



Chrome 145 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 28, 2026.

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

Chrome 145 release summary	2
Current Chrome browser updates	5
Current Chrome Enterprise Core updates	15
Current Chrome Enterprise Premium updates	17
Upcoming Chrome browser updates	18
Upcoming Chrome Enterprise Core updates	32
Upcoming Chrome Enterprise Premium updates	33
Additional resources	37
Still need help?	37

Chrome 145 release summary

Current Chrome browser updates	Security / Privacy	User productivity / Apps	Management
AI Mode and Lens enhancements		✓	
Disable force-installed extensions with non-malware violations	✓		
Change in release schedule in Chrome 145 (Early Stable only)			✓
Chrome WebGPU Toggle in AAPM	✓		
Chrome removes support for obsolete virtual cameras on macOS	✓	✓	✓
Credential Exchange on iOS	✓		
Device Bound Session Credentials	✓		
Introducing the Origin API	✓		
Local network access restrictions	✓		
Reduced User-Agent strings by default	✓		
Removal of the Google Cloud Print policy			✓
Use of CssPixels in LayoutShift API			✓
WebRequest.SecurityInfo in Controlled Frame		✓	
2SV enforcement for Admin accounts			✓
Import data from Safari to Chrome for iOS made easier			✓
On-device scam detection on Android	✓		

New policies in Chrome browser			✓
Removed policies in Chrome browser			✓
Chrome Enterprise Core updates	Security / Privacy	User productivity / Apps	Management
Introducing an AI-generated summary of the Release Notes in the Google Admin console			✓
Chrome Enterprise Premium updates	Security / Privacy	User productivity / Apps	Management
Hardening against local policy tampering	✓		✓
Upcoming Chrome browser updates	Security / Privacy	User productivity / Apps	Management
Bundled security settings	✓		
CSS Update: Decoupling of Width and Style Properties			✓
Remove third-party storage partitioning policies	✓		
Update to No HTTPS warning	✓		
X25519Kyber768 key encapsulation for TLS	✓		
Disallow spaces in non-file:// URL hosts	✓		
Gemini in Chrome		✓	
Origin-Bound cookies (by default)			✓
SafeBrowsing API v4 → v5 migration	✓		
UI Automation accessibility framework provider on Windows		✓	
Deprecation and removal of Privacy Sandbox APIs	✓	✓	

Enable "Always Use Secure Connections" by default	✓		
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
Experimental cryptographic compliance policies	✓		
Upcoming Chrome Enterprise Premium updates	Security / Privacy	User productivity / Apps	Management
Chrome Enterprise Connectors API	✓		✓
Enterprise cache encryption	✓		
Support for AllowList & BlockList for DeveloperToolsAvailability Policy	✓		✓
Support for AllowList & BlockList for IncognitoModeAvailability Policy	✓		✓
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 were 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]([Chrome Enterprise and Education Help Center](#) "Chrome—Generative AI features and policies").

In Chrome 144, we rolled 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).

Starting in Chrome 145 on Android and iOS, new AI Mode capabilities are integrated into Chrome browser.

- 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 145 on Android, iOS**
- Chrome 146 on macOS, Windows: Google Drive files become available as context. Admins can turn off these features (value 1) using the [SearchContentSharingSettings](#) policy.

- Chrome 147 on macOS, Windows: The [LensOverlaySettings](#), [LensDesktopNTPSearchEnabled](#) and [LensRegionSearchEnabled](#) policies will be deprecated. Admins can use [SearchContentSharingSettings](#) to control these features.

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 the policy 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.

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

Starting in Chrome 145, Chrome rolls 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 WebGPU toggle in AAPM

This update disables the WebGPU Javascript API in the Chrome browser for users enrolled in Android Advanced Protection Mode (AAPM).

Websites using [WebGPU](#) for 3D rendering (for example, Google Maps) will use slower alternatives like [WebGL](#). Expect decreased performance for heavy rendering (benchmarks indicated about a 5.78% latency decrease). Users are informed in AAPM settings.

For developers, the `navigator.gpu` object will be undefined, requiring you to implement a fallback option.

Admins retain control and may disable the feature if functional impact is prohibitive. The feature is toggled via an AAPM callback hook, requiring system/root access.

- **Chrome 145 on Android**

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**

Credential Exchange on iOS

Credential Exchange on iOS allows users to safely and securely export passwords and passkeys from Google Password Manager in Chrome on iOS to other credential manager apps on the device that support the [FIDO's Alliance Credential Exchange Protocol](#), implemented and facilitated by the OS.

Similarly, users can now import passwords and passkeys from participating credential manager apps on iOS.

Admins could control this feature using existing Enterprise policies [PasswordManagerEnabled](#) and [PasswordManagerPasskeysEnabled](#).

- **Chrome 145 on iOS:** Credential Exchange on iOS becomes available.

Device Bound Session Credentials

To enhance user security and combat session theft, Chrome is introducing [Device Bound Session Credentials \(DBSC\)](#). This feature allows websites to bind a user's session to their specific device, making it significantly harder for stolen session cookies to be used on other machines.

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

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**

Local network access restrictions

Chrome 142 restricted 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 145 introduces more granular permissions for websites requesting access to a user's local network. The previous single `local-network-access` permission is being split into two distinct permissions:

- `local-network`: Grants access to IP addresses in the local network space (for example, intranets, internal devices).
- `loopback-network`: Grants access to loopback IP addresses (for example., `localhost`, `127.0.0.1`).

The old `local-network` permission will remain as an alias, ensuring existing configurations and Permissions Policies continue to function as expected. This change provides both users and Admins with more precise control over how websites interact with internal network resources. Current enterprise policies managing local network access will not be affected by this change.

- **Chrome 145 on Android, Linux, macOS, Windows, Fuchsia:** The permission split is rolled out.
- Chrome 147 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](#) policy will be removed.

Reduced User-Agent strings by default

Starting in Chrome 145, we will remove the **UserAgentReduction** policy. 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, Chrome 145 removes the [CloudPrintProxyEnabled](#) policy. This policy previously 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 no longer needed in 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.

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

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 communicating with the correct server.

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

2SV enforcement for Admin accounts

To better protect your organization's information, Google now requires 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. In Chrome 145, 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

Import data from Safari to Chrome for iOS made easier

Users of Chrome for iOS can now 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

On-device scam detection on Android

When an on-device scam is detected using the visual features of the page, Chrome 145 now sends a request to **Safe Browsing** for a final verdict. Based on this verdict, Chrome decides whether to display a warning to the user.

This feature is enabled only for users in **Enhanced Protection** mode. The feature is disabled for **Standard Protection** mode users or users with **Safe Browsing** disabled. Admins can control this **Safe Browsing** setting with the [SafeBrowsingProtectionLevel](#) Chrome Enterprise policy.

- **Chrome 145 on Android**

New policies in Chrome browser

Policy	Description
BrowserSignin	Browser sign in settings
WebAppInstallByUserEnabled	Enable User Web App Install From Browser
EnableProxyOverrideRulesForAllUsers	Controls which managed users can set the ProxyOverrideRules policy.

Removed policies in Chrome browser

Policy	Description
UserAgentReduction	Control whether Chrome send a reduced or full User-Agent string
CloudPrintProxyEnabled	Enable the cloud print proxy
ExtensionForceInstallWithNonMalwareViolationsEnabled	Enable Force-installed Extensions With Non-Malware Violations
LocalNetworkAccessRestrictionsEnabled	Specifies whether to apply restrictions to requests to local network endpoints

Current Chrome Enterprise Core updates

Introducing an AI-generated summary of the Release Notes in the Google Admin console

Chrome 145 introduces AI-Generated Release Note Summaries in the Google Admin console. This Gemini-powered feature provides Admins to quickly digest key updates from the Chrome Enterprise Release Notes. Designed to streamline Chrome management, this new card provides AI-generated spotlight items and suggested actions, highlighting the most pertinent information for your domain, including new features, policy modifications and deprecation, and Chrome Enterprise Core functionalities. This will help Admins save time and more easily identify impactful changes and recommended actions.

This feature is planned for an early preview with Chrome Enterprise Trusted Testers starting with Chrome 145. For more details, see [Chrome Enterprise Trusted Testers](#).

- **Chrome 145 on Android, iOS, Linux, macOS, Windows** - Early preview available to Chrome Enterprise Trusted Testers

Admin

Home

Dashboard

Directory

Chrome browser

Overview

Setup guide

Managed browsers

Managed profiles

Virtual apps preview

Settings

Custom configurations

Tokens

Apps & extensions

Connectors

Reports

Devices

Apps

Security

Search

Chrome Browser > Overview

Overview

Insights from active browsers & profiles across your organization

Recommendations

0/2 items complete

Review AI synthesis of Chrome 138 release notes

Powered by Gemini

See release notes

Policies

Extensions

Management

End user Productivity

Security

Configure proxy override roles: In Chrome 144, use the ProxyOverrideRules policy to set routing rules that are evaluated before any existing proxy configuration.

Configure in JSON

Policy X deprecation: Chrome 138 will deprecate Policy Name X soon. This policy is still enabled in OU X.

Manage policy

AI synthesis of Chrome release notes can make mistakes, so double-check it

Customize your organization's Chrome Web Store

Showcase private extensions, recommend custom collections and more

Customize

Managed browsers

Active	Inactive	New
85.6k	12.4k	12
85.6%	12.4%	0.1%

Operating system

Windows 14.5	11k	62%
Windows 14.4	291	10%
MacOS 13.4	12	1%
Windows 13.3	21	2%
Other	1k	19%

View all

Managed profiles

Active	Inactive	New
53.2k	46.8k	3.2k
53.2%	46.8%	3.2%

Affiliation

Affiliated	13k	62%
Unaffiliated cloud machine	291	10%
Unaffiliated local machine	12	1%
Profile-only	21	2%
Unknown	1k	19%

View all

Current Chrome Enterprise Premium updates

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.

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

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**

CSS update: decoupling of Width and Style properties

Chrome will soon align with updated [CSS specifications](#) regarding the behavior of `border-width`, `outline-width`, and `column-rule-width` properties. Previously, if the corresponding `border-style`, `outline-style`, or `column-rule-style` was set to `none` or `hidden`, the computed width of these properties would be forced to `0px`, regardless of the specified value.

With this change, the computed values of `border-width`, `outline-width`, and `column-rule-width` will always reflect the author-specified values, independent of the `*-style` property. Additionally, the

resolved values (as returned by `getComputedStyle()`) for outline-width and column-rule-width also will reflect the specified values.

The change aligns Chrome with Firefox and WebKit, which have already implemented this behavior.

- **Chrome 146 on Windows, macOS, Linux, Android**

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.

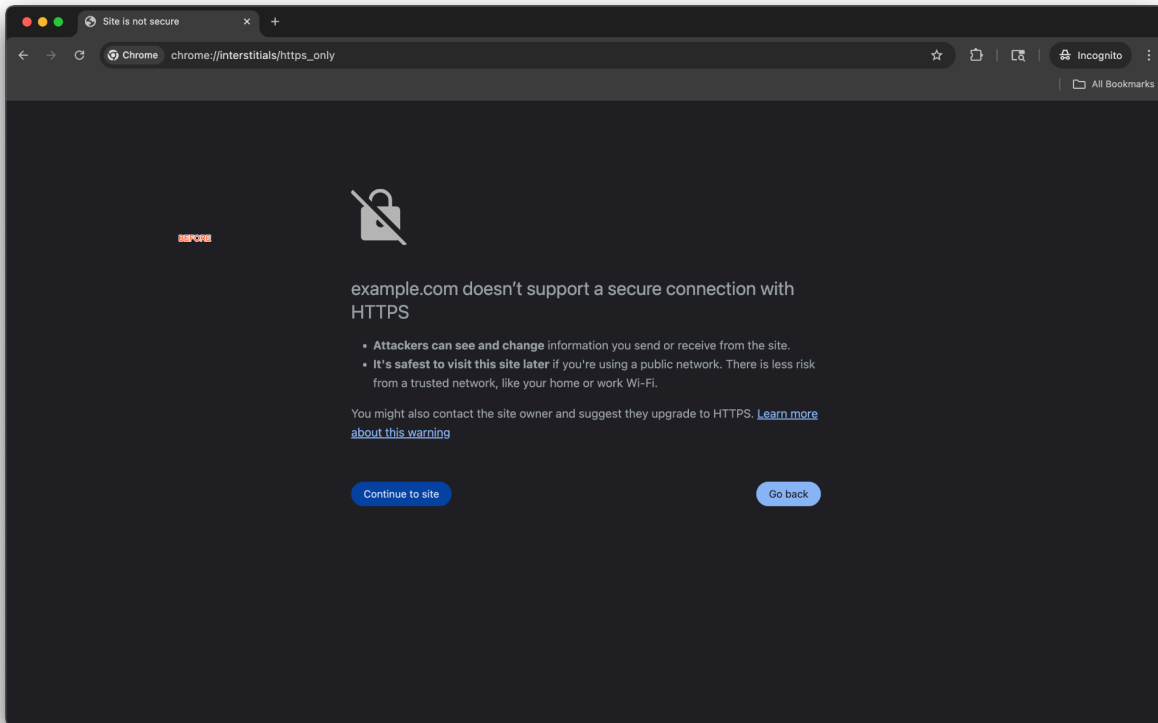
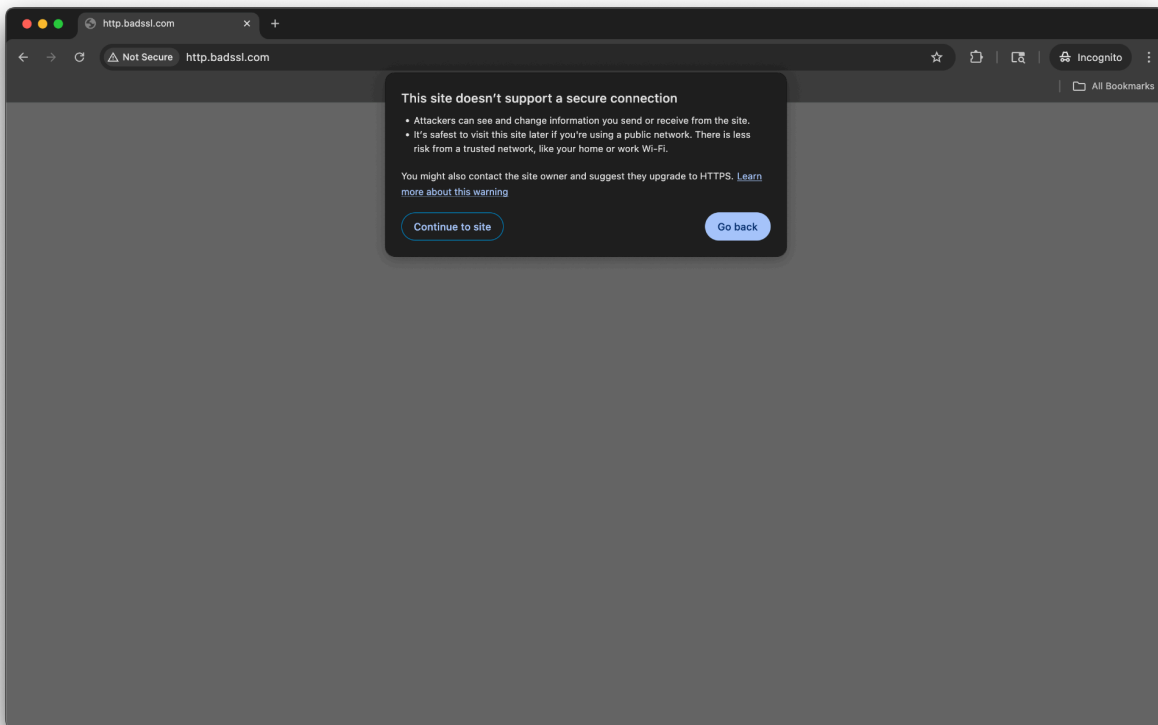
If you have any feedback, you can add it [here in the Chromium bug](#).

- **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.



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 Chrome 145. However, long term, post-quantum secure ciphers will be required in TLS and the enterprise policy will be removed as of Chrome 146. Post-quantum cryptography is required for CSNA 2.0. To learn more, see [Protect Chrome Traffic with Hybrid Kyber 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:** [PostQuantumKeyAgreementEnabled](#) 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**

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.

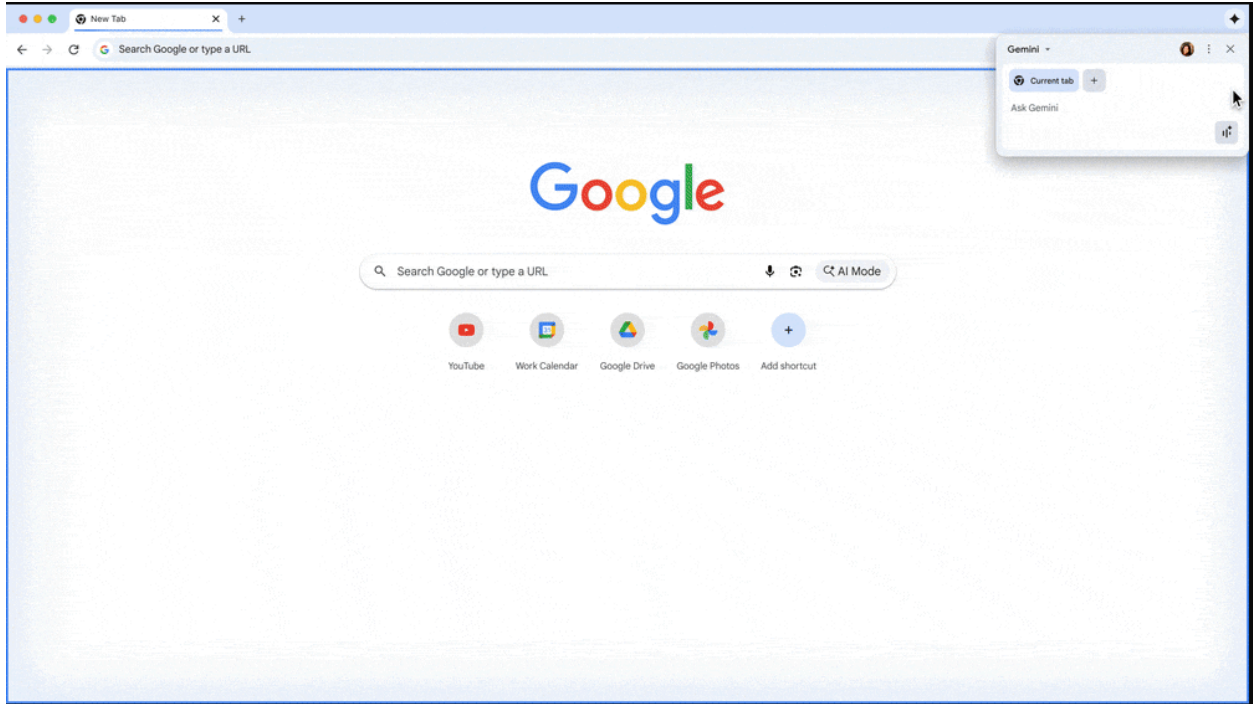
In Chrome 143, [Gemini in Chrome](#) started to roll out to most Google Workspace users with access to the Gemini app in the US. Admins can turn off this feature (value 1) using the [GeminiSettings](#) policy or by using the [GenAiDefaultSettings](#) (value 2). For more details, see [Gemini in Chrome](#) in the Help Center or this [blog post](#).

Also in Chrome 143, we announced 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.

In Chrome 144, agentic capabilities in Gemini in Chrome were 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 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](#) policy and the [OnBulkDataEntryEnterpriseConnector](#) settings.
- Chrome 144 on ChromeOS: 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 145 on ChromeOS, macOS, Windows:** Gemini in Chrome will gradually roll out to users in Canada, New Zealand and India in English
- 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.



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] (<https://developers.google.com/safe-browsing/v4>) 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**

UI Automation accessibility framework provider on Windows

Chrome 126 began to directly support 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 can 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 148. 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 148 on Windows:** The [UiAutomationProviderEnabled](#) policy will be removed from Chrome. All clients will use the browser's UI Automation accessibility framework provider.

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 began 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

Enable "Always Use Secure Connections" by default

Chrome 150 will enable the **Always Use Secure Connections** setting in the "public sites only" mode by default. This means Chrome will ask for the user's permission before the first access to any public site without HTTPS. Public sites are defined as sites that have a globally unique name, and excludes direct navigation to RFC 1918 addresses (192.168.0.1, 10.0.0.0/8, etc), as well as shortnames such as go/.

Prior to enabling it by default for all users, Chrome will enable **Always Use Secure Connections** for the users who have opted-in to [Enhanced Safe Browsing protections in Chrome](#).

If you are a website developer or IT professional, and you have users who may be impacted by this feature, we very strongly recommend enabling the "Always Use Secure Connections" setting today to help identify sites that you may need to work to migrate. Admins can use the [HttpAllowlist](#) and [HttpsOnlyMode](#) policies to override this behavior.

For more information, see our [adoption guide](#) and [announcement blog post](#).

- **Chrome 150 on Android, ChromeOS, Linux, macOS, Windows, Fuchsia:** Enable "Always Use Secure Connections" for users who have opted in to Enhanced Safe Browsing.
- **Chrome 154 on Android, ChromeOS, Linux, macOS, Windows, Fuchsia:** Enable "Always Use Secure Connections" by default for all users.

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

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.

Upcoming Chrome Enterprise Premium updates

Chrome Enterprise Connectors API

Chrome Enterprise will soon expand programmatic management for [Chrome Enterprise Connectors](#). This update will introduce resources to define and assign connector configurations, complementing the existing connector policies to allow administrators to manage the full life-cycle of these integrations at scale.

Previously, configuring Service Providers was a manual process in the Google Admin console. This update enables automation, which helps reduce manual errors and improve the efficiency of managing integrations with third-party security solutions.

Administrators can now use the Chrome Management API to manage ConnectorConfiguration resources (defining the provider). Connector Selection is managed via the Chrome Policy API, enabling the assignment of these configurations to Organizational Units or Groups. This works in tandem with existing Policy API settings for event reporting and content analysis, including policies such as [OnSecurityEventEnterpriseConnector](#), [OnFileAttachedEnterpriseConnector](#), [OnFileDownloadedEnterpriseConnector](#), [OnBulkDataEntryEnterpriseConnector](#), [OnPrintEnterpriseConnector](#), and [EnterpriseRealTimeUrlCheckMode](#). For technical details, developers should refer to the [Chrome Management API](#) and [Chrome Policy API documentation](#).

- Chrome 143 on Android, iOS, Linux, macOS, Windows: This rollout adds support for programmatic management of Chrome Enterprise Connectors via a new API
- **Chrome 146 on Android, iOS, Linux, macOS, Windows:** This rollout introduces the ConnectorConfiguration and ConnectorSelection resources, enabling the creation of service provider instances and their assignment to organizational units.

Enterprise cache encryption

Chrome Enterprise Premium will offer Enterprise cache encryption, a feature designed to mitigate data exfiltration risks by encrypting browser data stored at rest, specifically the HTTP cache. Using OS-level APIs for key storage through App-Bound Encryption, this functionality renders locally stored data inaccessible to malware if a device is compromised.

This feature operates transparently in the background, though it may impact performance due to real-time encryption. Administrators can manage this via the **CacheEncryptionEnabled** policy. Note that enabling or disabling this policy will automatically clear the existing cache to ensure data consistency.

- **Chrome 146 on Linux, macOS, Windows:** Cache encryption becomes available on desktop platforms

Support for AllowList and BlockList for DeveloperToolsAvailability policy

Chrome will introduce two new policies, **DeveloperToolsAvailabilityAllowlist** and **DeveloperToolsAvailabilityBlocklist**, which provide granular control over the availability of Developer Tools based on URL patterns.

Previously, administrators could only allow or disallow Developer Tools globally. With these new policies, admins can now enforce a general block on Developer Tools to secure sensitive corporate data, while explicitly permitting access on specific internal URLs for development or troubleshooting purposes.

These controls are available on Windows, Mac, Linux, and ChromeOS. If these new policies are not configured, the behavior of the existing [DeveloperToolsAvailability](#) policy remains unchanged.

- **Chrome 146 on ChromeOS, Linux, macOS, Windows** - Feature rolls out gradually. Introduces the **DeveloperToolsAvailabilityAllowlist** and **DeveloperToolsAvailabilityBlocklist** policies on Desktop platforms.

Support for AllowList and BlockList for IncognitoModeAvailability policy

Chrome will introduce two new policies, **IncognitoModeUrlBlocklist** and **IncognitoModeUrlAllowlist**, to provide administrators with more precise control over Incognito mode usage. Previously, administrators could only completely enable or disable Incognito mode via the [IncognitoModeAvailability](#) policy.

These new policies function similarly to the existing [URLBlocklist](#) and [URLAllowlist](#) policies but are specifically designated for Incognito sessions. This allows organizations to restrict access to specific URLs in Incognito mode to protect sensitive information while permitting legitimate usage on other sites.

- **Chrome 146 on Android, iOS, ChromeOS, Linux, macOS, Windows** - Feature rolls out gradually. Introduces the **IncognitoModeUrlBlocklist** and **IncognitoModeUrlAllowlist** policies.

Increased file size support for DLP scans

Chrome Enterprise Premium will extend 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](#)

Google and related marks and logos are trademarks of Google LLC. All other company and product names are trademarks of the companies with which they are associated.