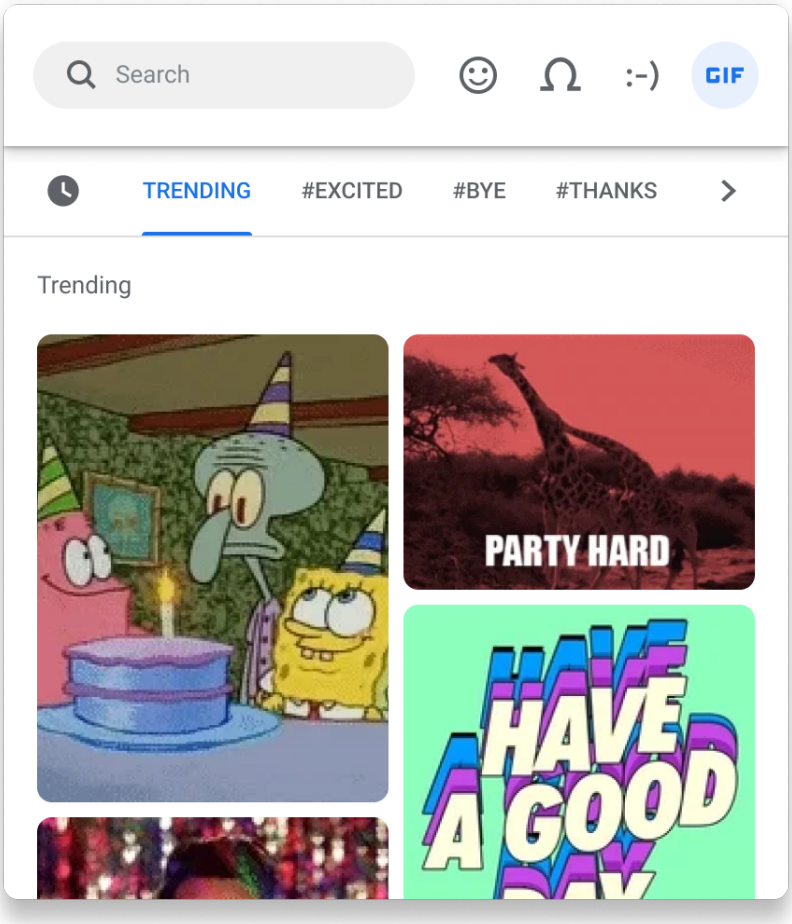
**Avoid content control escapes on the login or lock screen**

Administrators can now control and limit the available content on end-users login and lock screens when identity federation is used with a third party identity provider (using SAML or OIDC). This is achieved by introducing two new policies to block or allow external URLs on login and lock screens, DeviceAuthenticationURLAllowlist and DeviceAuthenticationURLBlocklist. As a result, you can prevent content control escapes.

**Emoji Picker with GIF support**

The emoji picker now supports GIFs. Search and find the perfect GIF to express yourself.

For managed devices, this feature is switched off by default.




**ChromeOS gets a makeover**

Thanks to Google Material 3, Google's new design platform, ChromeOS 117 brings with it:

- A new set of themes which dynamically update to reflect your wallpaper and style.
- A new look for almost all system surfaces with updated text, menus, icons or elements.

You can control the new look using the ChromeOS Personalization App.

### ChromeOS Personalization App

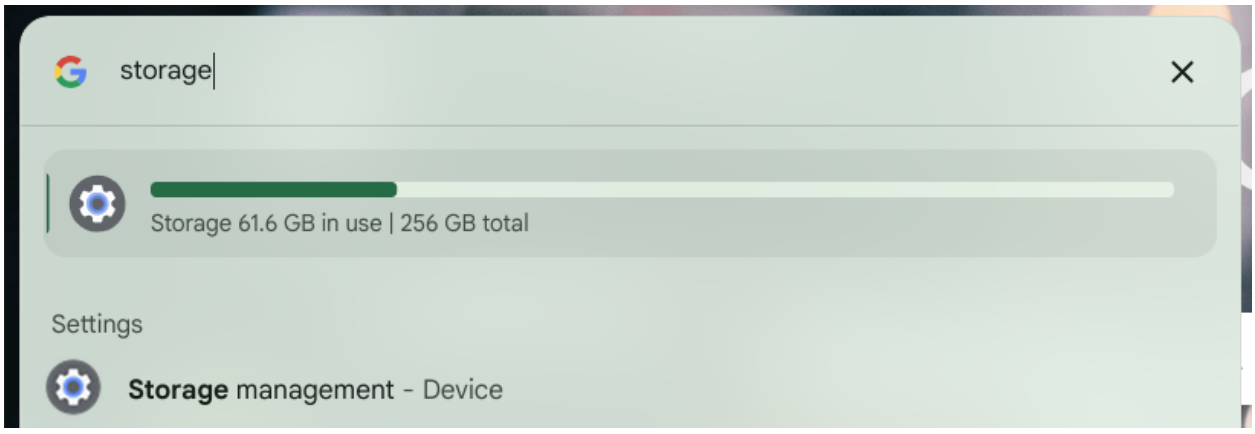
With this launch, your ChromeOS now has accent colors that match your wallpapers, creating a unique theme for your device. The accent colors also adapt to the light and dark modes.

### Color correction settings on ChromeOS

ChromeOS now has built-in color correction settings that make it easier for users to see colors on their screens. In ChromeOS Accessibility settings, under Display and Magnification, you can enable color filters for protanopia, deuteranopia or tritanopia, or to view the display in grayscale. Users can use a slider to customize the filters' intensity to meet their needs.

### System answer cards in Launcher search

When users search for the status of their OS version, battery, RAM, storage, or CPU, in Launcher, they can now see that information previewed in the search results.




### Nudge managed users towards enrolling non-ZTE devices

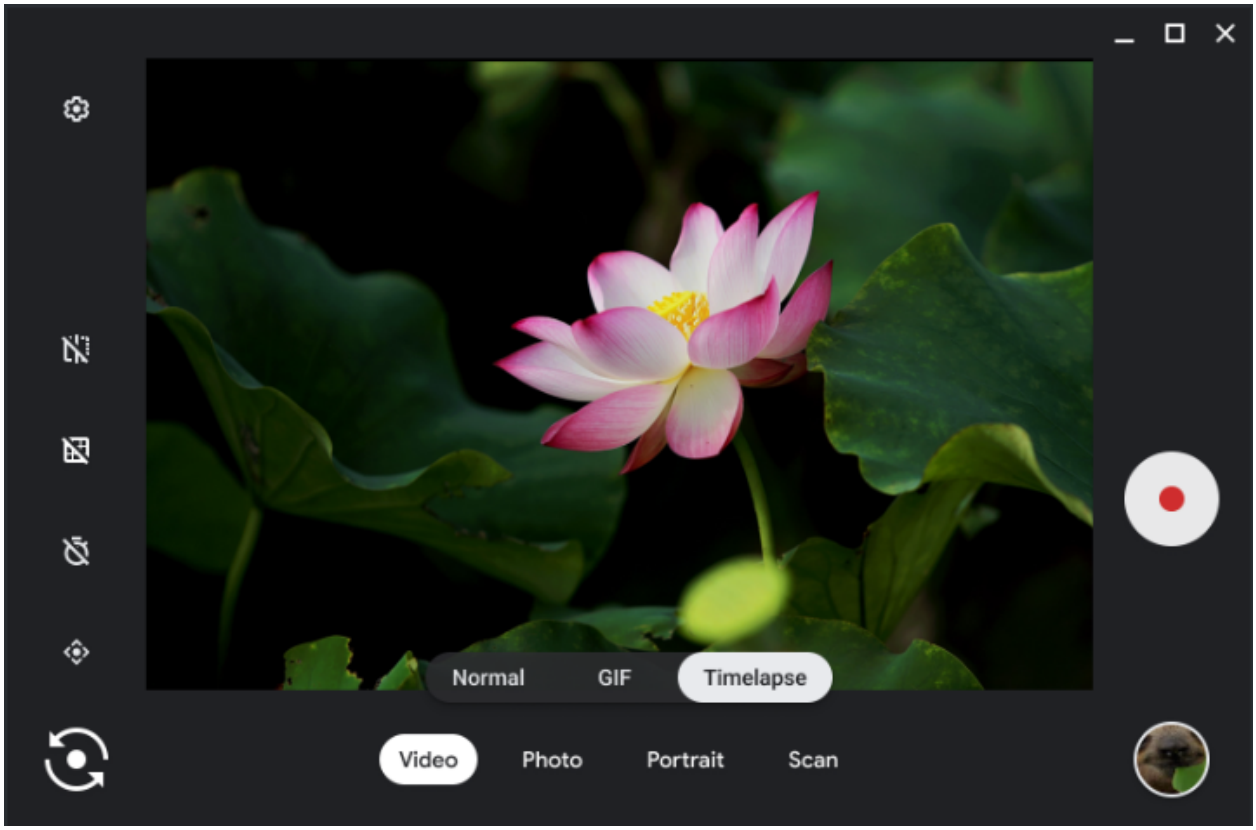
This feature enables administrators to demand managed users to enroll their non-zero touch devices by introducing a new user policy, **UserEnrollmentNudging**, which can be configured to require enrollment of the given user. If the policy is enabled and the managed user misses the enrollment step and performs first sign in on the device, a pop-up is shown suggesting to either switch to enrollment flow or use another email for sign-in, essentially preventing the managed user from signing in without enrollment.

**Replacing the Bluetooth stack on ChromeOS**

Starting in ChromeOS 117, and gradually applying to all ChromeOS devices, this Bluetooth software change brings the Android Bluetooth stack, Fluoride, to ChromeOS. The transition happens seamlessly on login, preserving existing paired devices, and should work with Bluetooth devices today with no interruptions. If you experience issues, please file feedback and, if necessary, disable the new stack via `chrome://flags/#bluetooth-use-floss`.

**Time-lapse recording**

The built-in Camera App now supports Time-Lapse recording. To use the feature, open the Camera App, select Video, then Time-Lapse. Recording can continue for as long as there is available storage space. Camera app determines the right speed for the time-lapse video based on duration recorded, to ensure your video always looks great.




**Enhanced options in clipboard history**

Enhancements to Clipboard History menu including introducing new entry points, ways to discover the feature and simplifying feature comprehension making it easier to discover and use. You can now see more detail for items in your clipboard history and can access clipboard history items nested directly in context menus. For users discovering Clipboard History for the first time, we are also introducing educational information to help with understanding this feature.

**ChromeVox dialog changes**

We've made some changes to the initial out-of-the-box experience (OOBE) dialog that explains what ChromeVox is, who might benefit from activating ChromeVox and requires

pressing **space** instead of offering an on-screen button. With this update, we hope to reduce the number of users who inadvertently activate ChromeVox.

#### Up Next Calendar view with *Join video call* integration

See your upcoming events directly from the calendar view and join any digital meetings directly with the new **Join** button.

#### Adaptive Charging

Adaptive Charging is a new ChromeOS power management feature. Devices with Adaptive Charging enabled via Settings charge to 80% and then complete charging to 100% based on an ML model's prediction for when the user will unplug their device. Reducing the time a device spends at 100% charge helps preserve the battery's health and ability to hold a charge over the lifetime of the device.

## Admin console updates

#### Printing reports now available in Chrome Management Reports API

Chrome 117 includes additional endpoints to Chrome Management Reports API that allow access to printing reports. The new endpoints provide per-user and per-printer summary printing reports, as well as a listing of all print jobs submitted to managed printers. The data provided by the new endpoints corresponds to the data in the **Print Usage** page of the Admin console. This update exposes the same data in the third-party Reports API.

**New policies in the Admin console**

| Policy Name | Pages | Supported on | Category/Field |
|---|---|---|---|
| BeforeUnloadEventCancelByPreventDefaultEnabled | User, Managed Guest | Chrome OS, Chrome Browser, Android | Legacy Site Compatibility |

# 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

**Chrome will introduce a chrome://policy/test page**

`chrome://policy/test` will allow customers to test out policies on the Beta, Dev, Canary channels. If there is enough customer demand, we will consider bringing this functionality to the Stable channel.

- **Chrome 118 on Android, iOS, Chrome OS, Linux, Mac, Windows**

**Network Service on Windows will be sandboxed**

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 118 on Windows:** Network Service sandboxed on Windows

**Removal ForceMajorVersionToMinorPositionInUserAgent policy**

Chrome plans to remove the ForceMajorVersionToMinorPositionInUserAgent policy. This policy was introduced in Chrome 99 to control whether the User-Agent string major version would be frozen at 99, in case of User-Agent string parsing bugs when the version changed to 100. Fortunately, we did not need to deploy this feature and only encountered a few minor 3-digit version parsing issues that have all since been fixed. Given that, we intend to remove this policy. If you have any feedback about this policy removal, or are aware of intranet breakage that depends on the policy, please comment on this bug.

- **Chrome 118 on Android, Chrome OS, Linux, Mac, Windows:** Removal of ForceMajorVersionToMinorPositionInUserAgent policy

**Remotely disable malicious off-store extensions**

When Enhanced Safe Browsing is enabled, users found to have a malicious off-store extension installed will have it disabled when the decision is entered on the Safe Browsing servers via either manually or by an automated detection system.

- **Chrome 118 on Chrome OS, Linux, Mac, Windows:** Feature launches

**Remove RendererCodeIntegrityEnabled policy**

The RendererCodeIntegrityEnabled policy will be removed. We recommend that you verify any potential incompatibilities with third party software by no longer applying the policy in advance of this release. You can report any issues you encounter by submitting a bug here.

- **Chrome 118 on Windows:** This policy is deprecated and will no longer take effect

**Support for passkeys in iCloud Keychain on macOS**

Chrome on macOS ≥ 13.5 will gain support for creating and using passkeys from iCloud Keychain. When signing in using WebAuthn, passkeys from iCloud Keychain will be listed as options once the user has granted Chrome the needed permission. If permission has not been granted then a generic "iCloud Keychain" option will appear that will prompt for permission before showing iCloud Keychain passkeys. If permission is denied then iCloud Keychain can still be used, but will have to be manually selected each time. When a site asks to create a platform passkey, Chrome might default to creating the passkey in iCloud Keychain based on whether iCloud Drive is in use and whether WebAuthn credentials from the current profile have been recently used. This can be controlled with a setting on `chrome://password-manager/settings`, and with the enterprise policy CreatePasskeysInICloudKeychain.

- **Chrome 118 on Mac:** The ability to use iCloud Keychain will be enabled in Chrome 118. Whether Chrome defaults to creating platform passkeys in iCloud Keychain may be altered by Finch during the lifetime of 118.

**Hash-prefix real-time lookups**

For standard Safe Browsing protection users, visited URLs now have their safety checked in real time instead of against a less frequently updated local list of unsafe URLs. This is done by sending partial hashes of the URLs to Google Safe Browsing through a proxy via Oblivious HTTP, so that the user's IP address is not linked to the partial hashes. This change improves security while maintaining privacy for users. If needed, the feature can be disabled through the policy SafeBrowsingProxiedRealTimeChecksAllowed.

- **Chrome 118 on iOS, Chrome OS, LaCrOS, Linux, Mac, Windows:** This will start with a 1% rollout and then proceed to 100% of users.

**Red interstitial facelift**

In Chrome 118, users will see minor updates to the red Safe Browsing interstitials. The main body text will include an explicit recommendation from Chrome and site ID will be specified in the details section instead of the main body. The warning icon will be replaced by the danger icon and styling will be updated to be consistent with the latest product standards. These changes will improve user comprehension of warnings.

- **Chrome 118 on Android, iOS, Chrome OS, LaCrOS, Linux, Mac, Windows**

**Form Controls Support Vertical Writing Mode**

CSS property writing-mode should be enabled for form controls elements as it will allow lines of text to be laid out horizontally or vertically and it sets the direction in which blocks progress. With this feature, we are allowing the form control elements select, meter, progress, button, textarea and input to have vertical-rl or vertical-lr writing mode. As needed for Web compatibility, we will slowly rollout the change for a number of form controls in 118 and continue in future milestones.

- **Chrome 118 on Windows, Mac, Linux, Android**

**Block all cookies set via JavaScript that contain control characters**

Updates how control characters in cookies set via JavaScript are handled. Specifically, all control characters cause the entire cookie to be rejected (previously a NULL character, a

carriage return character, or a line feed character in a cookie line caused it to be truncated instead of rejected entirely, which could have enabled malicious behavior in certain circumstances). This behavior aligns Chrome with the behavior indicated by the latest drafts of RFC6265bis. This change can be disabled using the `--disable-features=BlockTruncatedCookies` or the BlockTruncatedCookies enterprise policy, which will exist for several milestones in case this change causes any breakage.

- **Chrome 118 on Windows, Mac, Linux, Android**

**Clearer Safe Browsing protection level settings text and images**

In Chrome 118, some users will see new text describing the Safe Browsing protection level on both the Security Settings page and the Privacy Guide. The update clarifies the Enhanced Protection level by adding a table and linking to a help center article where users can learn more. The new table helps users understand the trade-offs when selecting that option versus choosing the other options. The descriptions for Standard Protection, No Protection and the password compromise warnings toggle have been simplified to make the options clearer. The Safe Browsing protection level is an existing setting and continues to be controlled by the SafeBrowsingProtectionLevel policy value.

- **Chrome 118:** Some users will see the updated text and images on the Chrome Security Settings page and on the Privacy Guide.

**WebUSB in Extension Service Workers**

Allows web developers to use WebUSB API when responding to extension events by exposing WebUSB API to Service Workers registered by browser extensions. This API will not

yet be exposed to Service Workers registered by sites but the implementation experience gained by supporting the API for extensions will be valuable for such a future project.

- **Chrome 118 on Windows, Mac, Linux**

**IP Protection Phase 0 for Chrome**

As early as Chrome 118, Chrome may route traffic for some network requests to Google-owned resources through a privacy proxy. This is an early milestone in a larger effort to protect users' identities by masking their IP address from known cross-site trackers. More information (including enterprise policies) will be provided in the near future.

**Include chrome.tabs API calls in extension telemetry reports**

When you enable Enhanced Safe Browsing, Chrome will now collect telemetry information about chrome.tabs API calls made by extensions. This information is analyzed on Google servers and further improves the detection of malicious and policy violating extensions. It will also allow better 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 (ie. disable Enhanced Safe Browsing).

- **Chrome 118 on Chrome OS, Linux, Mac, Windows:** Feature launches

**Remove non-standard appearance keywords**

Since only standard appearance keywords should be supported, we are removing the appearance (and -webkit-appearance) keywords that shouldn't be supported anymore:
* inner-spin-button
* media-slider
* media-sliderthumb
* media-volume-slider
* media-volume-sliderthumb
* push-button * searchfield-cancel-button
* slider-horizontal * sliderthumb-horizontal
* sliderthumb-vertical
* square-button

Note that value `slider-vertical` will not be removed as part of this patch; it is used for allowing `<input type=range> vertical`. It will be removed once feature **FormControlsVerticalWritingModeSupport** is enabled in Stable.

Previously, if using any of the above keywords, a console warning will be shown, but the keyword will be recognized as a valid value. With the feature enabled, the appearance property will be ignored and set to the empty string. As needed for Web compatibility, we will progressively remove the appearance keywords based on their counter usages on Chrome Status Metrics. For release 118, we will start with the following keywords, currently at page load usage below 0.001%:

* media-slider at 0.000361
* media-sliderthumb at 0.000187%
* media-volume-slider at 0.000143%
* media-volume-sliderthumb at 0.000109%

    * sliderthumb-horizontal at 0.000182%
    * sliderthumb-vertical at 0.000014%
- **Chrome 118 on Windows, Mac, Linux, Android**

**Chrome release schedule changes**

Chrome 119 and all subsequent releases will be shifted forward by one week. For example, Chrome 119 will have its early stable release on October 25 instead of Nov 1. Beta releases will also be shifted forward by one week starting in Chrome 119.

- **Chrome 119 on Android, iOS, Chrome OS, Linux, Mac, Windows**

**Permissions Prompt for Web MIDI API**

This feature gates the Web MIDI API access behind a permissions prompt. Today the use of SysEx messages with the Web MIDI API requires an explicit user permission. With this implementation, even access to the Web MIDI API without SysEx support will require a user permission. Three new policies—DefaultMidiSetting, MidiAllowedForUrls and MidiBlockedForUrls—will be available to allow administrators to pre-configure user access to the API.

- **Chrome 119 on Windows, Mac, Linux, Android**

**Migrate away from data URLs in SVG <use> element**

The SVG spec was recently updated to remove support for data: URLs in SVG <use> element. This improves security of the Web platform as well as compatibility between browsers as

Webkit does not support data: URLs in SVG <use> element. You can read more in this blog post.

For enterprises that need additional time to migrate, the DataUrlInSvgUseEnabled policy will be available temporarily to re-enable Data URL support for SVG <use> element.

- **Chrome 119 on Android, Chrome OS, LaCrOS, Linux, Mac, Windows, Fuchsia:** Remove support for data: URLs in SVG <use> element

**Chrome Browser Cloud Management: Crash Report**

The Crash Report is a new Chrome Browser Cloud Management report in the Admin console where IT admins can find a chart to easily visualize the number of crash events over time, based on the versions of Chrome that are running.

- **Chrome 119 on Android, iOS, Linux, Mac, Windows:** Crash Report launched in Chrome Browser Cloud Management

**Display banner allowing to resume last tab from other devices**

Help signed in users resume tasks when they have to switch devices during an immediate transition by offering to pick up tabs recently used on the previous device. Admins can control this feature via the existing enterprise policy called SyncTypesListDisabled.

- **Chrome 119 on iOS:** Feature launches


**Remove Sanitizer API**

The Sanitizer API aims to build an easy-to-use, always secure, browser-maintained HTML sanitizer into the platform. It is a cross-browser standardization effort starting in Q2/2020. We shipped an initial version of the Sanitizer API in Chrome 105, based on the then-current specification draft. However, the discussion has meanwhile moved on and the proposed API shape has changed substantially. In order to prevent the current API from becoming entrenched we would like to remove the current implementation.

We expect to re-implement the Sanitizer API when the proposed specification stabilizes again.

- **Use counters:** The Sanitizer API is currently used on 0.000000492% of page visits.
- **Old vs new API:** * Old explainer, API as implemented in "MVP" since Chrome 105: `https://github.com/WICG/sanitizer-api/blob/e72b56b361a31b722b4e14491a83e2d25943ba58/explainer.md` *
- **New explainer (still in progress):** `https://github.com/WICG/sanitizer-api/blob/main/explainer.md`
  - **Chrome 119 on Windows, Mac, Linux, Android**

**Tab Groups can be saved, recalled, and synced**

Users will be able to save tab groups, which will allow them to close and re-open the tabs in the group, as well as sync them across devices.

- **Chrome 119 on Chrome OS, Linux, Mac, Windows**

**Chrome profile separation: new policies**

Three new policies will be created to help enterprises configure enterprise profiles: ProfileSeparationSettings, ProfileSeparationDataMigrationSettings, ProfileSeparationSecondaryDomainAllowlist. These policies will basically be replacements for ManagedAccountsSigninRestriction, EnterpriseProfileCreationKeepBrowsingData.

- **Chrome 119 on Linux, Mac, Windows:** New profile separation policies available: ProfileSeparationSettings, ProfileSeparationDataMigrationSettings, ProfileSeparationSecondaryDomainAllowlist.

**Replace dangling markup in target name to `_blank`**

This change replaces the navigable target name (which is usually set by target attribute) to `_blank`, if it contains a dangling markup (i.e. `\n` and `<`). Which fixes a bypass in the dangling markup injection mitigation.

- **Chrome 119 on Windows, Mac, Linux, Android**

**Private Network Access restrictions for automotive**

This ships Private Network Access restrictions to Android Automotive (if BuildInfo::is_automotive), including: - Private Network Access preflight requests for subresources and Private Network Access for Workers. See Note that the two above features were shipped in warning only mode, but this features will enforce the restriction, i.e. failing the main request if restrictions are not satisfied.

- Chrome 5 on Windows, Mac, Linux
- **Chrome 119 on Android**

**Deprecate non-standard `shadowroot` attribute for declarative shadow DOM**

The standards-track `shadowrootmode` attribute, which enables declarative Shadow DOM, was shipped in Chrome 111 [1]. The older, non-standard `shadowroot` attribute is now deprecated. During the deprecation period, both attributes are functional, however the `shadowroot` attribute does not enable the new streaming behavior, whereas `shadowrootmode` allows streaming of content. There is a straightforward migration path: replace `shadowroot` with `shadowrootmode`. The old `shadowroot` attribute is deprecated as of Chrome Chrome 112, and it will be removed (no longer supported) in Chrome 119, which goes to Stable on November 1, 2023. [1] https://chromestatus.com/feature/5161240576393216

- **Chrome 119 on Windows, Mac, Linux, Android**

**Chrome on Android will no longer support Android Nougat**

The last version of Chrome that will support Android Nougat will be Chrome 119, and it includes a message to affected users informing them to upgrade their operating system. Chrome 120 will not support nor ship to users running Android Nougat.

- **Chrome 120 on Android:** Chrome on Android no longer supports Android Nougat

**Chrome Third-Party Cookie Deprecation (3PCD)**

In Chrome 120 and beyond (Jan 2024), Chrome will globally disable third-party cookies for 1% of Chrome traffic as part of our Chrome-facilitated testing in collaboration with the CMA, to allow sites to meaningfully preview what it's like to operate in a world without third-party cookies (3PCs). Most enterprise end users will be excluded from this experiment group automatically. But for the few that may be affected, enterprise admins will be able to utilize an enterprise policy to opt out their managed browsers ahead of the experiment and give enterprises time to make necessary changes to not rely on this policy or third party cookies. We plan to provide more details about this policy and provide more tooling to help identify 3PC use cases. In the meantime, refer to the 'Mode B: 1% third-party cookie deprecation' blog section for more details on how to prepare, provide feedback and report potential site issues.

- **Chrome 120 on Chrome OS, Linux, Mac, Windows**
  1% of global traffic has third party cookies disabled. Enterprise users are excluded from this automatically where possible, and a policy is available to override the change.

**Removal LegacySameSiteCookieBehaviorEnabledForDomainList policy**

In Chrome 79, we introduced the LegacySameSiteCookieBehaviorEnabledForDomainList policy to revert the SameSite behavior of cookies to legacy behavior on the specified domains. The LegacySameSiteCookieBehaviorEnabledForDomainList policy's lifetime has been extended and will be removed on the milestone listed below.

- **Chrome 127 on Android, Chrome OS, Linux, Mac, Windows:** Removal of LegacySameSiteCookieBehaviorEnabledForDomainList policy

**Intent to deprecate: Mutation Events**

Synchronous Mutation Events, including `DOMSubtreeModified`, `DOMNodeInserted`, `DOMNodeRemoved`, `DOMNodeRemovedFromDocument`, `DOMNodeInsertedIntoDocument`, and `DOMCharacterDataModified`, negatively affect page performance, and also significantly increase the complexity of adding new features to the Web. These APIs were deprecated from the spec in 2011, and were replaced (in 2012) by the much better-behaved Mutation Observer API. Usage of the obsolete Mutation Events must be removed or migrated to Mutation Observer.

- **Chrome 127 on Android, Chrome OS, Linux, Mac, Windows:** Mutation Events will stop functioning in Chrome 127, around July 30, 2024.

**Extensions must be updated to leverage Manifest V3**

Extensions must be updated to leverage Manifest V3 back to top 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 (https://developer.chrome.com/blog/more-mv2-transition/) 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. An Enterprise policy ExtensionManifestV2Availability is 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. 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 information on the Manifest timeline: https://developer.chrome.com/docs/extensions/migrating/mv2-sunset/

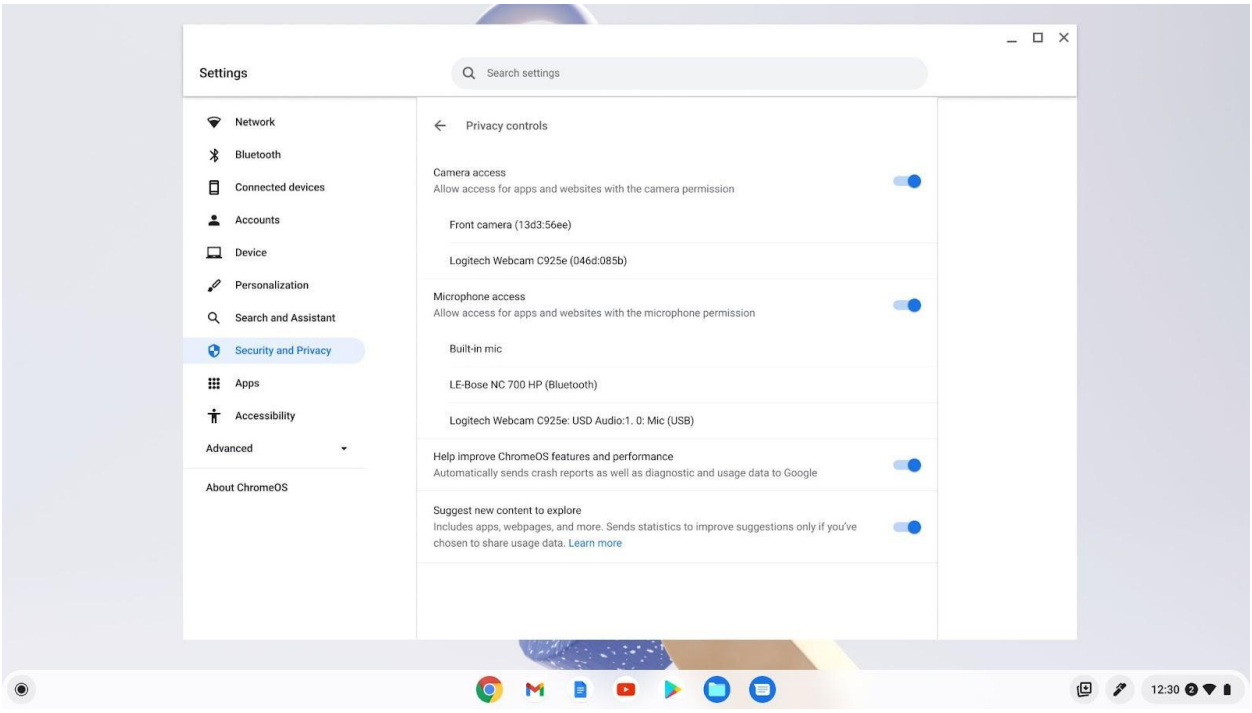
- Chrome 98 on Chrome OS, LaCrOS, Linux, Mac, Windows: Chrome Web Store stops accepting new Manifest V2 extensions with visibility set to "Public" or "Unlisted". The ability to change Manifest V2 extensions from "Private" to "Public" or "Unlisted" is removed.
- Chrome 103 on Chrome OS, LaCrOS, Linux, Mac, Windows: Chrome Web Store stops accepting new Manifest V2 extensions with visibility set to "Private".
- Chrome 110 on Chrome OS, LaCrOS, Linux, Mac, Windows: Enterprise policy ExtensionManifestV2Availability is 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.

**Future milestone on Chrome OS, LaCrOS, Linux, Mac, Windows:** Removal of ExtensionManifestV2Availability policy.

# Upcoming ChromeOS changes

### Privacy Hub

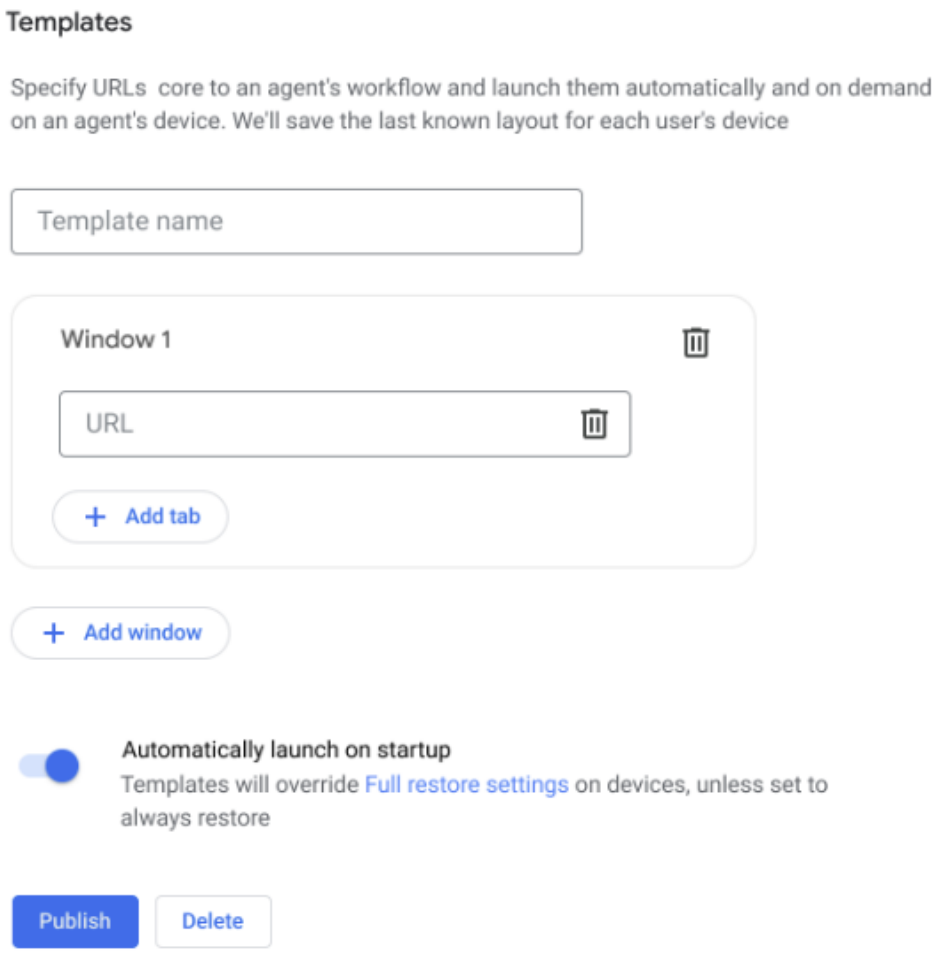
Later this year, users will be able to manage their camera and microphone settings across the operating system from one place in Settings. This way it only takes one click for users to completely turn off their camera or microphone all from one place when they need extra confidence in staying on mute.




### ChromeOS Admin templates

App Launch Automation can be configured by Administrators in the Admin console to contain groups of applications, windows and tools that can be launched automatically on startup or on-demand by users throughout their day. With App Launch Automation, you can:

get users up and running quickly at the start of their day, provide users with a way to easily get to an optimal starting point for new tasks, and remember the window layout each user sets up for their individual workflows for future use.



## Upcoming Admin console changes

**URL-keyed anonymized data collection in Kiosk mode**

The policy for URL-keyed anonymized data collection, UrlKeyedAnonymizedDataCollectionEnabled, will soon be supported in the Admin console.

This policy will be enforced starting October 1st and will remain disabled until then.

# Previous release notes

| Chrome version & targeted Stable channel release date | PDF |
|---|---|
| Chrome 116: August 09, 2023 | PDF |
| Chrome 115: July 12, 2023 | PDF |
| Chrome 114: May 24, 2023 | PDF |
| Chrome 113: Jan 10, 2023 | 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