Chrome 144 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 January 9, 2026.

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

Chrome 144 release summary

Current Chrome browser updates	Security / Privacy	User productivity / Apps	Management
AI Mode and Lens enhancements		✓	
Preference tampering protection for enterprise users on Windows	✓		
CSS find-in-page highlight pseudos			✓
Deprecate savedTabGroups as individual value in SyncTypesListDisabled			✓
Happy Eyeballs V3	✓		✓
Multicast support for Direct Sockets API			✓
ServiceWorkerAutoPreload browser mode			✓
Simplified New tab page			✓
Deprecation and removal of Privacy Sandbox APIs	✓	✓	
Gemini in Chrome		✓	
Remote debugging server can be started using chrome://inspect	✓		
New policies in Chrome browser			✓
Chrome Enterprise Core updates	**Security / Privacy**	**User productivity / Apps**	**Management**
Dynamic recommendations in the Admin console			✓
Experimental cryptographic compliance policies	✓		

New extension installation modes	✓	✓	✓
Chrome Enterprise Premium updates	**Security / Privacy**	**User productivity / Apps**	**Management**
Copy and Paste rules protection	✓		✓
Hardening against local policy tampering	✓		✓
Enforced download to Cloud	✓		✓
Proxy override rules	✓		✓
Upcoming Chrome browser updates	**Security / Privacy**	**User productivity / Apps**	**Management**
2SV enforcement for Admin accounts			✓
Change in release schedule in Chrome 145 (Early Stable only)			✓
Chrome removes support for obsolete virtual cameras on macOS			✓
Disable force-installed extensions with non-malware violations	✓		
Import data from Safari to Chrome for iOS made easier			✓
On-device scam detection on Android	✓		
Introducing the Origin API	✓		
Reduced User-Agent strings by default	✓		
Removal of the Google Cloud Print policy			✓
Use of CssPixels in LayoutShift API			✓
Bundled security settings	✓		
Local network access restrictions	✓		
Remove third-party storage partitioning policies	✓		

Update to "No HTTPS" warning	✓		
X25519Kyber768 key encapsulation for TLS	✓		
Disallow spaces in non-file:// URL hosts	✓		
UI Automation accessibility framework provider on Windows		✓	
WebRequest.SecurityInfo in Controlled Frame		✓	
Origin-Bound Cookies (by default)			✓
SafeBrowsing API v4 → v5 migration	✓		
Isolated Web Apps			✓
Chrome will remove support for macOS 12			✓
Deprecate and remove XSLT	✓	✓	✓
PostQuantum cryptography for DTLS in WebRTC	✓		
Upcoming Chrome Enterprise Core updates	**Security / Privacy**	**User productivity / Apps**	**Management**
No upcoming feature announcements			
Upcoming Chrome Enterprise Premium updates	**Security / Privacy**	**User productivity / Apps**	**Management**
Increased file size support for DLP scans	✓		✓

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 browser updates

AI Mode and Lens enhancements

Starting in Chrome 143 on macOS and Windows, new AI Mode capabilities are integrated into Chrome browser. Users can access AI Mode directly from the **New tab** page and the address bar, allowing users to ask complex questions directly from where they start browsing. Admins can turn off these features (value 1) using the AIModeSettings policy or by using the GenAiDefaultSettings (value 2). For more details, see this article in the Chrome Enterprise and Education Help Center.

In Chrome 144, we begin to roll out the multi-tab context feature on AI Mode and Lens. Users can choose to share the contents of one or more of their open tabs, helping them ask questions, compare, summarize, and find information more efficiently. Admins can turn off these features (value 1) using the SearchContentSharingSettings policy or by using the GenAiDefaultSettings (value 2).

- Chrome 143 on MacOS, Windows: New AI Model capabilities will be integrated into Chrome and can be controlled using AIModeSettings policy or the GenAiDefaultSettings policy
- **Chrome 144 on MacOS, Windows**: The multi-tab context feature will be available and can be controlled using the SearchContentSharingSettings policy or GenAiDefaultSettings policy
- Chrome 147 on MacOS, Windows: The LensOverlaySettings, LensDesktopNTPSearchEnabled and LensRegionSearchEnabled policies will be deprecated. Admins can use SearchContentSharingSettings to control these features.

Preference tampering protection for enterprise users on Windows

To provide stronger, more consistent protection against malicious software, Chrome's encrypted preference tampering protection for enterprise-managed browsers is now available on Windows.
Previously, this protection, which automatically resets tampered settings (like a hijacked search engine) to their default values, was not available for enterprise users on Windows. This exception was necessary because the legacy validation method was incompatible with roaming profiles, often causing incorrect resets.
Chrome 144 implements a new, more secure system using an encryptor. This new encryption method is fully compatible with enterprise users. As this new system resolves the root cause of the original issue, we no longer need the legacy Windows enterprise exception.
With this change, if Chrome detects that a sensitive preference has been modified by unauthorized software, it now automatically resets that preference to its default value. This behavior was previously disabled and is now being enabled. This change extends critical security protection to enterprise users, defending them against search hijacking and other malicious setting modifications.

- **Chrome 144 on Windows -** Feature rolls out gradually

CSS find-in-page highlight pseudos

This feature exposes **find-in-page** search result styling to authors as a highlight pseudo-element, like selection and spelling errors. This allows authors to change the foreground and background colors or add text decorations, which can be especially useful if the browser defaults have insufficient contrast with the page colors or are otherwise unsuitable.

- **Chrome 144 on Windows, MacOS, Linux, Android**

Deprecate savedTabGroups as individual value in SyncTypesListDisabled

To align desktop and ChromeOS behavior with mobile and to simplify sync management, the individual savedTabGroups datatype is now deprecated and is no longer an individually customizable value within the SyncTypesListDisabled policy. Previously, the SyncTypesListDisabled enterprise policy allowed administrators to disable the synchronization of savedTabGroups datatype on desktop and ChromeOS platforms. On mobile platforms, however, tab group synchronization is already managed by the tabs datatype.
Starting with Chrome 144, if your SyncTypesListDisabled policy disables either tabs or savedTabGroups, both data types are now considered disabled. This means that disabling tabs also disables saved tab groups, and the other way around. The savedTabGroups value is entirely removed from the list of supported datatypes for this policy. For admins who have saved tab groups disabled, and intend to keep this behavior, make sure to explicitly disable the tabs datatype. This guarantees the desired behavior before the savedTabGroups value is fully removed.

- **Chrome 144 on ChromeOS, Linux, MacOS, Windows**

Happy Eyeballs V3

Happy Eyeballs V3 is an algorithm used to reduce user-visible network connection delay. It performs DNS resolutions asynchronously and staggers connection attempts with preferable protocols (H3/H2/H1) and address families (IPv6/IPv4). Chrome 144 implements Happy Eyeballs V3 to achieve better network connection concurrency. You can control this feature using a temporary policy, HappyEyeballsV3Enabled.

- **Chrome 144 on Android, ChromeOS, Linux, MacOS, Windows**

Multicast support for Direct Sockets API

This feature allows Isolated Web Apps (IWAs) to subscribe to multicast groups and receive User Datagram Protocol (UDP) packets from there. IWAs can now also specify additional parameters when sending UDP packets to multicast addresses.

- **Chrome 144 on Windows, MacOS, Linux**

ServiceWorkerAutoPreload browser mode

ServiceWorkerAutoPreload is a mode where the browser issues the network request in parallel with the service worker bootstrap. If the fetch handler returns the response with respondWith(), the browser consumes the network request result inside the fetch handler. If the fetch handler result is fallback, it passes the network response directly to the browser. ServiceWorkerAutoPreload is an optional browser optimization that changes the existing service worker behavior. Admins can control this feature using an enterprise policy called ServiceWorkerAutoPreloadEnabled.

- Chrome 140 on Android, Windows: ServiceWorkerAutoPreloadEnabled policy will be available
- **Chrome 144 on Android, Windows:** ServiceWorkerAutoPreloadEnabled policy will be removed

Simplified New tab page

This feature reduces visual clutter and enhances user control on the appearance of the **New tab** page (NTP). This simplification of the **New tab** page removes the **Dismiss module** button. Modules not managed by a policy can also be auto-removed after an extended period of inactivity.

- **Chrome 144 on ChromeOS, Linux, MacOS, Windows** - Feature rolls out gradually

Deprecation and removal of Privacy Sandbox APIs

Chrome has recently announced that the current approach to third-party cookies is to be maintained, following which, we plan to deprecate and remove the following APIs.

- Topics
- Protected Audience
- Shared Storage
- Attribution Reporting
- Private Aggregation
- Related Web Sites
- requestStorageAccessFor

The following are the enterprise policies associated with the above APIs.

- PrivacySandboxSiteEnabledAdsEnabled
- PrivacySandboxAdTopicsEnabled
- PrivacySandboxAdMeasurementEnabled
- RelatedWebsiteSetsOverrides
- RelatedWebsiteSetsEnabled

Deprecation will begin with Chrome 144, and removal is planned for Chrome 150. After deprecation, the APIs will continue to exist, and most users will see no disruptions. However, some users who rely on server-side integrations (such as k-anonymity server, or coordinators) will see a break in the services. We have proactively reached out to users of the APIs with our

deprecation plans. At the time of removal, Chrome 150, all the policies associated with these APIs will also be removed.
None of the APIs are enabled by default to enterprise users. Enterprise teams may want to review the status for any managed profile in their **Admin console**.

- **Chrome 144 on Android, ChromeOS, Linux, MacOS, Windows:** Deprecation launch
- Chrome 150 on Android, ChromeOS, Linux, MacOS, Windows: APIs and the associated Policies removal

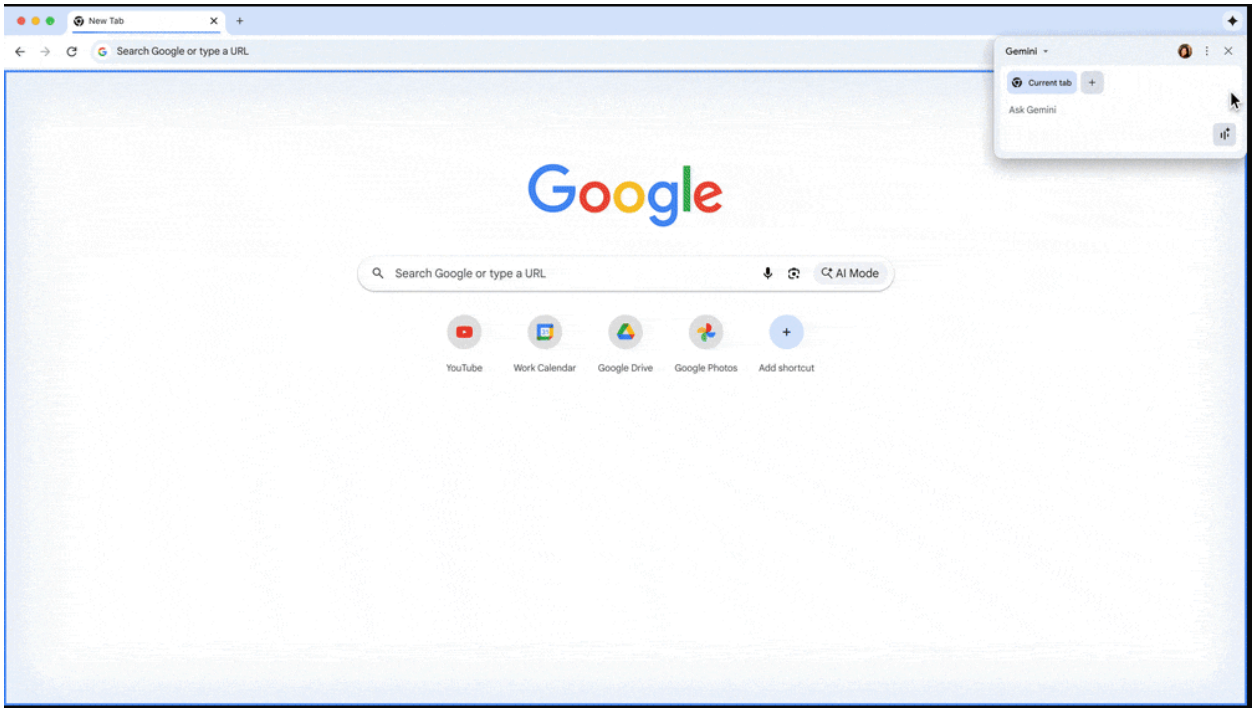
Gemini in Chrome

Gemini is now integrated into Chrome on macOS and Windows, and can understand the content of your current page. Users can now seamlessly get key takeaways, clarify concepts, and find answers, all without leaving their Chrome tab. This integration includes both chat—where users can interact with Gemini via text, and **Gemini Live*, by which users can interact with Gemini via voice.
In Chrome 143, Gemini in Chrome will start the roll out to most Google Workspace users with access to the Gemini app in the US. Admins can turn off this feature (value 1) using the GeminiSettings policy or by using the GenAiDefaultSettings (value 2). For more details, see Gemini in Chrome in the Help Center or this blog post.
Also coming in Chrome 143 is the multi-tab context feature. Gemini in Chrome can now see more of your opened tabs (10 max) so you can ask questions across multiple pages to help you compare, find information more efficiently. Gemini in Chrome also serves as a productivity agent by enabling YouTube, Maps, Gmail, Drive, Keep, Calendar, and Tasks tools.
As early as Chrome 144, agentic capabilities in Gemini in Chrome will be made available to some users (non-enterprise). An enterprise policy GeminiActOnWebSettings will be available at launch. For more details, see the rollout steps below.

- Chrome 137 on MacOS, Windows: Feature is available for some Google AI Pro and Ultra subscribers in the US and on pre-Stable (Dev, Canary, Beta) channels in the US.
- Chrome 143 on MacOS, Windows: Feature gradually rolls out in Canada, New Zealand, Australia in English

- **Chrome 144 on MacOS, Windows:** Agentic capabilities in Gemini in Chrome available to some users (non-enterprise). Enterprise policy GeminiActOnWebSettings will be available at launch.
  Users will be able to upload rendered images directly to Gemini in Chrome using a Chrome context menu item. Users can then use prompts within Gemini in Chrome to generate new, derivative images. With the user's permission, Gemini in Chrome can also use Google Password Manager to sign in to sites.
  Image upload context menu item available to enterprise users. Feature will respect rules set via the DataControlsRules policy and the OnBulkDataEntryEnterpriseConnector settings.

- **Chrome 144 on MacOS, Windows**: Image upload context menu item available to enterprise users. Feature will respect rules set via the [DataControlsRules] (https://chromeenterprise.google/policies/#DataControlsRules) policy and the [OnBulkDataEntryEnterpriseConnector] (https://chromeenterprise.google/policies/#OnBulkDataEntryEnterpriseConnector) settings.
- **Chrome 144 on ChromeOS**: As early as 144 Gemini in Chrome will be rolling out gradually to selective ChromeOS devices
- **Chrome 144 on MacOS, Windows**: Gemini in Chrome will allow some 3P tools that are available as Gemini Extensions to be called
- Chrome 147 on MacOS, Windows: Agentic capabilities in Gemini in Chrome available to enterprise users.
- Chrome 148 on MacOS, Windows: As early as Chrome 148 on macOS, Windows: Agentic capabilities in Gemini in Chrome available to enterprise users.



Remote debugging server can be started using chrome://inspect

The feature allows the user to start a remote debugging server from the chrome://inspect page without restarting Chrome (previously only possible via CLI arguments). Admins can control this feature using the existing RemoteDebuggingAllowed policy and the feature will not be available if the policy is set to false.

- **Chrome 144 on ChromeOS, Linux, MacOS, Windows**: Remote debugging server can be started via chrome://inspect

New policies in Chrome browser

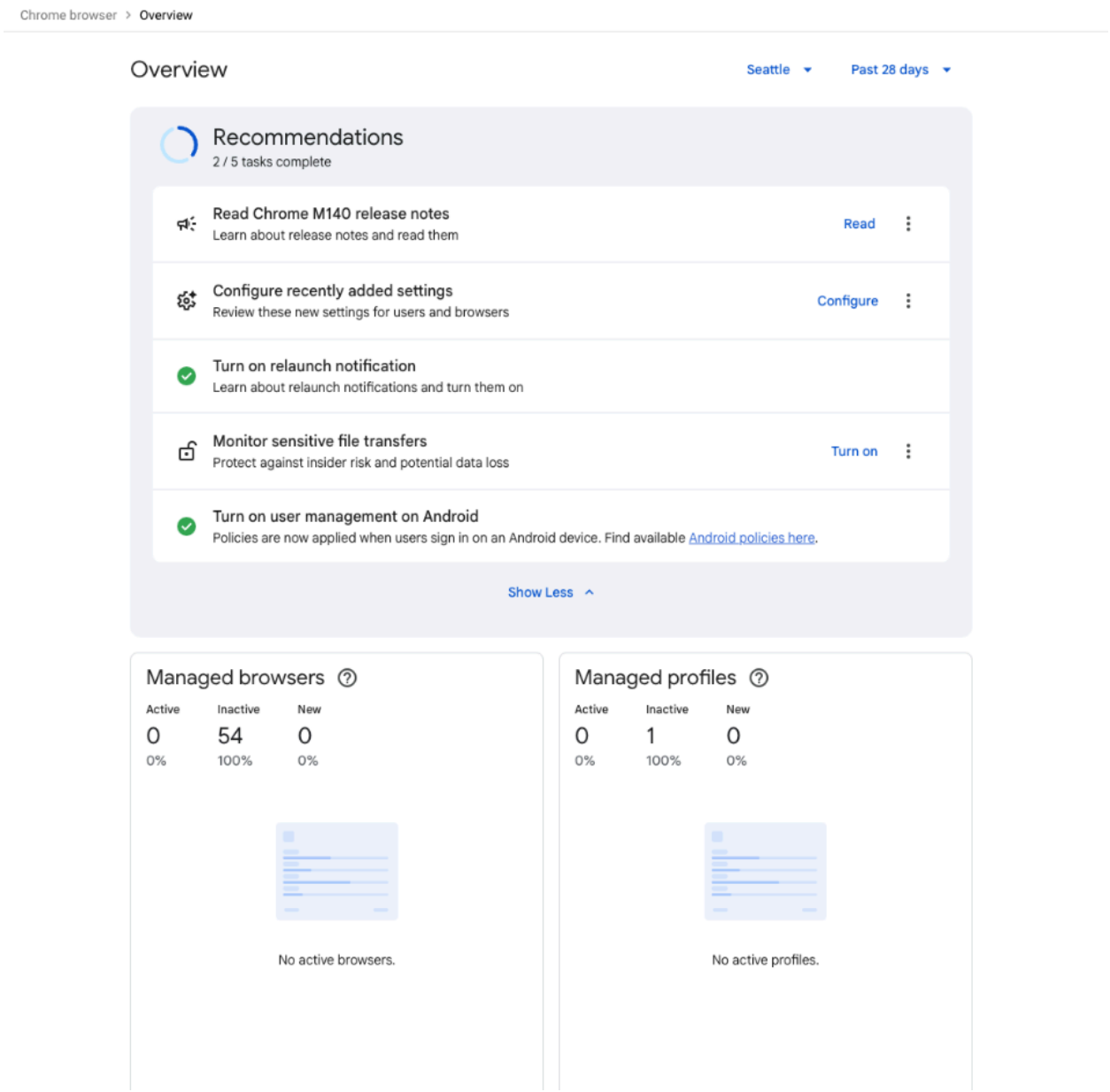
Policy	Description
DataControlsRules	This policy is used to set Data Controls rules.
ShowHomeButton	Configure the Home button on the toolbar.
SilentPrintingEnabled	Enable silent printing.
ProxyOverrideRules	Configure proxy override rules.
SearchContentSharingSettings	Controls whether users can share page content with the search provider (e.g. Google). This includes sharing page text, images, and other content. This policy also controls the behavior of features such as AI Mode, Lens, and other features that involve sharing page content with the search provider.
GeolocationBlockedForUrls	Block geolocation access for specific sites.
BookmarkBarEnabled	Enables the bookmark bar.
UserSecurityAuthenticatedReporting	Controls if user security events on unmanaged devices should be reported with a device user name or not.
PreciseGeolocationAllowedForUrls	Allow precise geolocation access for specific sites.
HomepageIsNewTabPage	Use the New Tab Page as the homepage.
StaticStorageQuotaEnabled	Enable static storage quota for sites.
UserSecuritySignalsReporting	Controls if user security signals on unmanaged devices should be reported or not.

Current Chrome Enterprise Core updates

Dynamic recommendations in the Admin console

Chrome Enterprise is launching a new dynamic recommendations list on the **Overview** page in the Google Admin console.
This recommendation list helps IT admins understand what to do next, get alerts on important changes, discover what's new in the Release Notes, configure popular settings, and more. The list dynamically changes based on the Admin's configuration for each organization unit.
Admins can try this feature directly on the **Admin console** by navigating to **Chrome browser > Overview**.

- Chrome 143 on Android, iOS, Linux, MacOS, Windows: Available to Chrome Enterprise Trusted Testers.
- **Chrome 144 on Android, iOS, Linux, MacOS, Windows:** Feature rolls out gradually



Experimental cryptographic compliance policies

PreferSlowKEXAlgorithms and **PreferSlowCiphers** are two new, experimental enterprise policies that configure Chrome to order its preferred key agreement algorithms (supported groups) and encryption cipher algorithms, in TLS 1.3, to reflect a preference for algorithms that have been approved by a specific compliance regime. Currently, the only compliance regime is CNSA2. This does not guarantee that any specific algorithms will be negotiated. It allows server

operators who want to support clients with and without compliance requirements to differentiate between clients, and only use certain non-default algorithms with increased cryptographic strength for those explicitly configured to prefer them. This policy is not required for security. The default cryptography used by Chrome is strong enough to withstand a brute force attack using the entire power of the sun. Setting this policy will cause Chrome to be slower when accessing websites. This policy only affects TLS 1.3 and QUIC, it does not affect earlier versions of TLS.
These policies are temporarily available as a single combined flag, chrome://#cryptography-compliance-cnsa.

- Chrome 143 on Android, ChromeOS, Linux, MacOS, Windows, Fuchsia: The policies are available but marked as experimental for Chrome browser
- **Chrome 144 on ChromeOS:** The additional policies that apply to the ChromeOS device login screen are available but marked as experimental.
- Chrome 146 on Android, ChromeOS, Linux, MacOS, Windows: Around Chrome 146, the TLS servers for Google properties will be updated to negotiate ML-KEM-1024 when this flag is set. At that point, the policy will no longer be marked as experimental.

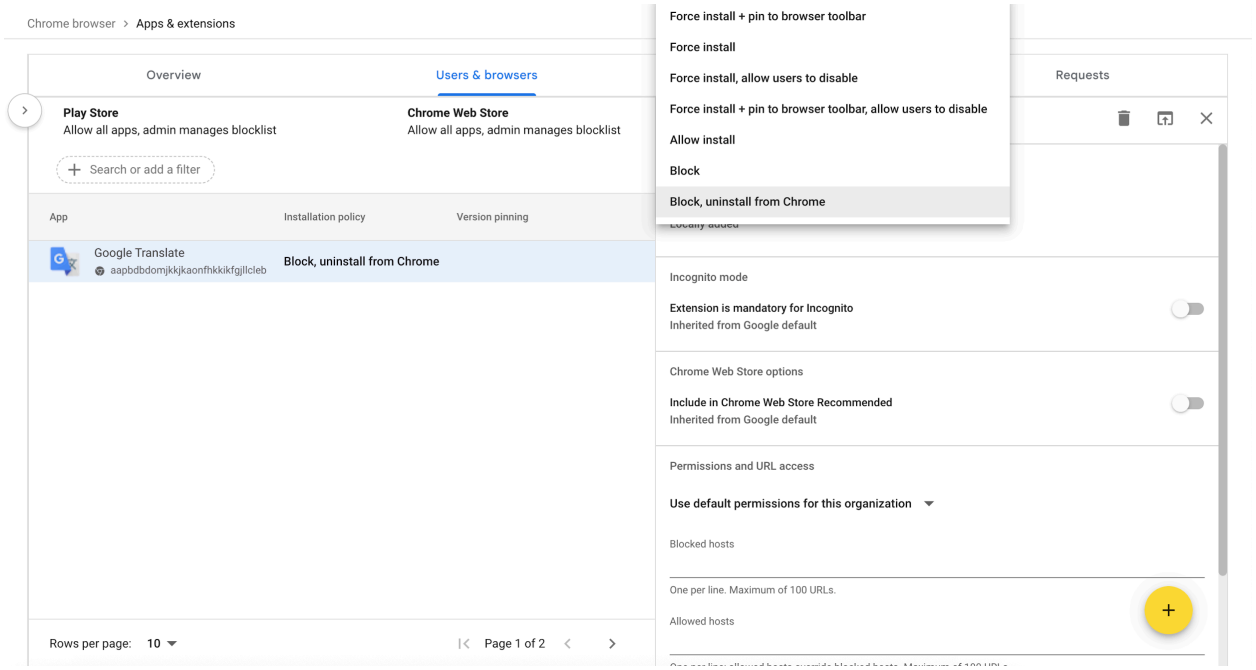
New extension installation modes

Chrome Enterprise will be supporting new extension installation modes in the **Admin console**. Administrators can now:

- **block and uninstall an extension** from Chrome
- **force install an extension**
- or allow users to disable an extension

These new installation modes are available on the **Apps & extensions** settings page, on the **User & browsers** tab, where Admins can select new **installation policy** modes.

- **Chrome 144 on Linux, MacOS, Windows** - Feature rolls out gradually


Chrome browser > Apps & extensions
Overview
Users & browsers
Requests
Play Store
Allow all apps, admin manages blocklist
Chrome Web Store
Allow all apps, admin manages blocklist
Search or add a filter
App
Installation policy
Version pinning
Google Translate
aapbdbdomjkkjkaonfhkkikfgjllcleb
Block, uninstall from Chrome
Rows per page: 10
Page 1 of 2
Force install + pin to browser toolbar
Force install
Force install, allow users to disable
Force install + pin to browser toolbar, allow users to disable
Allow install
Block
Block, uninstall from Chrome
Incognito mode
Extension is mandatory for Incognito
Inherited from Google default
Chrome Web Store options
Include in Chrome Web Store Recommended
Inherited from Google default
Permissions and URL access
Use default permissions for this organization
Blocked hosts
One per line. Maximum of 100 URLs.
Allowed hosts

Current Chrome Enterprise Premium updates

Copy and Paste rules protection

To help organizations better prevent data exfiltration on mobile devices, Chrome is extending its existing desktop clipboard data controls. Administrators can now use the DataControlsRules policy to set rules that block or warn users when they attempt to copy or paste content that violates organizational policies.
This feature allows admins to define data boundaries and prevent sensitive information from being pasted from a work context into personal apps or websites on their mobile fleet. This addresses a significant security gap and a frequently requested feature from enterprise customers who have cited the lack of mobile data controls as a concern.
To use this feature, administrators can configure clipboard restrictions within the DataControlsRules policy, providing a consistent management experience across desktop and mobile to strengthen their organization's overall security posture. For more details, see this help center article, which provides further context on how administrators can configure and manage Chrome Enterprise reporting connectors to forward browser security and data protection events to third-party services for analysis.

- Chrome 140 on Android: Copy and Paste rules protection becomes available on Android.
- **Chrome 144 on iOS**: Copy and Paste rules protection becomes available on iOS.

Hardening against local policy tampering

Policy conflict detection signals for Context-Aware Access (CAA), closes a significant security gap by enabling the detection of corporate policies being overridden by conflicting local settings on BYOD devices.
This is achieved by integrating new policy conflict signals from the managed Chrome profile into the existing security reporting pipeline, controlled by the UserSecuritySignalsReporting policy.
This visibility allows Admins to set CAA rules in Chrome Enterprise Premium's (CEP) Data and Threat Protection tools or Security Gateway to automatically block access to corporate

applications if critical policies, such as DLP controls, Safe Browsing, or Extension blocklists, are found to be non-compliant.

- **Chrome 144 on Linux, MacOS, Windows:** Detection and reporting of policy conflict metadata begins.
- Chrome 145 on Linux, MacOS, Windows: Enables the Context-Aware Access (CAA) evaluation flow to allow Admins to write enforcement rules based on the existence of a conflict.
- Chrome 146 on Linux, MacOS, Windows: Admin console UI is updated to display conflict signals and policy values begin reporting.

Enforced download to Cloud

Admins can now configure a Data Loss Prevention (DLP) rule that automatically redirects sensitive file downloads from a user's local device to their corporate Google Drive. This **Force save to cloud storage** action prevents sensitive data from resting on unmanaged local disks (for example, C:\Downloads), ensuring a secure chain of custody. When a user attempts to download a file flagged by DLP policies, the Secure Enterprise Browser extension intercepts the download and uploads it directly to the user's corporate drive.

- **Chrome 144 on Linux, MacOS, Windows** - Feature rolls out gradually: The **Enforced download to Cloud** remediation action becomes available in the Data Loss Prevention (DLP) rule builder.

Proxy override rules

To simplify proxy management in complex enterprise environments, Chrome 144 introduces two new policies: ProxyOverrideRules and **EnableProxyOverrideRulesForAllUsers**. Previously, organizations that used multiple proxy solutions (for example, a general proxy and a specific one for Google's Secure Gateway) or have different admin teams (for example, for GPO and the

Google Admin console) had to manually merge complex PAC files. This process is error-prone and creates significant administrative friction.
The new ProxyOverrideRules policy allows administrators to configure a list of routing rules that are evaluated before any existing proxy configuration, including PAC files set by the ProxySettings policy. This enables admins to easily **prepend or override** specific routes (for example, to send traffic for private web apps to a secure gateway) without modifying the primary, company-wide PAC script.
Users will see a notification in their chrome://settings page to inform them when these administrative proxy rules are active.

- **Chrome 144 on ChromeOS, Linux, MacOS, Windows**: ProxyOverrideRules becomes available.

Coming soon

Note: The items listed below are experimental or planned updates. They might change, be delayed, or canceled before launching.

Upcoming Chrome browser updates

2SV enforcement for Admin accounts

To better protect your organization's information, Google will soon require all accounts with access to **admin.google.com** to have 2-Step Verification (2SV) enabled. As a Google Workspace administrator, you need to confirm your identity with 2SV, which requires your password plus something additional, such as your phone or a security key. The enforcement will be rolled out gradually over the coming months. You should enable 2SV for the admin accounts in your organization before Google enforces it. For more information, see this About 2SV enforcement for admins.

- Chrome 137 on ChromeOS, Linux, MacOS, Windows: 2SV enforcement starts
- **Chrome 145 on ChromeOS, Linux, MacOS, Windows:** 2SV mandatory

Change in release schedule in Chrome 145 (Early Stable only)

Starting in Chrome 145, Chrome will be rolled out to the Early Stable channel one week earlier than previously communicated. For example, the Chrome 145 Early Stable release moves from February 4, 2026 to January 28, 2026. There are no changes to the Stable channel release. For reference, you can check the updated Release Schedule.

- **Chrome 145 on Android, iOS, MacOS, Windows:** Chrome will be rolled out to the Early Stable channel one week earlier.

Chrome removes support for obsolete virtual cameras on macOS

As early as Chrome 145, Chrome will remove support for obsolete virtual cameras for all macOS releases that it supports.
On macOS, modern virtual cameras are built using the Core Media IO framework, which has been available since macOS 12.3. Apple has performed outreach, and all modern virtual camera software has been migrated to use this Core Media IO framework.
Obsolete virtual cameras, built as DAL plugins, have been blocked by macOS itself starting with macOS 14.1 (2023), and have been unsupported in Safari since 2018, if not earlier.
Chrome will remove support for obsolete virtual cameras for all macOS releases that it supports. This allows Chrome to improve security by fully disallowing loading of third-party libraries into Chrome processes.

- **Chrome 145 on Windows, MacOS, Linux**

Disable force-installed extensions with non-malware violations

This feature silently disables force-installed extensions exhibiting violations of Chrome Web Store policies in unmanaged browser environments. Such violations include general program violations, unwanted software and potential security vulnerabilities not classified as malware. Users retain the ability to enable or disable these extensions, but will not be able to remove them.
A new enterprise policy, ExtensionForceInstallWithNonMalwareViolationEnabled, was added in 142 to preserve the existing behavior for unmanaged browser environments, but will be removed in 145.
This change does not affect managed instances of Chrome that are joined to a Microsoft Active Directory domain, joined to Microsoft Azure Active Directory or enrolled in Chrome Enterprise Core. On macOS, this change does not affect instances of Chrome that are managed via MDM, joined to a domain or enrolled in Chrome Enterprise Core.

- Chrome 142 on MacOS, Windows: In Chrome 142 for Windows and macOS, force-installed extensions with minor policy violations will be silently disabled in low-trust environments.
- **Chrome 145 on MacOS, Windows** - Feature rolls out gradually: The ExtensionForceInstallWithNonMalwareViolationEnabled policy will be removed.

Import data from Safari to Chrome for iOS made easier

Users of Chrome for iOS will be able to import data (bookmarks, history, passwords, payment cards, and reading list entries) that they have previously exported from Safari. This helps users who are switching browsers to get set up faster and bring their existing data with them.
Chrome cannot access this data directly; the user must provide a zip file containing their data, which can be exported through iOS settings. Chrome provides instructions on how to do so.

- **Chrome 145 on iOS** - Feature rolls out gradually

Introducing the Origin API

The origin is a fundamental component of the web's implementation, essential to both the security and privacy boundaries which user agents maintain. The concept is well-defined between HTML and URL, along with widely-used adjacent concepts like *site*.
Origins, however, are not directly exposed to web developers. Though there are various origin getters on various objects, each of those returns the ASCII serialization of an origin, not the origin itself. This has a few negative implications. Practically, developers attempting to do same-origin or same-site comparisons when handling serialized origins often get things wrong in ways that lead to vulnerabilities. Philosophically, it seems like a missing security primitive that developers struggle to polyfill accurately.
As early as Chrome 145, we plan to address this gap in the platform by introducing an Origin object that encapsulates the origin concept, and provides helpful methods for comparison, serialization, parsing, and so on.

- **Chrome 145 on Windows, MacOS, Linux, Android**

On-device scam detection on Android

Chrome 145 will send a request to Safe Browsing for a final verdict when an on-device scam is detected using the visual features of the page. Based on this verdict, Chrome will decide whether to display a warning to the user.
This feature will be enabled only for users in **Enhanced Protection** mode. The feature will be disabled for **Standard Protection** mode users or users with Safe Browsing disabled. Enterprise admins can control this **Safe Browsing** setting with the SafeBrowsingProtectionLevel Chrome Enterprise policy.

- **Chrome 145 on Android**

Reduced User-Agent strings by default

Starting in Chrome 145, the **UserAgentReduction** policy will be completely removed. This policy was previously available to control whether Chrome sent a reduced or full User-Agent string.
To enhance user privacy and reduce passive tracking capabilities, Chrome began reducing the information contained in the User-Agent header by default in Chrome version 110. The **UserAgentReduction** policy was provided as a temporary measure for enterprises to manage this transition.
The recommended mechanism for websites to access browser and device information is now User-Agent Client Hints (UA-CH). UA-CH requires websites to actively request specific information, which is a more privacy-preserving approach than the legacy User-Agent string. For more details, see this article on web.dev, Migrate to User-Agent Client Hints.
From Chrome 145 onwards, the **UserAgentReduction** policy will have no effect. Chrome will send a reduced User-Agent string by default. Systems or applications that relied on this policy to receive the full (legacy) User-Agent string may no longer receive the detailed information they expect.

- **Chrome 145 on Windows, MacOS, Linux, Android**

Removal of the Google Cloud Print policy

Following the retirement of Google Cloud Print, we are removing the CloudPrintProxyEnabled policy. This policy allowed administrators to enable or disable the Google Cloud Print proxy in Chrome. Since the Google Cloud Print service is no longer available, the policy and its associated settings are being removed from Chrome.

- **Chrome 145 on Linux, MacOS, Windows:** Removal of the CloudPrintProxyEnabled policy

Use of CssPixels in LayoutShift API

This feature changes the attribution data (prevRect and currentRect) in the LayoutShift API to be reported in CSS pixels instead of physical pixels. The current behavior is inconsistent with other layout-related APIs, which all use CSS pixels. This change improves consistency, simplifies usage for developers, and aligns with expected units in debugging and tooling. The feature is gated behind a flag for experimentation and evaluation. The feature can be enabled for testing using the command-line flag: --enable-blink-features=ReportLayoutShiftRectsInCssPixels

- **Chrome 145 on Windows, MacOS, Linux, Android**

Bundled security settings

This feature provides users with bundled security options to configure security settings based on their desired level of protection while using Chrome. Users can choose between *Enhanced* for the highest level of security and *Standard* for the default balanced protection. Users can still set custom values for the settings, as they can today. This simplifies the user experience and makes it easier for users to get the level of protection they want without needing to understand advanced configuration options. Existing enterprise policies take precedence over end-user

bundle selections. If an existing policy is configured for security settings, the values will not be overridden by a user's choice of security bundle.

- **Chrome 146 on ChromeOS, Linux, MacOS, Windows**

Local network access restrictions

Chrome 142 restricts the ability to make requests to the user's local network, gated behind a permission prompt.
A local network request is any request from a public website to a local IP address or loopback, or from a local website (for example, intranet) to loopback. Gating the ability for websites to perform these requests behind a permission mitigates the risk of cross-site request forgery attacks against local network devices such as routers, and reduces the ability of sites to use these requests to fingerprint the user's local network.
This permission is restricted to secure contexts. If granted, the permissions additionally relaxes mixed content blocking for local network requests (since many local devices are not able to obtain publicly trusted TLS certificates for various reasons).
This work supersedes a prior effort called Private Network Access, which used preflight requests to have local devices opt-in.
For more information on this feature, see Adapting your website for new Local Network Access restrictions in Chrome.

- **Chrome 146 on Android, ChromeOS, Linux, MacOS, Windows**: Local Network Access restrictions expanded to include WebSocket and WebTransport connections.
- Chrome 152 on Android, ChromeOS, Linux, MacOS, Windows: LocalNetworkAccessRestrictionsTemporaryOptOut will be removed.

Remove third-party storage partitioning policies

Third-party storage partitioning became the default in Chrome 115. The chrome:// flag that allowed users to disable this feature was removed in Chrome 128, and the deprecation trial

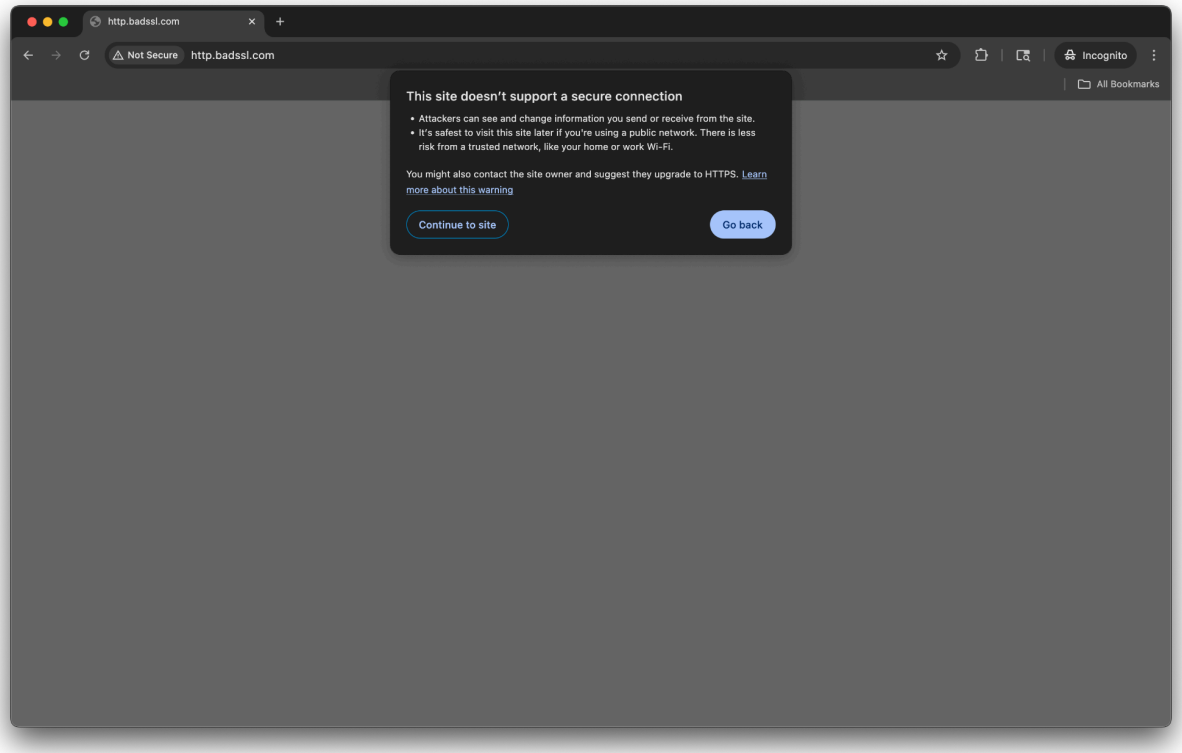
ended with Chrome 139. In Chrome 146, the enterprise policies DefaultThirdPartyStoragePartitioningSetting and ThirdPartyStoragePartitioningBlockedForOrigins will be removed. Users are advised to transition to alternative storage solutions, either by adapting to third-party storage partitioning or by using document.requestStorageAccess({...}) where needed.
If you have any feedback, you can add it here in the Chromium bug

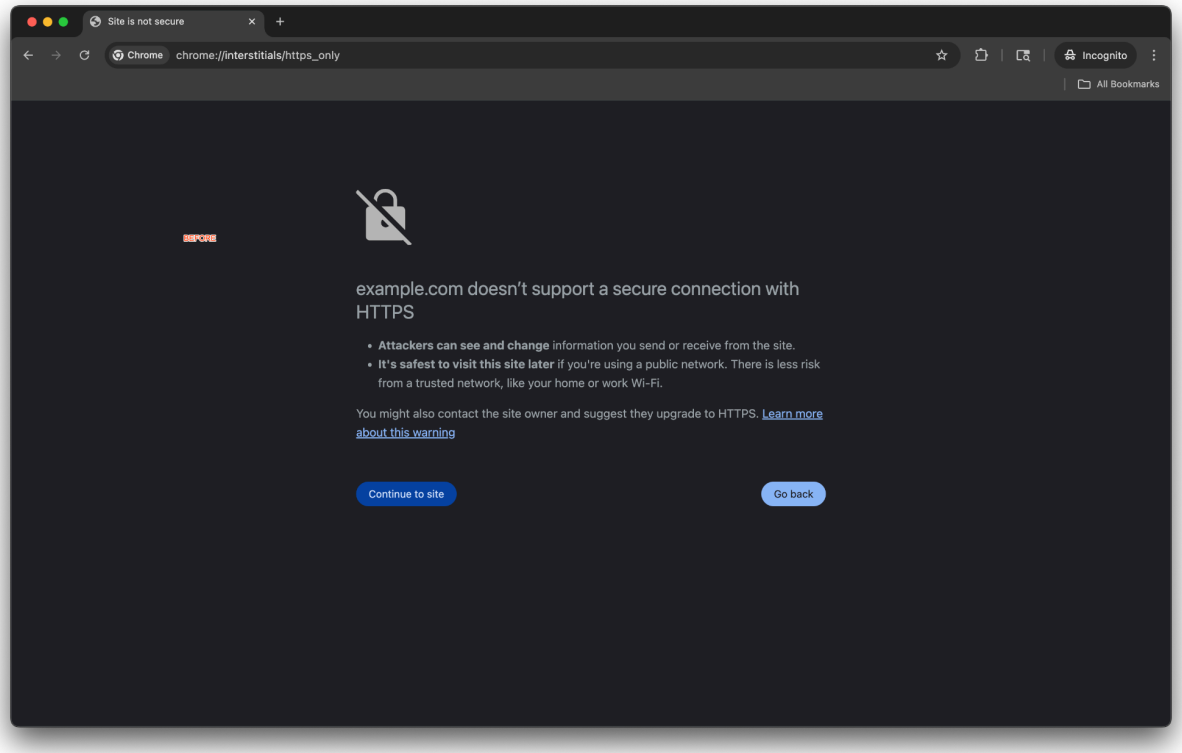
- **Chrome 146 on Android, ChromeOS, Linux, MacOS, Windows, Fuchsia**: Removal of DefaultThirdPartyStoragePartitioningSetting and ThirdPartyStoragePartitioningBlockedForOrigins Policies

Update to No HTTPS warning

The warning displayed when a user opts-in to the **Always Use Secure Connections** on chrome://settings/security is changing from an interstitial to a dialog. Full page load remains blocked, and the functionality remains the same. The URL content security indicator on the warning is changing from the indicator to the broken lock. Some users may see this warning automatically when visiting HTTP sites. Users can opt-in to the warning on chrome://settings/security.

- Chrome 141 on ChromeOS, Linux, MacOS, Windows: New warning design on desktop platforms.
- **Chrome 146 on Android**: Similar updated warning design on Android, using a warning bubble instead of a full interstitial.


http.badssl.com
Not Secure
http.badssl.com
Incognito
All Bookmarks
This site doesn't support a secure connection
• Attackers can see and change information you send or receive from the site.
• It's safest to visit this site later if you're using a public network. There is less risk from a trusted network, like your home or work Wi-Fi.
You might also contact the site owner and suggest they upgrade to HTTPS. Learn more about this warning
Continue to site
Go back


Site is not secure
Chrome
chrome://interstitials/https_only
Incognito
All Bookmarks
BEFORE
example.com doesn't support a secure connection with HTTPS
• Attackers can see and change information you send or receive from the site.
• It's safest to visit this site later if you're using a public network. There is less risk from a trusted network, like your home or work Wi-Fi.
You might also contact the site owner and suggest they upgrade to HTTPS. Learn more about this warning
Continue to site
Go back

X25519Kyber768 key encapsulation for TLS

Chrome 124 enabled 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. To learn more, see Protect Chrome Traffic with Hybrid Kyper KEM.

- Chrome 131 on Linux, MacOS, Windows: Chrome will switch the key encapsulation mechanism to the final standard version of ML-KEM
- **Chrome 146 on Linux, MacOS, Windows:** Enterprise policy will be removed

Disallow spaces in non-file:// URL hosts

According to the URL Standard specification URL hosts cannot contain the space character, but currently URL parsing in Chromium allows spaces in the host. This causes Chromium to fail several tests included in the Interop2024 HTTPS URLs for WebSocket and URL focus areas. To bring Chromium into spec compliance, we would like to remove spaces from URL hosts altogether, but a difficulty with this is that they are used in the host part in Windows file:// URLs. For more details, see this Github discussion.

- **Chrome 147 on Android, ChromeOS, LaCrOS, Linux, MacOS, Windows, Fuchsia**

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 may use the UiAutomationProviderEnabled enterprise policy starting in 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 147, and will be removed in Chrome 147. 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 146.
- **Chrome 147 on Windows:** The UiAutomationProviderEnabled policy will be removed from Chrome. All clients will use the browser's UI Automation accessibility framework provider.

WebRequest.SecurityInfo in Controlled Frame

This feature introduces a WebRequest.SecurityInfo API for ControlledFrame. It allows a web app to intercept an HTTPS, WSS or WebTransport request to a server, retrieve the server's certificate fingerprint (as verified by the browser), and then use that fingerprint to manually verify the certificate of a separate raw TCP/UDP connection to the same server. This provides a simple way for the app to confirm it's talking to the correct server.

- **Chrome 147 on Windows, MacOS, Linux**

Origin-Bound cookies (by default)

In Chrome 148, cookies are bound to their setting origin (by default) such that they're only accessible by that origin, that is, they are sent on a request or visible through document.cookie. Cookies might ease the host and port binding restrictions through use of the Domain attribute but all cookies will be bound to their setting scheme.
Temporary enterprise policies **LegacyCookieScopeEnabled** and **LegacyCookieScopeEnabledForDomainList** will be made available to revert this change. These policies will stop working in Chrome 150.

- **Chrome 148 on Android, iOS, Linux, MacOS, Windows**: Enterprise policies are available.
- Chrome 150 on Android, iOS, Linux, MacOS, Windows: Enterprise policies will be removed.

SafeBrowsing API v4 → 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. For more details, see Migration From V4 - Safe Browsing.

- **Chrome 148 on Android, iOS, ChromeOS, Linux, MacOS, Windows** - Feature rolls out gradually

Isolated Web Apps

Isolated Web Apps (IWAs) are an extension of existing work on PWA installation and Web Packaging that provide stronger protections against server compromise and other tampering that is necessary for developers of security-sensitive applications. Rather than being hosted on live web servers and fetched over HTTPS, these applications are packaged into Web Bundles, signed by their developer, and distributed to end-users through one or more of the potential methods described in the explainer.
As early as Chrome 150, IWAs will only be installable through an admin policy on enterprise-managed ChromeOS devices.

- **Chrome 150 on Windows:** This rollout adds support for Isolated Web Apps in enterprise-managed browser configurations on Windows.

Chrome will remove support for macOS 12

Chrome 150 will be the last release to support macOS 12; Chrome 151+ will no longer support macOS 12, which is outside of its support window with Apple. Running on a supported operating system is essential to maintaining security.
On Macs running macOS 12, Chrome will continue to work, showing a warning infobar, but will not update any further. If a user wishes to have their Chrome updated, they need to update their computer to a support version of macOS.

For new installations of Chrome 151+, macOS 13+ will be required.

- **Chrome 151 on Windows, MacOS, Linux**

Deprecate and remove XSLT

XSLT v1.0, which all browsers adhere to, was standardized in 1999. In the meantime, XSLT has evolved to v2.0 and v3.0, adding features, and growing apart from the old version frozen into browsers. This lack of advancement, coupled with the rise of JavaScript libraries and frameworks that offer more flexible and powerful DOM manipulation, has led to a significant decline in the use of client-side XSLT. Its role within the web browser has been largely superseded by JavaScript-based technologies, such as JSON+React.
Chromium uses the libxslt library to process these transformations, and libxslt was unmaintained for ~6 months of 2025. Libxslt is a complex, aging C codebase of the type notoriously susceptible to memory safety vulnerabilities like buffer overflows, which can lead to arbitrary code execution. Because client-side XSLT is now a niche, rarely-used feature, these libraries receive far less maintenance and security scrutiny than core JavaScript engines, yet they represent a direct, potent attack surface for processing untrusted web content. Indeed, XSLT is the source of several recent high-profile security exploits that continue to put browser users at risk. For these reasons, Chromium (along with both other browser engines) plans to deprecate and remove XSLT from the web platform. For more details, see this Chrome for Developers article.

- Chrome 143 on Android, ChromeOS, Linux, MacOS, Windows: Deprecation (but not removal) of the APIs.
- **Chrome 152 on Android, ChromeOS, Linux, MacOS, Windows:** Origin Trial (OT) and Enterprise Policy go live for testing. These allow sites and enterprises to continue using features past the removal date.
- Chrome 155 on Android, ChromeOS, Linux, MacOS, Windows: XSLT stops functioning on Stable releases, for all users other than Origin Trial and Enterprise Policy participants.
- Chrome 164 on Android, ChromeOS, Linux, MacOS, Windows: Origin Trial and Enterprise Policy stop functioning. XSLT is disabled for all users.

PostQuantum cryptography for DTLS in WebRTC

This feature will enable the use of PostQuantum Cryptography (PQC) with WebRTC connections. The motivation for PQC is to get WebRTC media traffic up to date with the latest cryptography protocols and prevent *Harvest Now to Crack Later* scenarios.
Admins will be able to control this feature using an enterprise policy WebRtcPostQuantumKeyAgreement, to allow enterprise users to opt out of PQC. The policy will be temporary and is planned to be removed by Chrome 152.

- Chrome 142 on Android, ChromeOS, Linux, MacOS, Windows, Fuchsia - Feature rolls out gradually
- **Chrome 152 on Android, ChromeOS, Linux, MacOS, Windows, Fuchsia**: Remove WebRtcPostQuantumKeyAgreement enterprise policy

Upcoming Chrome Enterprise Core updates

There are no Upcoming Chrome Enterprise Core updates.

Upcoming Chrome Enterprise Premium updates

Increased file size support for DLP scans

Chrome Enterprise Premium now extends its Data Loss Prevention (DLP) and malware scanning capabilities to include large and encrypted files.
Previously, files larger than 50 MB and all encrypted files were skipped during content scanning. This update closes that critical security gap. For policies configured to save evidence, files **up to 2GB** can now be sent to the Evidence Locker. This provides administrators with greater visibility and control, significantly reducing the risk of data exfiltration through large file transfers.
No new policy is required to enable this feature. It is automatically controlled by your existing DLP rule configurations in the Google Admin Console. If admins have rules that apply to file uploads, downloads, or printing, they will now also apply to large and encrypted files.
For more information, see What are ChromeOS data controls?

- **Chrome 147 on Linux, MacOS, Windows**: This stage enables the collection of large (>50 MB) and encrypted files for the Evidence Locker, closing a key Data Loss Prevention security gap.

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