Chrome 118 Enterprise and Education release notes

For administrators who manage Chrome browser or Chrome devices for a business or school.

These release notes were published on October 4, 2023.

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

Chrome 118 release summary

Chrome Browser updates	**Security/Privacy**	**User productivity/Apps**	**Management**
Remove *ForceMajorVersionToMinorPositionInUserAgent* policy			✓
Remotely disable malicious off-store extensions	✓		
Remove *RendererCodeIntegrityEnabled* policy			✓
Support for passkeys in iCloud Keychain on macOS		✓	✓
Hash-prefix real-time lookups	✓		
Updates to the red Safe Browsing interstitials	✓	✓	
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		✓	
Enrollment for Privacy Sandbox	✓		
Discounts shown on product pages and on Quests on the New Tab Page		✓	
Encrypted archive deep scanning for Enhanced Safe Browsing users	✓		

Flag for enabling the *chrome://policy/test* page			✓
TLS Encrypted Client Hello (ECH)	✓		
New and updated policies in Chrome browser			✓
Removed policies in Chrome browser			✓
ChromeOS updates	**Security/Privacy**	**User productivity/Apps**	**Management**
Password recovery	✓		
Tabbed PWAs		✓	
Printer setup assistance		✓	
Imprivata integration v4	✓	✓	
Touch text editing redesign		✓	
Admin Console Updates	**Security/Privacy**	**User productivity/Apps**	**Management**
New policies in the Admin console			✓
Upcoming Chrome Browser updates	**Security/Privacy**	**User productivity/Apps**	**Management**
Chrome release schedule changes			✓
Deprecate and remove WebSQL		✓	
Native Client support updates	✓		
Migrate away from data URLs in SVG <*use*> element	✓	✓	
Network Service on Windows will be sandboxed	✓		
Display banner allowing to resume last tab from other devices		✓	
Remove Sanitizer API	✓		
Tab groups can be saved, recalled, and synced		✓	

Chrome profile separation: new policies			✓
Private Network Access restrictions for automotive	✓		
Deprecate non-standard *shadowroot* attribute for declarative shadow DOM	✓		
Remove support for UserAgentClientHintsGREASEUpdateEnabled			✓
Revamped Safety Check on Desktop	✓		
Permissions prompt for Web MIDI API	✓		
Default Search Engine choice screen		✓	
Shifting UI strings in Chrome from Clear to Delete when getting rid of data			✓
DevTools internal errors will be reported to Chrome internal crash reporting			✓
SharedImages for PPAPI Video Decode	✓		
Private Aggregation API bundled enhancements	✓		✓
Remove Authorization header upon cross-origin redirect	✓		
Desktop Responsive Toolbar		✓	
Chrome on Android will no longer support Android Nougat			✓
Chrome Third-Party Cookie Deprecation (3PCD)	✓		
IP Protection Phase 0 for Chrome	✓		

Apps & Extensions Usage Report: Highlight extensions removed from the Chrome Web Store			✓
Remove LegacySameSiteCookieBehaviorEnabledForDomainList policy			✓
Intent to deprecate: Mutation Events		✓	
Extensions must be updated to leverage Manifest V3	✓	✓	✓
Upcoming ChromeOS updates	**Security/Privacy**	**User productivity/Apps**	**Management**
Privacy Hub	✓		
ChromeOS Admin templates			✓
Upcoming Admin Console Updates	**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

Remove ForceMajorVersionToMinorPositionInUserAgent policy

Chrome 118 removes 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 can now remove this policy. If you have any feedback about this policy removal, or are aware of intranet functionality that depends on the policy, comment on this bug.

- **Chrome 118 on Android, ChromeOS, Linux, Mac, Windows:** Remove ForceMajorVersionToMinorPositionInUserAgent policy

Remotely disable malicious off-store extensions

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

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

Remove RendererCodeIntegrityEnabled policy

The Renderer Code Integrity security feature is no longer controlled by the RendererCodeIntegrityEnabled policy; it is now switched on by default. We recommend that you verify any potential incompatibilities with third party software by no longer using the policy in advance of this release. To report any issues you encounter, submit 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 now supports creating and using passkeys from iCloud Keychain. When signing in using WebAuthn, passkeys from iCloud Keychain are listed as options once the user has granted Chrome the needed permission. If permission has not been granted, a generic **iCloud Keychain** option appears that prompts for permission before showing iCloud Keychain passkeys. If permission is denied, the iCloud Keychain can still be used, but it has 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:** Chrome 118 supports iCloud Keychain. Whether Chrome defaults to creating platform passkeys in iCloud Keychain can be altered by Chrome Variations during the lifetime of 118.

Hash-prefix real-time lookups

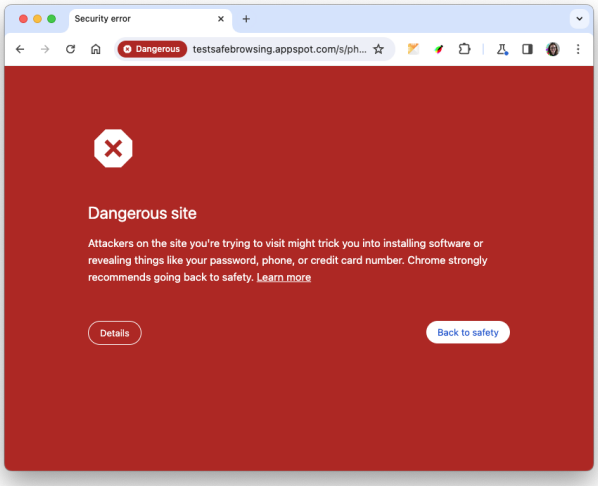
For standard Safe Browsing protection users, visited URLs now have their safety checked in real time, instead of less frequently using an updated local list of unsafe URLs. This is done by sending partial hashes of the URLs to Google Safe Browsing through a proxy via Oblivious HTTP, so that the user's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

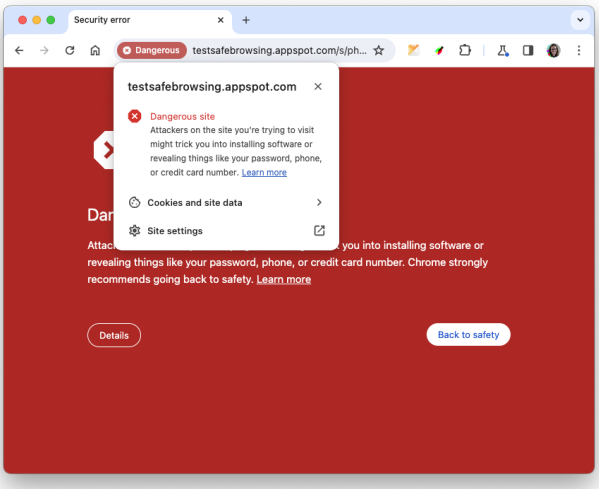
- **Chrome 118 on iOS, ChromeOS, LaCrOS, Linux, Mac, Windows**

Updates to the red Safe Browsing interstitials

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

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





Form controls support vertical writing mode

The CSS property `writing-mode` should be enabled for form controls elements as it allows 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 now begin to slowly roll out the change for a number of form controls in 118, and we will continue in future milestones.

You can control this feature with the following command line flags:

```
--enable-features= FormControlsVerticalWritingModeSupport

--enable-features= FormControlsVerticalWritingModeTextSupport
```

- **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.

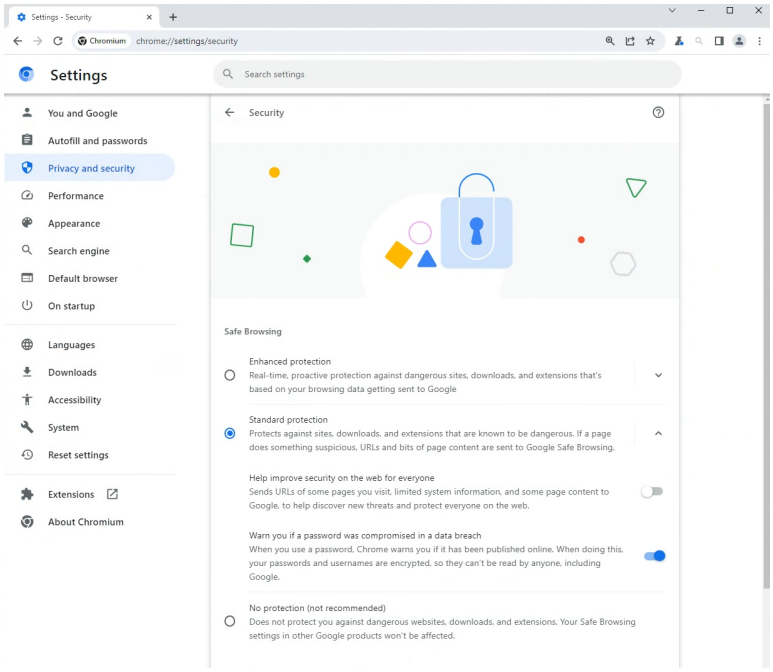
You can control this feature using the `--disable-features=BlockTruncatedCookies` or the BlockTruncatedCookies enterprise policy, which will be available for several milestones in case this change causes any breakage.

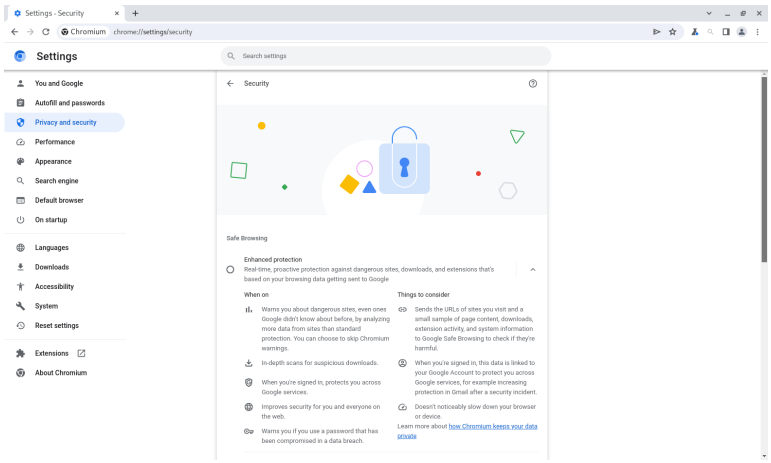
- **Chrome 118 on Windows, Mac, Linux, Android**

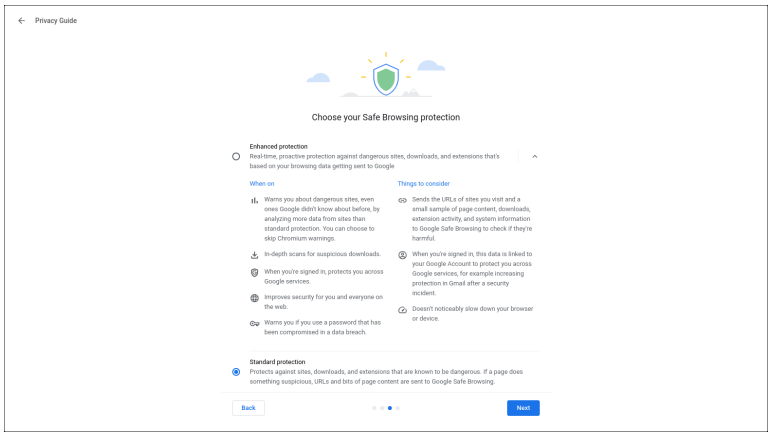
Clearer Safe Browsing protection level settings text and images

In Chrome 118, some users 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 feature, still controlled by the SafeBrowsingProtectionLevel policy.

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


Settings - Security
Chromium
chrome://settings/security
Settings
Search settings
You and Google
Autofill and passwords
Privacy and security
Performance
Appearance
Search engine
Default browser
On startup
Languages
Downloads
Accessibility
System
Reset settings
Extensions
About Chromium
Security
Safe Browsing
Enhanced protection
Real-time, proactive protection against dangerous sites, downloads, and extensions that's based on your browsing data getting sent to Google
Standard protection
Protects against sites, downloads, and extensions that are known to be dangerous. If a page does something suspicious, URLs and bits of page content are sent to Google Safe Browsing.
Help improve security on the web for everyone
Sends URLs of some pages you visit, limited system information, and some page content to Google, to help discover new threats and protect everyone on the web.
Warn you if a password was compromised in a data breach
When you use a password, Chrome warns you if it has been published online. When doing this, your passwords and usernames are encrypted, so they can't be read by anyone, including Google.
No protection (not recommended)
Does not protect you against dangerous websites, downloads, and extensions. Your Safe Browsing settings in other Google products won't be affected.


Settings - Security
Chromium
chrome://settings/security
Settings
Search settings
Security
Safe Browsing
Enhanced protection
When on
Things to consider
Learn more about how Chromium keeps your data private


Privacy Guide
Choose your Safe Browsing protection
Enhanced protection
When on
Things to consider
Standard protection
Protects against sites, downloads, and extensions that are known to be dangerous. If a page does something suspicious, URLs and bits of page content are sent to Google Safe Browsing.
Back
Next

WebUSB in Extension Service Workers

Web developers can use the WebUSB API when responding to extension events by exposing WebUSB API to Service Workers registered by browser extensions. This API is not yet 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, ChromeOS**

Include chrome.tabs API calls in extension telemetry reports

When you switch on Enhanced Safe Browsing, Chrome now collects 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 also allows better protection for all Chrome extension users. You can turn off this functionality along with the extension telemetry feature by setting SafeBrowsingProtectionLevel to any value other than 2, which turns off Enhanced Safe Browsing.

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

Remove non-standard appearance keywords

Since only standard appearance keywords should be supported, Chrome 118 removes appearance (and -webkit-appearance) keywords, including:

```
* 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 appeared, but the keyword was 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 Chrome 118, we 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**

Enrollment for Privacy Sandbox

As the Privacy Sandbox relevance and measurement APIs start ramping up for general availability, we want to make sure these technologies are used as intended and with transparency. The APIs include Attribution Reporting, the Protected Audience API, Topics, Private Aggregation and Shared Storage. Privacy Sandbox is introducing a new Developer Enrollment process for Privacy Sandbox relevance and measurement APIs. Chrome will fetch the enrolled-sites list from the enrollment server (via component updater) and use it to gate access to the Privacy Sandbox APIs.

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

Discounts shown on product pages and on Quests on the *New tab* page

Starting in Chrome 118, users sometimes see discounts, shown as annotations on page visits, in the Quests cards shown on the **New tab** page. Clicking through on the discount shows the relevant information on the product page. Quests as a whole are controlled by the NTPCardsVisible policy. Users also sometimes see discounts directly on the product page, available through an icon in the Omnibox.

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

Encrypted archive deep scanning for Enhanced Safe Browsing users

Google Chrome offers deep scanning of some suspicious downloads to users who have opted in to Enhanced Safe Browsing. This sends the file content to Safe Browsing for a real-time evaluation of the file's safety. Starting in Chrome 118, deep scans of encrypted archives, for example, ZIP and RAR files, prompt the user to provide the archive password along with the file content. This is necessary for Safe Browsing to provide a useful verdict about the contents of the archive. Enterprises who do not want to see this prompt can prevent users from enabling Enhanced Safe Browsing with the SafeBrowsingProtectionLevel policy. Starting in Chrome 119, enterprises who want to switch off file deep scans while still enabling Enhanced Safe Browsing can do so with the **SafeBrowsingDeepScanningEnabled** policy.

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

Flag for enabling the chrome://policy/test page

The `#enable-policy-test-page` flag allows admins and developers to use the `chrome://policy/test` page to more easily test policies on the Beta, Dev, Canary channels.

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

TLS Encrypted Client Hello (ECH)

The TLS Encrypted ClientHello (ECH) extension allows 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. If you notice any incompatibilities, you can use the EncryptedClientHelloEnabled enterprise policy to disable support for ECH.

- **Chrome 118 on Chrome OS, Linux, Mac, Windows:** rolled out to 100% of users

New and updated policies in Chrome browser

Policy	Description
BlockTruncatedCookies	Block truncated cookies
CompressionDictionaryTransportEnabled	Enable compression dictionary transport support
CreatePasskeysInICloudKeychain	Control whether passkey creation will default to iCloud Keychain.
LegacyTechReportAllowlist	Specifies URLs that allow legacy technology report
SafeBrowsingProxiedRealTimeChecksAllowed	Allow Safe Browsing Proxied Real Time Checks

Removed policies in Chrome browser

Policy	Description

ForceMajorVersionToMinorPositionInUserAgent	Freeze User-Agent string major version at 99
RendererCodeIntegrityEnabled	Enable Renderer Code Integrity

ChromeOS updates

Password recovery

ChromeOS users who have forgotten their password can now recover their account along with all associated local data. Gone are the days where all local data is lost when a password has been forgotten! You can control this feature with the RecoveryFactorBehavior policy.

Tabbed PWAs

Developers can now choose to display their Progressive Web App (PWA) in *tabbed* mode, allowing users to manage and navigate multiple documents within a single window using a familiar tab strip. Developers should also specify a home tab where appropriate, which provides a consistent place for users to access documents and settings.

Printer setup assistance

To simplify a user's printing journey, ChromeOS provides more in context help when it comes to using their printer: an easier way to save printers, new set up instructions and help content, printer status directly integrated on the settings page. Moreover, we now also provide users an easy route to manage their printer when they face issues with it while trying to print.

Imprivata integration v4

For caregivers, Imprivata OneSign compatibility with Google ChromeOS devices and the Chrome browser means fast, secure access, and better cost efficiency. This fourth version of Imprivata integration, Imprivata v4, adds deployment, stability, and workflow improvements. It improves support for assigned devices by allowing for Imprivata sign-in to ChromeOS user sessions. In addition, ChromeOS 118 now supports all 12 languages of Imprivata and SPINE workflows.

Touch text editing redesign

Improved text editing interaction with user's fingers on the touchscreen, including a much more intuitive gesture system, usability improvements around gesture intentions and text legibility, a brand new magnifier that automatically shows cursor position with precision.

Admin console updates

New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
ForcePermissionPolicyUnloadDefaultEnabled	User, Managed Guest Session	Chrome (Android) Chrome (Linux, Mac, Windows) ChromeOS	Legacy site compatibility
SafeBrowsingSurveysEnabled	User, MGS	Chrome (Linux, Mac, Windows) ChromeOS	Chrome safe browsing
EmojiPickerGifSupportEnabled	User, MGS	Chrome (Linux, Mac, Windows) ChromeOS	User experience
ColorCorrectionEnabled	User, MGS	ChromeOS	User accessibility
CreatePasskeysInICloudKeychain	User, MGS	Chrome (Mac)	Content
SafeBrowsingProxiedRealTimeChecksAllowed	User, MGS	Chrome (Linux, Mac, Windows) ChromeOS, Chrome (iOS and iPadOS)	Chrome safe browsing

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 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, ChromeOS, Linux, Mac, Windows**

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.

Native Client support updates

Native Client NaCl support was removed from extensions on Windows, macOS, and Linux. A temporary enterprise policy is available, NativeClientForceAllowed, which allows 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

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 until Chrome 128 to re-enable Data URL support for SVG `<use>` element.

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

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 119 on Windows:** Network Service sandboxed on Windows

Display banner allowing to resume last tab from other devices

Help signed in users resume tasks when they have to switch devices immediately 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. We shipped an initial version of the Sanitizer API in Chrome 105, based on the then-current specification draft. However, the standards discussion has meanwhile moved on and the proposed API shape has changed substantially. To prevent the

current API from becoming entrenched, we plan to remove the current implementation. We expect to re-implement the Sanitizer API when the proposed specification stabilizes again.

- **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. You can disable syncing Tab Groups using the SyncTypesListDisabled policy.

- **Chrome 119 on ChromeOS, 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 be simpler to use and will replace ManagedAccountsSigninRestriction and EnterpriseProfileCreationKeepBrowsingData.

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

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. Note that the two above features were shipped in warning only mode, but these features will enforce the restriction, that is, failing the main request if restrictions are not satisfied.

- **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 (ChromeStatus). 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 112, and it will be removed (no longer supported) in Chrome 119, which goes to Stable on November 1, 2023.

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

Remove support for UserAgentClientHintsGREASEUpdateEnabled

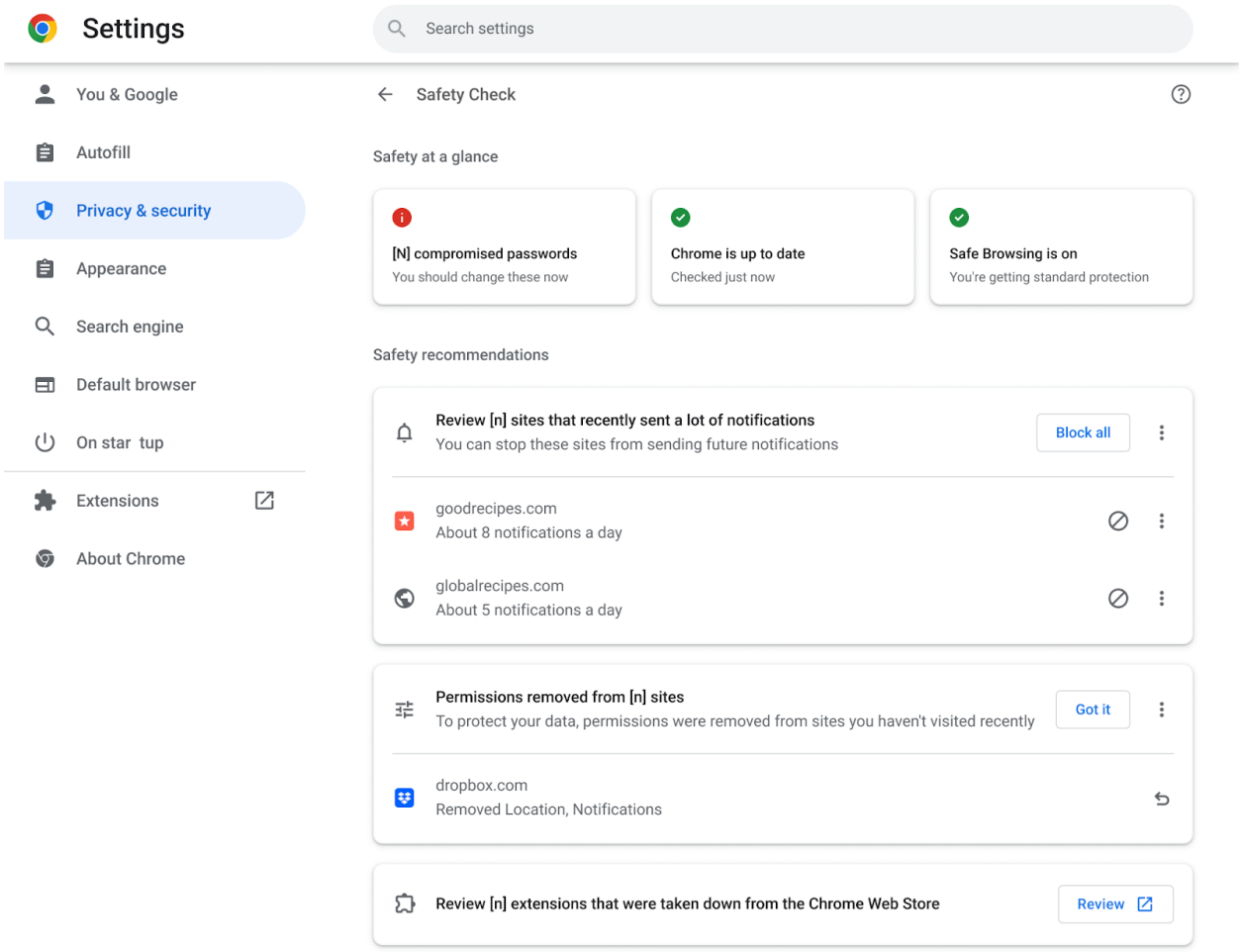
Deprecate the UserAgentClientHintsGREASEUpdateEnabled policy since the updated GREASE algorithm has been on by default for over a year and then eventually remove it.

- **Chrome 119 on Android, ChromeOS, Linux, Mac, Windows:** Policy is deprecated
- Chrome 122 on Android, ChromeOS, Linux, Mac, Windows: Policy is removed

Revamped Safety Check on Desktop

We plan to introduce a new proactive **Safety Check** that regularly checks the browser for safety related issues and informs users when there's anything that needs their attention. Our **Safety Check** launch also introduces a new page with Chrome's proactive safety-related actions and information tailored to each user, designed to make it easier for users to stay safe online.

- **Chrome 120 on ChromeOS, LaCrOS, 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 120 on Windows, Mac, Linux, Android**

Default Search Engine choice screen

As early as Chrome 119, enterprise end-users may be prompted to choose their default search engine within Chrome.
As part of our building for DMA compliance, some users will be prompted to choose their default search engine for Chrome. This prompt controls the default search engine setting, currently available at `chrome://settings/search`. The enterprise policies, DefaultSearchProviderEnabled and DefaultSearchProviderSearchUrl, will continue to control this setting as it does today, if it is set by the IT admin. Read more on this policy and the related atomic group.

- **Chrome 119 on iOS, ChromeOS, LaCrOS, Linux, Mac, Windows:** 1% users will start getting the choice screen with Chrome 119. 100% by Chrome 122

Shifting UI strings in Chrome from *Clear* to *Delete* when getting rid of data

Chrome is updating settings text to reflect *delete* instead of *clear* when referring to the destruction of data. We expect the change will improve user comprehension. Users who intend to get rid of data should feel reassured that the data is actually *deleted* and not just *cleared* from one view but accessible elsewhere.

- **Chrome 119 on Android, iOS, ChromeOS, Mac, Windows:** The earliest milestone that users may see these changes is 119.

DevTools internal errors will be reported to Chrome internal crash reporting

To improve Chrome's stability, DevTools internal errors will be reported through Chrome's existing crash reporting pipeline. This will provide visibility into the stability of the Chrome DevTools. Admins can control all crash reporting, including these errors, using the MetricsReportingEnabled enterprise policy.

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

SharedImages for PPAPI Video Decode

The **PPAPISharedImagesForVideoDecoderAllowed** policy controls the recent refactor for VideoDecoder APIs in PPAPI plugin. The migration only affects internal implementation details and should not change any behavior. However, this policy can be used in case any PPAPI applications do not work as expected.

When the policy is left unset or set to Enabled, the browser will decide which implementation is used.
When the policy is set to Disabled, Chrome will use the old implementation until the policy expires.

NOTE: Only newly-started renderer processes will reflect changes to this policy while the browser is running.

- **Chrome 119 on ChromeOS, LaCrOS:** Escape hatch policy introduced.
- Chrome 122 on ChromeOS, LaCrOS: Escape hatch policy and corresponding old code paths are removed.

Private Aggregation API bundled enhancements

We're planning a few bundled changes to Private Aggregation:
- **Null report fixes:** Currently reports with no contributions are inadvertently dropped. This change ensures that, when a context ID is specified, a null report is sent even if budget is denied. Separately, it fixes a bug causing budget to always be denied for null reports.
- **Debug mode eligibility changes:** Currently, debug mode is always available. This change only allows debug mode for callers that are allowed access to third-party cookies, silently dropping the debug mode otherwise. Note that this will allow debug mode to automatically sunset when third-party cookies are deprecated.
- **Padding report payloads:** To avoid the payload size being dependent on the number of contributions, we will pad it with 'null' contributions to a fixed length. Note that this change will also affect Attribution Reporting reports.

- **Reducing delay:** When a context ID is specified, we remove the randomized 10-60 minute delay, which is superfluous as a report is always sent in this case. Instead, we just wait until the Shared Storage operation timeout.

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

Remove Authorization header upon cross-origin redirect

The Fetch standard has been updated to remove Authorization header on cross origin redirects. Chrome should follow the spec change.

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

Desktop Responsive Toolbar

As early as Chrome 120, Chrome Desktop customers across form factors and input modalities (e.g. Mouse, Touch) will experience a toolbar that seamlessly responds to changing window sizes albeit by manually selecting and dragging a window smaller/larger or using operating system specific window management tools.

- **Chrome 120 on ChromeOS, LaCrOS, Linux, Mac, Windows**

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 ChromeOS, 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.

IP Protection Phase 0 for Chrome

As early as Chrome 122, 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) can be found in the explainer. Enterprise policies will be in place to allow admins to disable the feature before it's launched.

- **Chrome 122 on ChromeOS, Linux, Mac, Windows, Android**

Apps & Extensions Usage Report: Highlight extensions removed from the Chrome Web Store

Chrome is adding new information on the Apps & Extensions Usage Report to help you identify if an extension was recently removed from the Chrome Web Store. On the App Details page, you can find the reason why an extension was removed from the Chrome Web

Store. This feature will help IT administrators identify the impact of using the policy to disable unpublished extensions.

- **Chrome 122 on LaCrOS, Linux, Mac, Windows**

Remove 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, ChromeOS, Linux, Mac, Windows:** Remove 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, ChromeOS, 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. 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 , 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. Read more on the Manifest timeline, including:

- Chrome 98 on ChromeOS, 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 ChromeOS, LaCrOS, Linux, Mac, Windows: Chrome Web Store stops accepting new Manifest V2 extensions with visibility set to "Private".
- Chrome 110 on ChromeOS, 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.

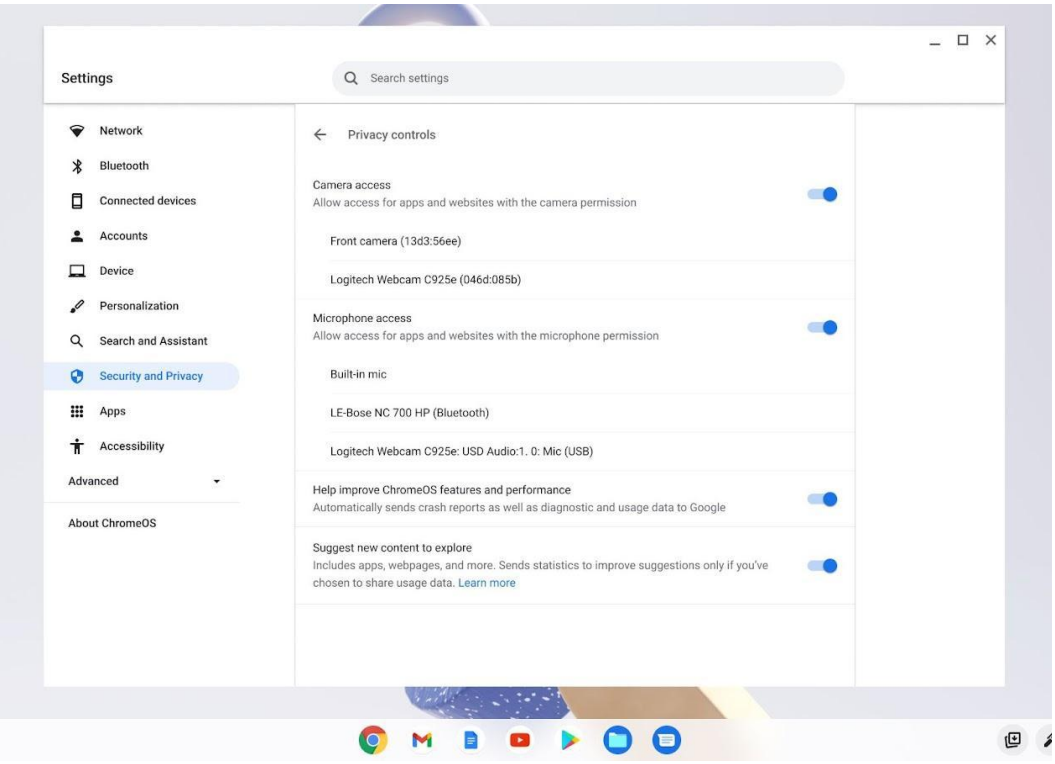
Future milestone on ChromeOS, LaCrOS, Linux, Mac, Windows: Remove ExtensionManifestV2Availability policy.

Upcoming ChromeOS changes

Privacy Hub

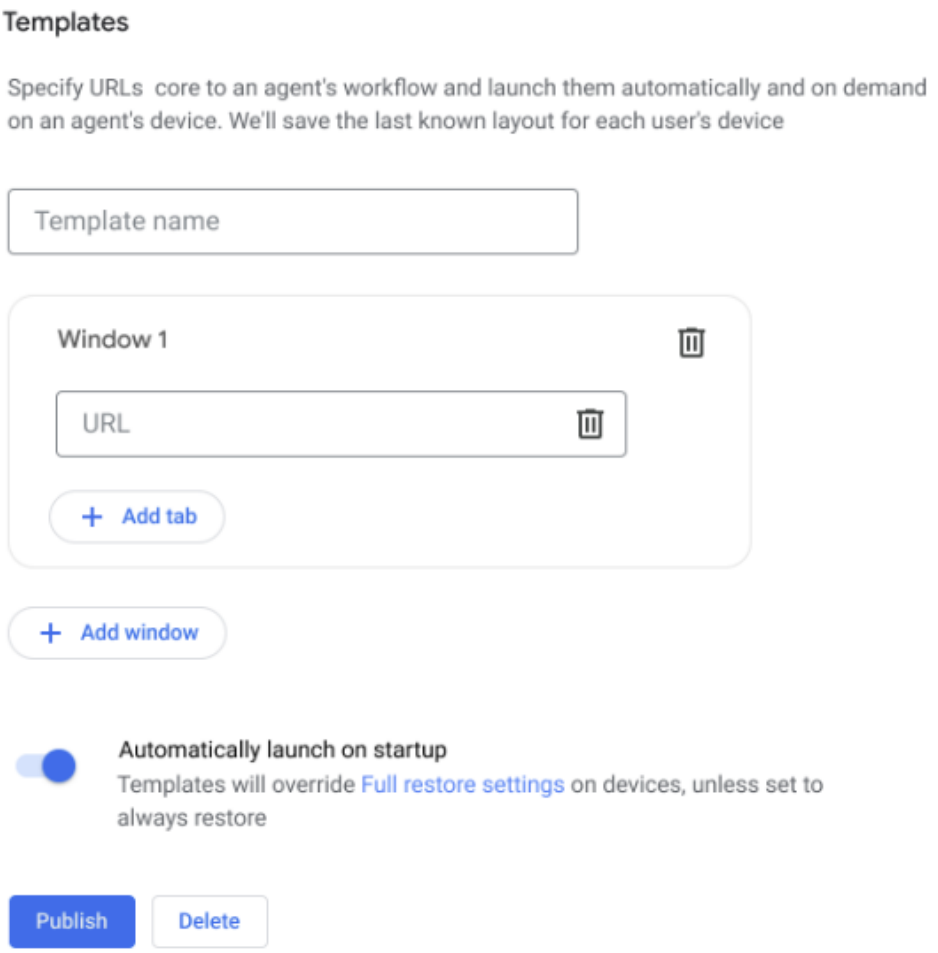
Later this year, users will be able to manage their camera and microphone settings across the operating system from one place in **Settings**. This way it only takes one click for users to

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 117: September 08, 2023	PDF
Chrome 116: August 09, 2023	PDF
Chrome 115: July 12, 2023	PDF
Chrome 114: May 24, 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