chrome enterprise

Chrome 130 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 9, 2024.

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

Chrome 130 release summary

Current Chrome browser changes	Security / Privacy	User productivity / Apps	Management
Desktop toasts		✓	
Platform picker for screen sharing on macOS		✓	
New Account menu		✓	
PDF Viewer on Android		✓	
Tab freezing on Energy saver		✓	
Compression dictionary transport with Shared Brotli and Shared Zstandard	✓		
Keyboard-focusable scroll containers		✓	
Support non-special scheme URLs	✓		
Chrome on Android now supports 3P autofill and password providers		✓	✓
<meter> element fallback styles	✓		
New and updated policies in Chrome browser			✓
Current Chrome Enterprise Core changes	**Security/Privacy**	**User productivity/Apps**	**Management**
GenAI Defaults policy			✓
Support for user-level settings on Custom configurations			✓
Audit-only URL navigation rules			✓
Chrome Security Insights	✓		✓

Extension risk score Phase 2	✓		✓
Current Chrome Enterprise Premium changes	**Security/Privacy**	**User productivity/Apps**	**Management**
No updates in Chrome 130.			
Upcoming Chrome browser changes	**Security / Privacy**	**User productivity / Apps**	**Management**
Search and receive answers in your Chrome history with AI		✓	
Ad-hoc code signatures for PWA shims on macOS		✓	
Asynchronous real-time Safe Browsing check	✓		
Remove non-standard GPUAdapter requestAdapterInfo() method	✓		
Deprecate Safe Browsing Extended reporting	✓		
Update Google Play Services to fix issues with on-device passwords			✓
Entrust certificate distrust	✓		
Simplified sign-in and sync experience		✓	✓
User Link capturing on PWAs		✓	✓
Deprecation of CSS Anchor Positioning property *inset-area*	✓		
X25519Kyber768 key encapsulation for TLS	✓		
Chrome PDF Viewer OCR		✓	
Insecure form warnings on iOS	✓		

Network Service on Windows will be sandboxed			✓
Read aloud in Reading mode		✓	
Capture all screens			✓
SafeBrowsing API v4 to v5 migration	✓		
Private network access checks for navigation requests: warning-only mode			✓
Deprecate mutation events	✓		✓
UI Automation accessibility framework provider on Windows		✓	
Upcoming Chrome Enterprise Core changes	**Security / Privacy**	**User productivity / Apps**	**Management**
Chrome extension telemetry integration with Google SecOps	✓		✓
Remove enterprise policy used for legacy same site behavior			✓
Default change for GenAI policies			✓
Upcoming Chrome Enterprise Premium changes	**Security/Privacy**	**User productivity/Apps**	**Management**
Chrome Enterprise Data Controls: Clipboard	✓		
Screenshot protections	✓		

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. Allow 1 to 2 weeks for translation for some languages.

Chrome Enterprise and Education release notes are published in line with the Chrome release schedule, on the Early Stable date for Chrome browser.

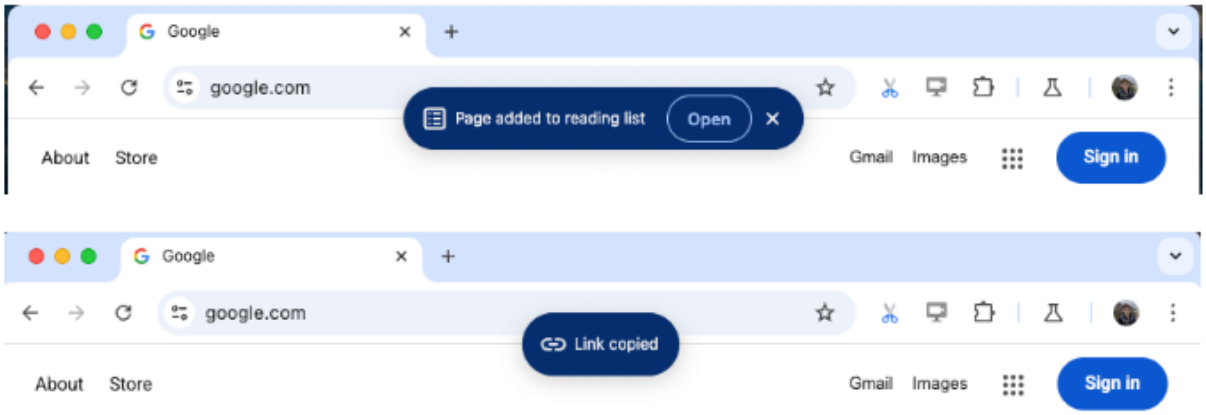
Current Chrome version release notes

Current Chrome browser changes

Desktop toasts

Chrome 130 introduces a new Toast pattern that will allow features to provide visual confirmation of user actions or a quick way to take a follow up action. For example, when adding something to a reading list, a Toast confirms that the item was added and offers a quick link to the reading list side panel. Toasts appear as a small chip that partially overlaps with the web contents and partially with the top toolbar of the browser.

- **Chrome 130 on ChromeOS, Linux, macOS, Windows:** This will be enabled for an initial set of features in Chrome 130. Subsequent toasts will be rolled out independently by other teams utilizing the pattern.



Platform picker for screen sharing on macOS

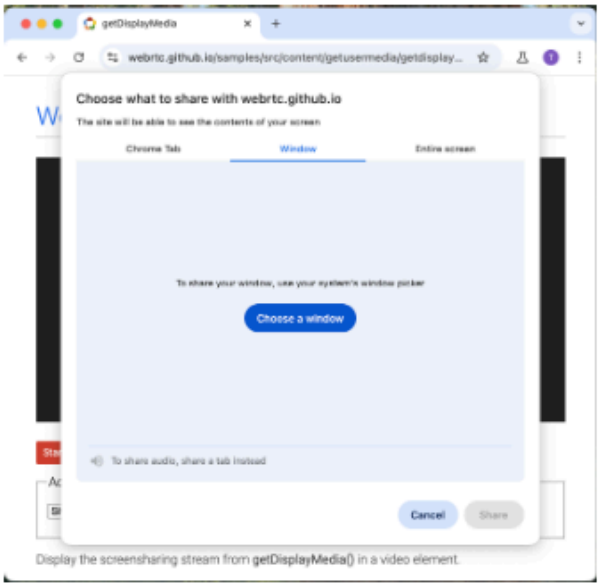
When screen sharing in Chrome on macOS X Sequoia, users can now select a window or screen to share using the updated platform picker. This new platform picker removes the need for assigning screen recording permission to Chrome and is consistent with screen sharing in other macOS applications.
The new picker will not be activated before the first update of macOS Sequoia, version 15.1 expected a month after the initial version of 15.0. Before that Chrome users might see a warning dialog that Chrome is not using the new picker API yet.

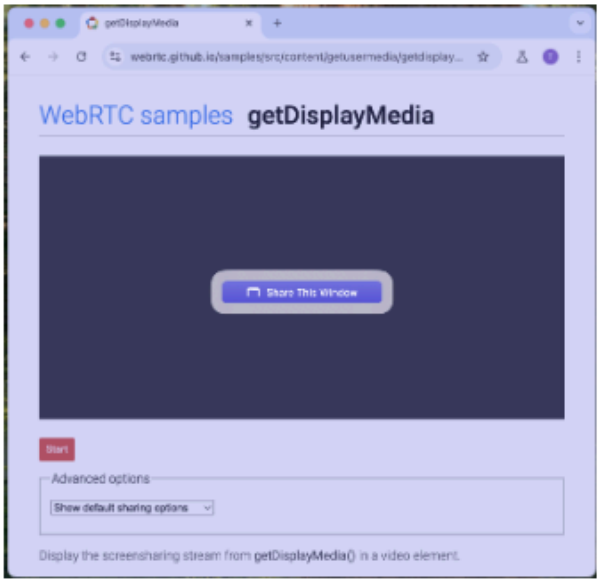
To test the new screen share picker experience:

1. Update Chrome to version 129 or later.
2. On your macOS, open the Terminal.
3. At the prompt, type: `open -b com.google.Chrome --args -enable-features=UseSCContentSharingPicker`
4. To execute the command, on your keyboard, press **Enter**.

The feature can also be enabled in `chrome://flags`.

- **Chrome 130 on macOS**

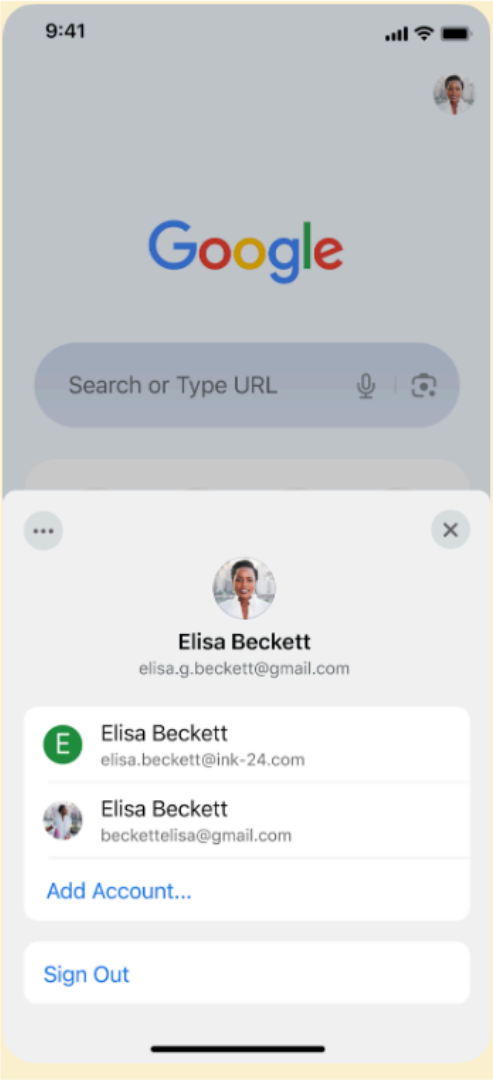




New Account menu

Some users can now access a new **Account** menu by tapping on their avatar on the **New tab** page. The new **Account** menu allows them to sign out, switch accounts easily and resolve errors related to their account in Chrome. Existing policies like BrowserSignin and RestrictAccountsToPatterns can be used to determine which accounts a user can sign in or switch to.

- **Chrome 130 on iOS**



PDF Viewer on Android

This feature provides the ability to view PDFs within Chrome browser UI. Prior to this change, users have to complete many steps to view a PDF document. These steps force them out of Chrome to view the PDF document. With this feature, PDFs will render seamlessly in Chrome. Users will still be able to download PDFs and open with other first- or third-party apps of choice.

- **Chrome 130 on Android**

Tab freezing on Energy saver

When Energy saver is active, Chrome now freezes a tab that has been hidden and silent for >5 minutes and uses a lot of CPU, unless:

- the tab provides audio- or video- conferencing functionality (detected via microphone, camera or screen, window, or tab capture, or an RTCPeerConnection with an *open* RTCDataChannel or a *live* MediaStreamTrack).
- the tab controls an external device (detected using Web USB, Web Bluetooth, Web HID or Web Serial).

This will extend battery life and speed up Chrome through reduced CPU usage.

- **Chrome 130 on ChromeOS, Linux, macOS, Windows:** The feature can be tested in Chrome 130 via the `#freezing-on-energy-saver entry` in `about:flags`. Alternatively, it can be tested with the `#freezing-on-energy-saver-testing` which simulates that Energy saver is active and that all tabs use a lot of CPU (this allows verifying whether a tab is eligible for freezing and would be frozen if it used a lot of CPU). Energy saver availability can be controlled via the BatterySaverModeAvailability policy (this change has no effect when Energy saver is inactive).
- Chrome 131 on ChromeOS, Linux, macOS, Windows: The feature will start rolling out to 1% of Stable in Chrome 131. It will gradually be ramped up to 100% of Stable. Energy saver availability can be controlled via the BatterySaverModeAvailability policy (this change has no effect when Energy saver is inactive).

Compression dictionary transport with Shared Brotli and Shared Zstandard

This feature adds support for using designated previous responses as an external dictionary for content encoding compressing responses with Brotli or Zstandard.

Enterprises might experience potential compatibility issues with enterprise network infrastructure that intercepts HTTPS traffic and is sensitive to unknown content encodings. The enterprise policy CompressionDictionaryTransportEnabled is available to turn off the compression dictionary transport feature.

- **Chrome 130 on Windows, macOS, Linux, Android**

Keyboard-focusable scroll containers

Chrome 130 improves accessibility by making scroll containers focusable using sequential focus navigation. Today, the tab key doesn't focus scrollers unless `tabIndex` is explicitly set to 0 or more.

By making scrollers focusable by default, users who can't (or don't want to) use a mouse can now focus clipped content using tab and arrow keys. This behavior is enabled only if the scroller does not contain any keyboard-focusable children. This logic is necessary so we don't cause regressions for existing focusable elements that might exist within a scroller like a `<textarea>`.

Note: The previous rollout of this feature (started in Chrome 127) was stopped due to web compatibility issues, which should be fixed in the implementation shipping in Chrome 130.

- **Chrome 130 on Windows, macOS, Linux, Android**

Support non-special scheme URLs

Chrome 130 supports non-special scheme URLs, for example, `git://example.com/path`. Previously, the Chromium URL parser didn't support non-special URLs. The parser parses non-special URLs as if they had an opaque path, which is not aligned with the URL standard. Now, the Chromium

URL parser parses non-special URLs correctly, following the URL standard. For more details, see http://bit.ly/url-non-special.

- **Chrome 130 on Windows, macOS, Linux, Android**

Chrome on Android now supports third-party autofill and password providers

Until now, third-party autofill and password providers could be used in Chrome on Android via accessibility APIs. In Chrome 130, we're adding direct support for Android Autofill which means these providers now work with Chrome on Android without the need for accessibility APIs. This should improve the performance of Chrome on Android. To take advantage of this, users need to ensure they have their third party provider configured in Android settings. Then, in Chrome they'll need to open **Settings > Autofill services** and choose **Autofill using another service**. If users do not change **both** settings, they will continue to use Google to autofill their passwords, payment and address information.

- **Chrome 130 on Android:** The new setting will be available from Chrome 130. If users use the new setting it will take immediate effect. If the new setting is not used, users will continue to use either Google and a third party via accessibility (if installed). The support for accessibility APIs will be deprecated in early 2025, at which point the new settings will be honored for all users.

<meter> element fallback styles

In Chrome 130, <meter> elements with `appearance: none` now have a reasonable fallback style that matches Safari and Firefox, instead of just disappearing from the page. Additionally, developers can now custom style the <meter> elements.

A feature flag `MeterAppearanceNoneFallbackStyle` is available in `chrome://flags` until Chrome 133 to control this feature.

- **Chrome 130 on Windows, macOS, Linux, Android**

New policies in Chrome browser

Policy	Description
GenAiDefaultSettings	Set the default policy value for Google Chrome's covered Generative AI features
DataURLWhitespacePreservationEnabled	DataURL Whitespace Preservation for all media types
CloudProfileReportingEnabled	Enable Google Chrome cloud reporting for managed profile

Current Chrome Enterprise Core changes

GenAI Defaults policy

Starting in 130, Chrome Enterprise Core offers a policy to control the default behavior of multiple GenAI policies via our Trusted Tester program. You can sign up for our Trusted Tester program here. This policy does not impact any manually-set policy values for generative AI features. This policy controls the default settings for following policies:

- CreateThemesSettings
- DevToolsGenAiSettings
- HelpMeWriteSettings
- HistorySearchSettings
- TabOrganizerSettings
- TabCompareSettings

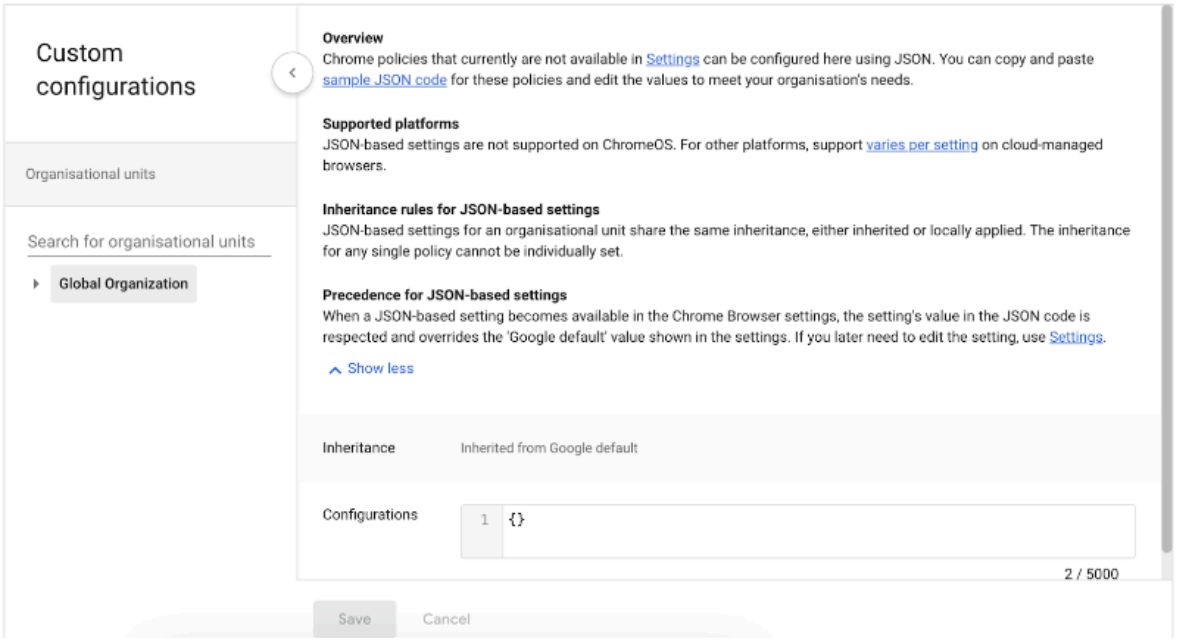
- **Currently available to Trusted Testers.** You can sign up for our Trusted Tester program here.
- As early as Chrome 131: policy rolls out

Support for user-level settings on Custom configurations

Custom configurations recently launched in Chrome 127 and this feature allows IT admins to configure Chrome policies that are not yet in the Admin console, using JSON scripts. **As early as October 15**, **Custom configurations** will support applying settings at the user-level, in addition to device-level support. In order words, you will be able to enforce policies when users sign in to a managed Google account using Custom configurations.

- **As early as October 15 2024, on Android, iOS, Linux, macOS, Windows:** Feature rolls out

To get started, you can navigate to **Chrome browser > Custom configurations** in the Admin console; the Chrome Enterprise Core SKU is required to access this feature.



Audit-only URL navigation rules

This feature lets customers create Chrome URL navigation rules with the Audit action. These rules allow admins to dry-run URL navigation rules before starting to show user warnings. They also allow admins to silently audit users' navigation to restricted or sensitive URLs.

URL auditing is part of the existing real-time URL check connector policy, EnterpriseRealTimeUrlCheckMode, which can be turned on by Organizational Unit or by Group.

- **Chrome 130 on ChromeOS, Linux, macOS, Windows**

Chrome Security Insights

You can now enable Chrome Security Insights to monitor insider risk and data loss with enhanced monitoring for Chrome activity. This feature is available for the following licenses:

- Chrome Enterprise Core
- Workspace Enterprise Standard
- Workspace Enterprise Plus.

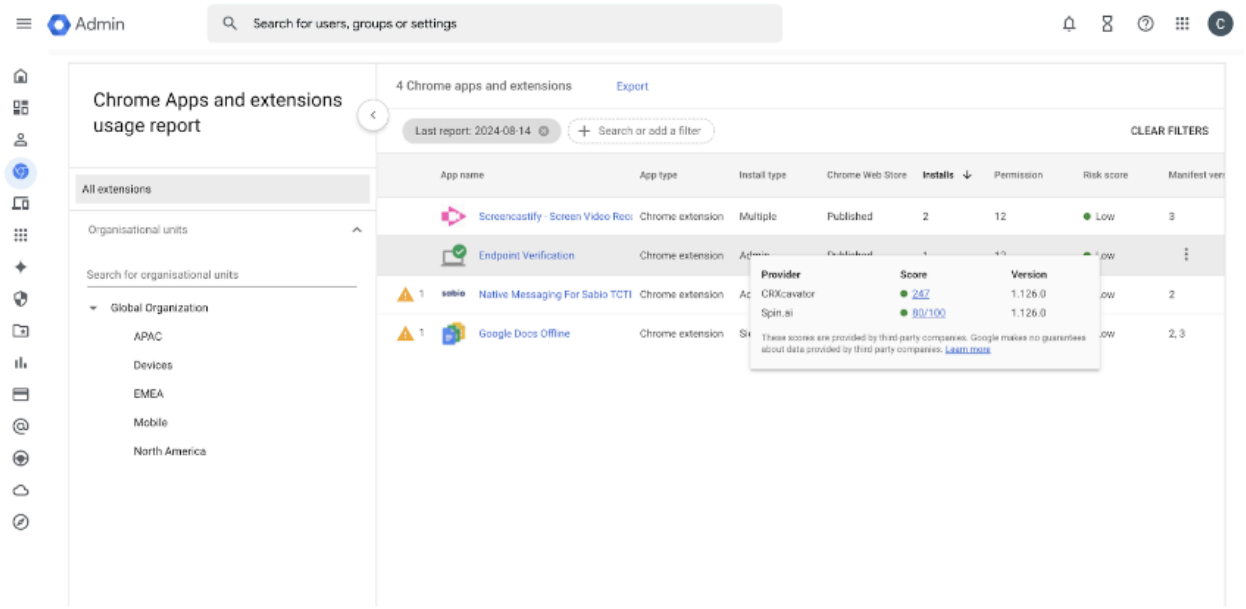
For more information, see Monitoring for insider risk and data loss.

- Chrome 125 on ChromeOS, Linux, macOS, Windows: Feature enabled for Chrome Enterprise Core
- **Chrome 130 on ChromeOS, Linux, macOS, Windows:** Feature enabled for EDU customers (except K-12)

Risk score on the Chrome Apps and extensions usage report

This feature adds a new column in the Admin console for browser management that displays the risk assessment for installed extensions in the admin's environment. This new addition allows IT admins to quickly identify extensions with a high, medium or low risk score using the sorting and filtering functionality of the report.

- **Currently available to Trusted Testers.** You can sign up for our Trusted Tester program here.
- **As early as October 15 on Linux, macOS, Windows:** Addition of risk assessment to summary view.



Current Chrome Enterprise Premium changes

In Chrome 130, there are no updates for Chrome Enterprise Premium.

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

Search and receive answers in your Chrome history with AI

Starting in Chrome 131, users will be able to search their browsing history and receive generated answers based on page contents. Initially, this feature will only be available to users in English in the US. Admins can control this feature by using the HistorySearchSettings policy. You have the following options for your organization:

- 0 = Enable the feature for users, and send relevant data to Google to help train or improve AI models. Relevant data may include prompts, inputs, outputs, and source materials, depending on the feature. It may be reviewed by humans for the sole purpose of improving AI models.
- 1 = Enable the feature for users, but do not send data to Google to train or improve AI models.
- 2 = Fully disable feature

For more information, see Search your history in Chrome with AI.

- **Chrome 131 on Linux, Mac, Windows:** the feature generates answers to your search queries.

Ad-hoc code signatures for Progressive Web App shims on macOS

Code signatures for application shims that are created when installing a Progressive Web App (PWA) on macOS are changing to use ad-hoc code signatures, which are created when the application is installed. The code signature is used by macOS as part of the application's identity. These ad-hoc

signatures will result in each PWA shim having a unique identity to macOS; currently every PWA looks like the same application to macOS.

This will address problems when attempting to include multiple PWAs in the macOS *Open at Login* preference pane, and will permit future improvements for handling user notifications within PWAs on macOS.

Administrators should test for compatibility with any endpoint security or binary authorization tools they use (such as Santa). The feature can be enabled for this testing via `chrome://flags/#use-adhoc-signing-for-web-app-shims`. They can then install a Progressive Web Apps and ensure that it launches as expected.

If there is an incompatibility between the feature and their current security policies, the enterprise policy, AdHocCodeSigningForPWAsEnabled, can be used to disable the feature while they deploy an updated endpoint security policy. The enterprise policy is intended to be used to disable the feature only until endpoint security policies have been updated, at which point it should be unset.

- **Chrome 129 on macOS:** Feature disabled behind a flag (`chrome://flags/#use-adhoc-signing-for-web-app-shims`) so that enterprises can test for compatibility with their endpoint security tools, such as Santa (`https://santa.dev/`). If it is not currently compatible they can disable the feature via the enterprise policy while they update their endpoint security configurations. The enterprise policy is intended to be used to disable the feature only until endpoint security policies have been updated.
- **Chrome 131 on macOS:** Feature will begin to roll out to Stable, starting at 1% rollout.

Asynchronous real-time Safe Browsing check

Today, Safe Browsing checks are on the blocking path of page loads, meaning that the user cannot see the page until the checks are completed. In Chrome 122 and later on Android, ChromeOS, LaCrOS, Linux, macOS, Windows, to improve Chrome's loading speed, real-time Safe Browsing checks no longer block page loads. We have evaluated the risk and put mitigations in place:

1. For malware and 0-day attacks, local-blocklist checks will still be conducted in a synchronous manner so that malicious payloads are still blocked by Safe Browsing.
2. For phishing attacks, we've looked at data and it is unlikely the user would have interacted with the page (for example, type a password) by the time we show the warning.

- Chrome 122 on Android, ChromeOS, LaCrOS, Linux, macOS, Windows
- **Chrome 131 on iOS**

Remove non-standard GPUAdapter requestAdapterInfo() method

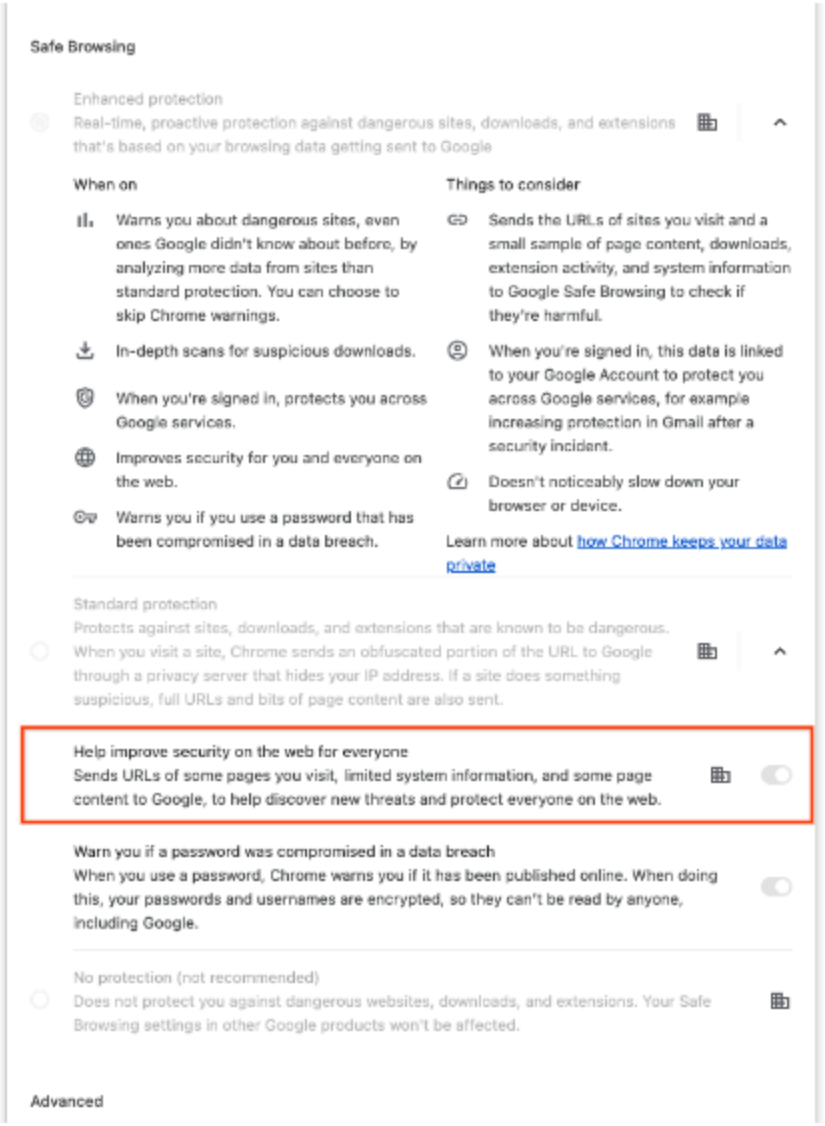
The WebGPU working group decided it was impractical for `requestAdapterInfo()` to trigger a permission prompt so they've removed that option and replaced it with the `GPUAdapter` info attribute. This means that web developers can get the same `GPUAdapterInfo` value synchronously. For more information, see the previous Intent to Ship: WebGPU: GPUAdapter info attribute.

- **Chrome 131 on Windows, macOS, Linux, Android**

Deprecate Safe Browsing Extended reporting

Safe Browsing Extended reporting is a feature that enhances the security of all users by collecting telemetry information from participating users that is used for Google Safe Browsing protections. The data collected includes URLs of visited web pages, limited system information, and some page content. However, this feature is now superseded by **Enhanced protection** mode. We suggest users switch to **Enhanced protection** to continue providing security for all users in addition to enabling the strongest security available in Chrome. For more information, see Safe Browsing protection levels.

- Chrome 129 on Android, iOS, ChromeOS, Linux, macOS, Windows: Deprecation of Safe Browsing Extended Reporting. Excluding real-time Client Safe Browsing Report Request
- **Chrome 131 on Android, iOS, ChromeOS, Linux, macOS, Windows:** Deprecating SafeBrowsingExtendedReportingEnabled for real-time Client Safe Browsing Report Request



Update Google Play Services to fix issues with on-device passwords

Users with old versions of Google Play Services will experience reduced functionality with their on-device passwords, and **Password Manager** might soon stop working for them altogether. These users will need to update Google Play Services, or will be guided through other troubleshooting methods depending on their state. This is part of an ongoing migration that only affects Android users of Google **Password Manager**.

- **Chrome 131 on Android**

Entrust certificate distrust

In response to sustained compliance failures, Chrome 127 changes how publicly-trusted TLS server authentication, that is, websites or certificates issued by Entrust, are trusted by default. This applies to Chrome 127 and later on Windows, macOS, ChromeOS, Android, and Linux; iOS policies do not allow use of the Chrome Root Store in Chrome for iOS.

Specifically, TLS certificates validating to the Entrust root CA certificates included in the Chrome Root Store and issued:

- after October 31, 2024, will no longer be trusted by default.
- on or before October 31, 2024, will be unaffected by this change.

If a Chrome user or an enterprise explicitly trusts any of the affected Entrust certificates on a platform and version of Chrome relying on the Chrome Root Store, for example, when explicit trust is conveyed through a Windows Group Policy Object, the Signed Certificate Timestamp (SCT) constraints described above will be overridden and certificates will function as they do today.

For additional information and testing resources, see Sustaining Digital Certificate Security - Entrust Certificate Distrust.

To learn more about the Chrome Root Store, see this FAQ.

- **Chrome 131 on Android, ChromeOS, Linux, macOS, Windows:** All versions of Chrome 131 and higher that rely on the Chrome Root Store will honor the blocking action, but the blocking action will only begin for certificates issued after November 11, 2024.

Simplified sign-in and sync experience

Starting in Chrome 131, existing users with Chrome sync turned on will experience 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 controlled by SyncTypesListDisabled. Sign-in to Chrome can be disabled via BrowserSignin as before.

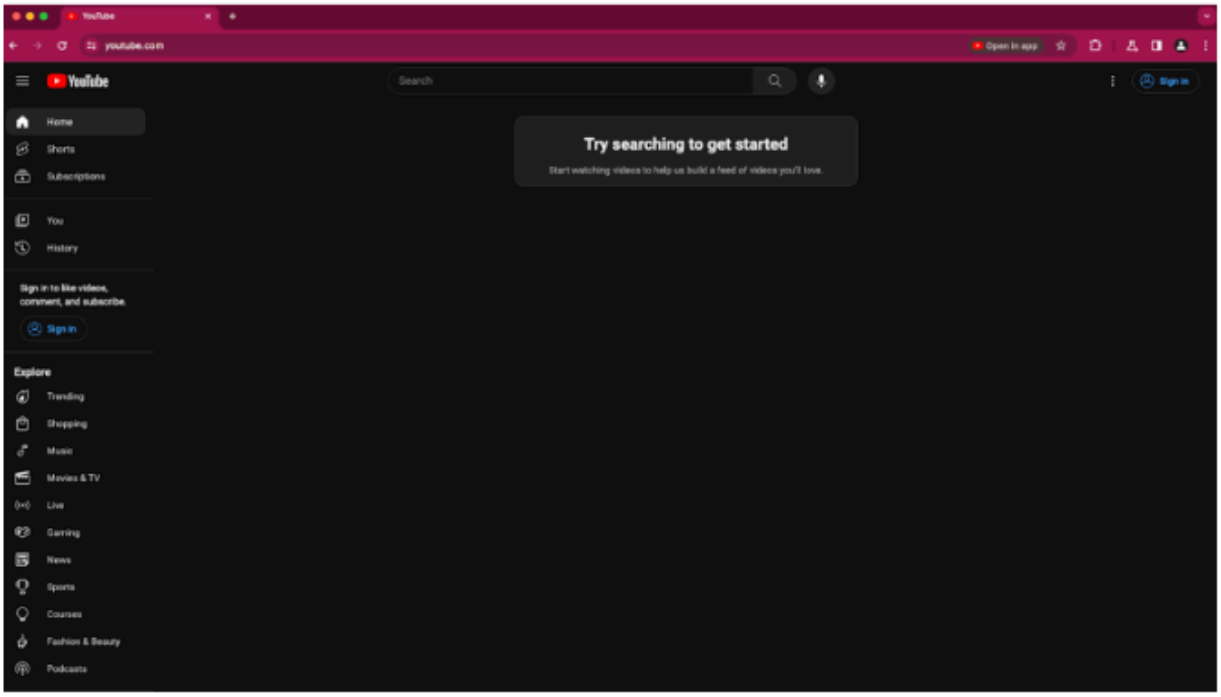
Note that the changes do not affect users' ability to sign in to Google services on the web (like Gmail) without signing in to Chrome, their ability to stay signed out of Chrome, or their ability to control what information is synced with their Google Account.

- **Chrome 131 on Android**

User Link capturing on PWAs

Web links automatically direct users to installed web apps. To better align with users' expectations around installed web apps, Chrome makes it easier to move between the browser and installed web apps. When the user clicks a link that could be handled by an installed web app, Chrome adds a chip in the address bar to suggest switching over to the app. When the user clicks the chip, this either launches the app directly, or opens a grid of apps that can support that link. For some users, clicking a link always automatically opens the app.

- Chrome 121 on Linux, macOS, Windows: When some users click a link, it always opens in an installed PWA, while some users see the link open in a new tab with a chip in the address bar, clicking on which will launch the app. A flag is available to control this feature: `chrome://flags/#enable-user-link-capturing-pwa`.
- **Chrome 131 on Linux, macOS, Windows:** Launch to 100% of Stable with either a default on (always launch apps on link clicks) or a default off (always open in a tab, only launch if the user clicks on chip on address bar).



Deprecation of CSS Anchor Positioning property *inset-area*

The CSS working group (CSSWG) resolved to rename the `inset-area` property to `position-area`. For more details, see the CSSWG discussion on github. The new property name, `position-area`, as a synonym for `inset-area` shipped via this feature update described on Chrome Platform Status, describing the deprecation and removal of the `inset-area` property.

- **Chrome 131 on Windows, macOS, Linux, Android**

X25519Kyber768 key encapsulation for TLS

Starting in Chrome 124, Chrome enables by default on all desktop platforms a new post-quantum secure TLS key encapsulation mechanism X25519Kyber768, based on a NIST standard (ML-KEM). This protects network traffic from Chrome with servers that also support ML-KEM from decryption by a future quantum computer. This change should be transparent to server operators. This cipher will be used for both TLS 1.3 and QUIC connections.

However, some TLS middleboxes might be unprepared for the size of a Kyber (ML-KEM) key encapsulation, or a new TLS ClientHello cipher code point, leading to dropped or hanging connections. This can be resolved by updating your middlebox, or disabling the key encapsulation mechanism via the temporary PostQuantumKeyAgreementEnabled enterprise policy, which will be available through the end of 2024. However, long term, post-quantum secure ciphers will be required in TLS and the enterprise policy will be removed. Post-quantum cryptography is required for CSNA 2.0.

For more detail, see this Chromium blog post and this Google Security blog post.

- Chrome 124 on Windows, Mac, Linux: new post-quantum secure TLS key encapsulation mechanism X25519Kyber768 is enabled
- **Chrome 131 on Windows, Mac, Linux:** Switch to standard version of ML-KEM
- Chrome 141 on Windows, Mac, Linux: Remove enterprise policy PostQuantumKeyAgreementEnabled

Chrome PDF Viewer OCR

Chrome Desktop now makes scanned PDFs more accessible. Using on-device OCR to maintain privacy (no content is sent to Google), Chrome automatically converts scanned PDFs, allowing you to select text, Ctrl+F, copy, and paste. The feature does not bypass secure PDFs. It will only OCR PDFs the user has access to. The solution unlocks PDF accessibility to Chrome users without any extra steps, making PDFs as accessible as the rest of the web.

- **Chrome 131 on ChromeOS, Linux, macOS, Windows**

Insecure form warnings on iOS

Chrome 125 started to block form submissions from secure pages to insecure pages on iOS. When Chrome detects an insecure form submission, it now displays a warning asking the user to confirm the submission. The goal is to prevent leaking of form data over plain text without the user'swithout user's explicit approval. A policy InsecureFormsWarningsEnabled is available to control this feature, and will be removed in Chrome 131.

- Chrome 125 on iOS: Feature rolls out
- **Chrome 131 on iOS**: InsecureFormsWarningsEnabled policy will be removed

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. You can use the Chromium bug tracker to report any issues you encounter.

- **Chrome 132 on Windows:** Network Service sandboxed on Windows

Read aloud in Reading mode

Reading mode is a side-panel feature that provides a simplified view of text-dense web pages. Reading mode will now include a Read aloud feature which allows users to hear the text they are reading spoken out loud. Users can choose different natural voices and speeds, and see visual highlights.

- **Chrome 132 on ChromeOS, Linux, macOS, Windows**

Capture all screens

This feature captures all the screens currently connected to the device using `getAllScreensMedia()`. Calling `getDisplayMedia()` multiple times requires multiple user gestures, burdens the user with choosing the next screen each time, and does not guarantee to the app that all the screens were selected. `getAllScreensMedia()` improves on all of these fronts.

This feature is only exposed behind the MultiScreenCaptureAllowedForUrls enterprise policy, and users are warned before recording even starts, that recording *could* start at some point. The API will only work for origins that are specified in the MultiScreenCaptureAllowedForUrls allowlist. Any origin not specified there, will not have access to it.

- **Chrome 132 on ChromeOS**

SafeBrowsing API v4 to v5 migration

Chrome calls into the SafeBrowsing v4 API will be migrated to call into the v5 API instead. The method names are also different between v4 and v5.

If admins have any v4-specific URL allowlisting to allow network requests to `https://safebrowsing.googleapis.com/v4*`, these should be modified to allow network requests to the whole domain instead: `safebrowsing.googleapis.com`. Otherwise, rejected network requests to the v5 API will cause security regressions for users.

- **Chrome 133 on Android, iOS, ChromeOS, LaCrOS, Linux, macOS, Windows:** This will be a gradual roll-out.

Private network access checks for navigation requests: warning-only mode

Before a website A navigates to another site B in the user's private network, this feature does the following:

1. Checks whether the request has been initiated from a secure context.
2. Sends a preflight request, and checks whether B responds with a header that allows private network access.

There are already features for subresources and workers, but this one is for navigation requests specifically. These checks protect the user's private network.
Since this feature is the warning-only mode, we do not fail the requests if any of the checks fail. Instead, a warning will be shown in the DevTools console, to help developers prepare for the coming enforcement.

- **Chrome 133 on Windows, macOS, Linux, Android**

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. Starting in Chrome 124, a temporary enterprise policy, MutationEventsEnabled, will be available to re-enable deprecated or removed mutation events. If you encounter any issues, file a bug here.

Mutation event support will be disabled by default starting in Chrome 127, around July 30, 2024. Code should be migrated before that date to avoid site breakage. If more time is needed, there are a few options:

- The Mutation Events Deprecation Trial can be used to re-enable the feature for a limited time on a given site. This can be used through Chrome 134, ending March 25, 2025.
- A MutationEventsEnabled enterprise policy can also be used for the same purpose, also through Chrome 134.

Please see this blog post for more detail. Report any issues here.

- **Chrome 135 on Android, Linux, macOS, Windows:** The MutationEventsEnabled enterprise policy will be deprecated.

UI Automation accessibility framework provider on Windows

Starting in Chrome 126, Chrome will start directly supporting accessibility client software that uses Microsoft Windows's UI Automation accessibility framework. Prior to this change, such software interoperated with Chrome by way of a compatibility shim in Microsoft Windows. This change is being made to improve the accessible user experience for many users. It provides complete support for Narrator, Magnifier, and Voice Access; and will improve third-party apps that use Windows's UI

Automation accessibility framework. Users of Chrome will find reduced memory usage and processing overhead when used with accessibility tools. It will also ease development of software using assistive technologies.

Administrators might use the UiAutomationProviderEnabled enterprise policy, available from Chrome 125, to either force-enable the new provider (so that all users receive the new functionality), or disable the new provider. This policy will be supported through Chrome 136, and will be removed in Chrome 137. This one-year period is intended to give enterprises sufficient time to work with third-party vendors so that they may fix any incompatibilities resulting from the switch from Microsoft's compatibility shim to Chrome's UI Automation provider.

- Chrome 125 on Windows:The UiAutomationProviderEnabled policy is introduced so that administrators can enable Chrome's UI Automation accessibility framework provider and validate that third-party accessibility tools continue to work.
- Chrome 126 on Windows: The Chrome variations framework will be used to begin enabling Chrome's UI Automation accessibility framework provider for users. It will be progressively enabled to the full Stable population, with pauses as needed to address compatibility issues that can be resolved in Chrome. Enterprise administrators may continue to use the UiAutomationProviderEnabled policy to either opt-in early to the new behavior, or to temporarily opt-out through Chrome 136.
- **Chrome 137 on Windows:** The UiAutomationProviderEnabled policy will be removed from Chrome. All clients will use the browser's UI Automation accessibility framework provider.

Upcoming Chrome Enterprise Core changes

Chrome extension telemetry integration with SecOps

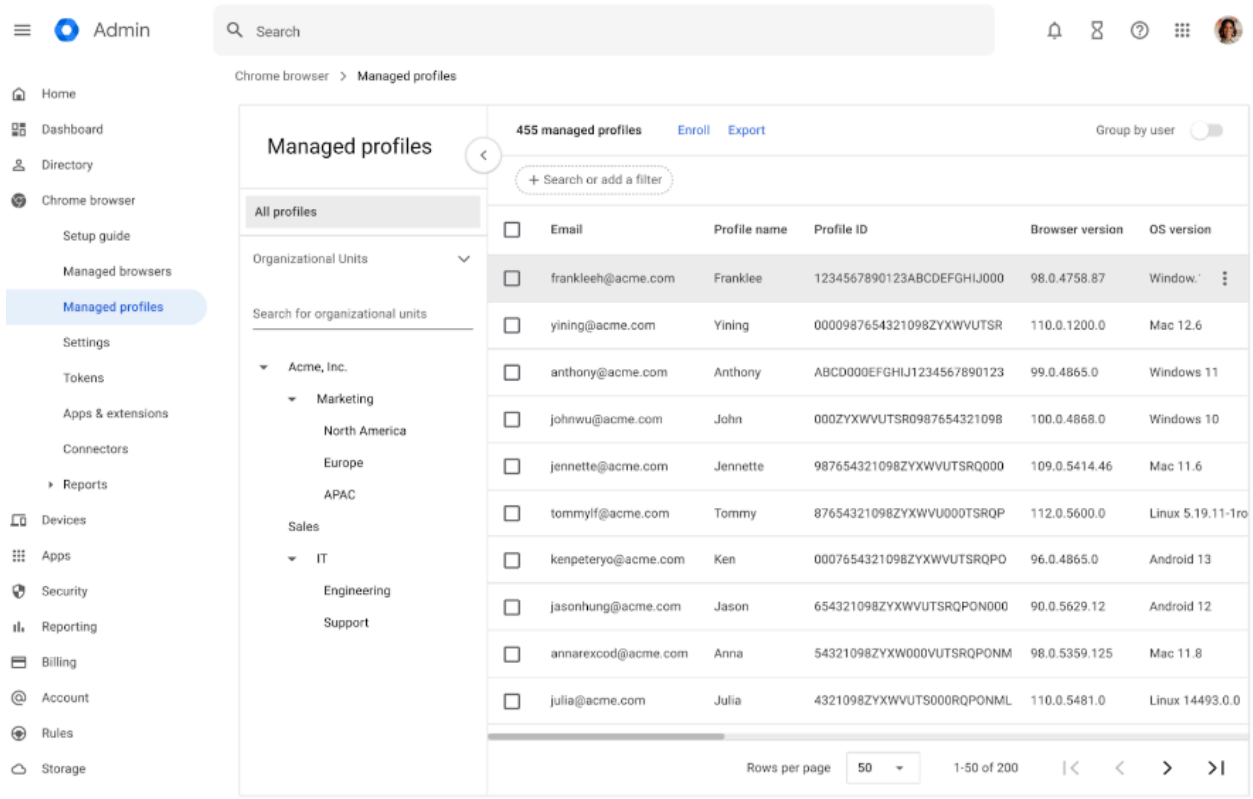
We will begin to collect relevant Chronicle extension telemetry data from within Chrome, for managed profiles and devices, and send it to Google SecOps. Google SecOps will analyze the data to provide instant analysis and context on risky activity; this data is further enriched to provide additional context and is searchable for a year.

- **Chrome 131 on ChromeOS, LaCrOS, Linux, macOS, Windows**

New managed profile list and reporting for signed-in users

Chrome Enterprise Core will introduce a new Managed profile list and reporting in the Admin console. This feature will provide a list of profiles for managed users who sign in to Chrome using a Google Account. IT administrators will need to enable the new Chrome Profile Reporting policy to view more information about a managed profile. The reporting will include details on managed profiles such as the browser versions, policies applied (including conflicts), extensions installed, and more.

- **Currently available on Android, Linux, macOS, Windows for the Trusted Tester program.** You can sign up for our Trusted Tester program here.
- **As early as Chrome 130 on Android, Linux, macOS, Windows**



Remove enterprise policy used for legacy same site behavior

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 132 on Android, ChromeOS, Linux, macOS, Windows:** Remove LegacySameSiteCookieBehaviorEnabledForDomainList policy.

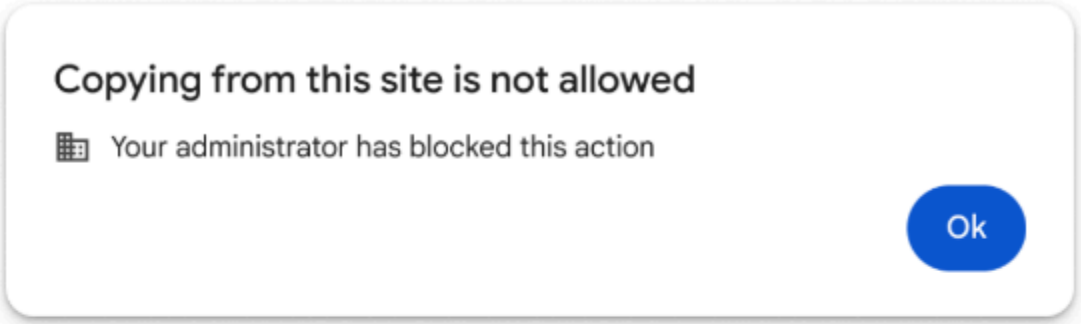
Upcoming Chrome Enterprise Premium changes

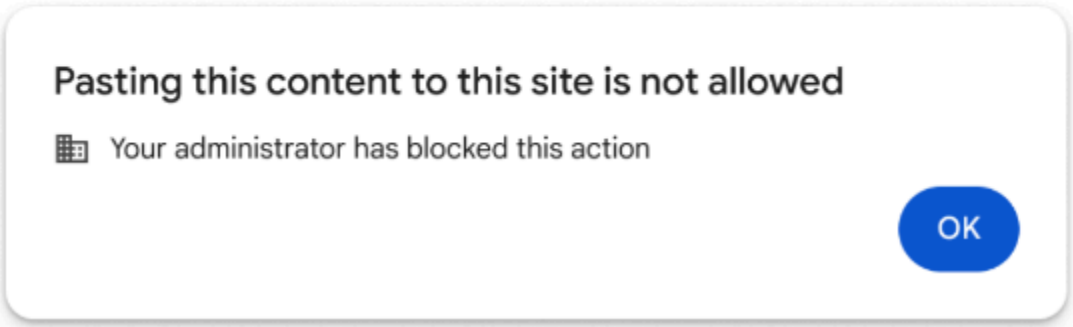
Chrome Enterprise Data Controls: Clipboard

Admins can set data control rules in the Google Admin console to protect end users from data leakage on Chrome browser. Data Controls are lightweight rules set in the Google Admin console that allow admins to set a Chrome policy to control sensitive user actions such as copying and pasting sensitive data and taking screenshots or screen sharing.

This feature can be controlled via DataControlsRules policy. This feature is available to test for the members of the Chrome Enterprise Trusted Tester program. You can sign up for our Trusted Tester program here.

- Chrome 128 on ChromeOS, Linux, macOS, Windows: Trusted Tester program
- **Chrome 131 on ChromeOS, Linux, macOS, Windows: Feature rolls out**





Screenshot protections

Admins can prevent users from taking screenshots or screen sharing specific web pages considered to contain sensitive data. Admins create a DLP URL filtering rule to block users taking screenshots or screen sharing specific URLs or categories of URLs. This feature can be controlled via the same EnterpriseRealTimeUrlCheckMode policy that enables all real-time URL lookups.

This feature is available to test for the members of the Chrome Enterprise Trusted Tester program. You can sign up for our Trusted Tester program here.

- Chrome 129 on ChromeOS, Linux, macOS, Windows: Trusted Tester program
- **Chrome 131 on ChromeOS, Linux, macOS, Windows:** Feature rolls out.

Previous release notes

Chrome version & targeted Stable channel release date	PDF
Chrome 129: September 11, 2024	PDF
Chrome 128: August 14, 2024	PDF
Chrome 127: July 17, 2024	PDF
Chrome 126: June 5, 2024	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