chrome enterprise

Chrome 146 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 February 25, 2026.

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

Chrome 146 release summary

Current Chrome browser updates	**Security / Privacy**	**User productivity / Apps**	**Management**
AI Mode and Lens enhancements		✓	
Extended Autofill experience		✓	
Local network access restrictions	✓		
Bundled security settings	✓		
Remove third-party storage partitioning policies	✓		
New policies in Chrome browser			✓
Removed policies in Chrome browser			✓
Chrome Enterprise Core updates	**Security / Privacy**	**User productivity / Apps**	**Management**
Spin.AI Risk score update in the Admin console	✓		✓
Experimental cryptographic compliance policies	✓		
Seamless Okta Single Sign-On on macOS	✓		
Chrome Enterprise Premium updates	**Security / Privacy**	**User productivity / Apps**	**Management**
Enterprise cache encryption	✓		
Hardening against local policy tampering	✓		✓
Upcoming Chrome browser updates	**Security / Privacy**	**User productivity / Apps**	**Management**

CSS update: decoupling of Width and Style properties			✓
Device Bound Session Credentials	✓		
Disallow spaces in non-file:// URL hosts	✓		
Gemini in Chrome		✓	
Report-a-Scam	✓		
UI Automation accessibility framework provider on Windows		✓	
X25519Kyber768 key encapsulation for TLS	✓		
Enhanced autofill		✓	
Origin-Bound cookies (by default)			✓
Update to No HTTPS warning	✓		
Deprecation and removal of Privacy Sandbox APIs	✓	✓	
Enable "Always Use Secure Connections" by default	✓		
Isolated Web Apps			✓
SafeBrowsing API v4 → v5 migration	✓		
Chrome will remove support for macOS 12			✓
Deprecate and remove XSLT	✓	✓	✓
PostQuantum cryptography for DTLS in WebRTC	✓		
Disallow spaces in non-file:// URL hosts	✓		
Upcoming Chrome Enterprise Core updates	**Security / Privacy**	**User productivity / Apps**	**Management**

There are no Upcoming Chrome Enterprise Core updates.			

Upcoming Chrome Enterprise Premium updates	**Security / Privacy**	**User productivity / Apps**	**Management**
Chrome Enterprise Connectors API	✓		✓
Increased file size support for DLP scans	✓		✓
Support for AllowList and BlockList for DeveloperToolsAvailability policy	✓		✓
Support for AllowList and BlockList for IncognitoModeAvailability policy	✓		✓
Enterprise extension DOM activity telemetry	✓		

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

Previously, 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.

In Chrome 145, 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). Also in Chrome 145 on Android and iOS, new AI Mode capabilities were integrated into Chrome browser.

In Chrome 146, Google Drive files become available as context. Admins can turn off these features (value 1) using the SearchContentSharingSettings policy.

- Chrome 143 on macOS, Windows: New AI Mode capabilities will be integrated into Chrome and can be controlled using AIModeSettings policy or the GenAiDefaultSettings policy
- Chrome 145 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: New AI Mode capabilities will gradually become available on Android and 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

Extended Autofill experience
Starting in Chrome 146, some users can save and autofill additional types of data previously only available to users with Enhanced autofill enabled. Admins can control the feature using the existing AutofillAddressEnabled, GenAiDefaultSettings and AutofillPredictionSettings policies.

- **Chrome 146 on ChromeOS, Linux, macOS, Windows** - Feature rolls out gradually

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 introduced 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 provided 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.

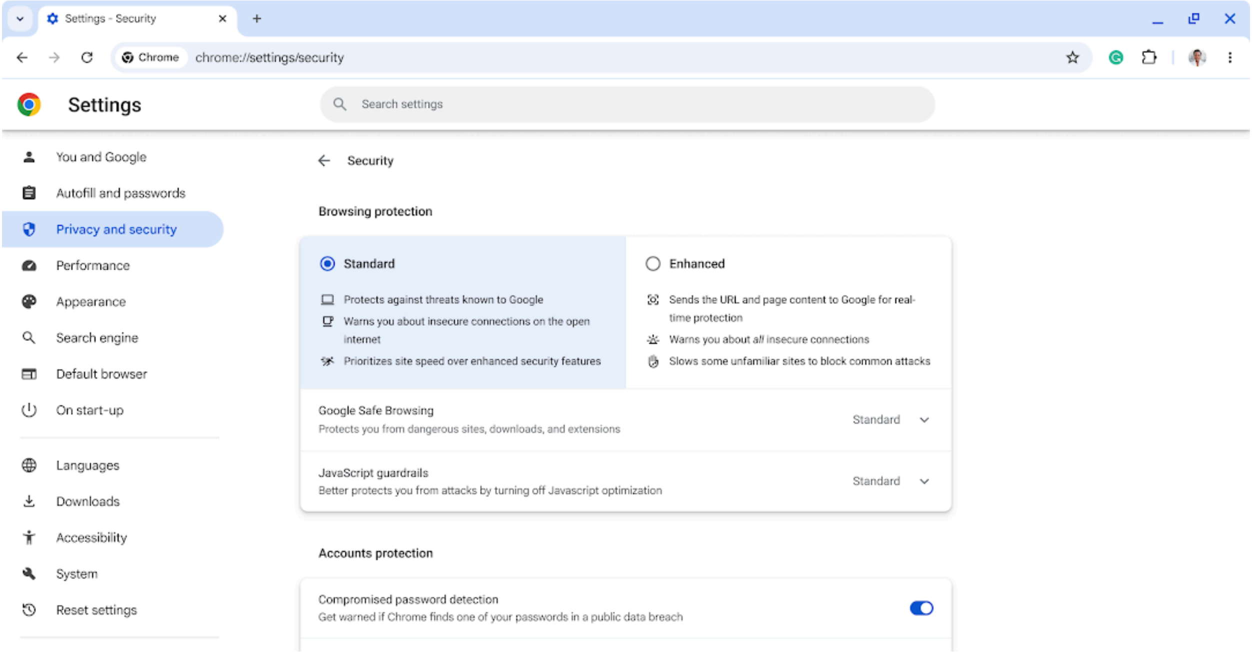
Chrome 146 introduces two new enterprise policies for managing local network access restrictions: LocalNetworkAccessIpAddressSpaceOverrides and LocalNetworkAccessPermissionsPolicyDefaultEnabled.

- Chrome 145 on Android, Linux, macOS, Windows, Fuchsia: The permission split is rolled out.
- **Chrome 146 on Android, ChromeOS, Linux, macOS, Windows, Fuchsia**: Two new enterprise policies will be available for managing local network access restrictions:
    - LocalNetworkAccessIpAddressSpaceOverrides could be used to mark IPv4 and IPv6 address blocks as public or private. IP ranges that are treated as public will not cause permission prompts when accessed by other pages. For example, CGNAT 100.64.0.0/10 can be marked as public. This is useful for certain VPN and proxy setups. Marking 0.0.0.0/0 and ::/0 as public is equivalent to disabling the local network access restrictions.
    - LocalNetworkAccessPermissionsPolicyDefaultEnabled can be used to cause the LNA permission to be automatically delegated to iframes by the parent frame, without requiring explicit annotation of the child iframes. This is useful in situations where local network access is performed by an embedded SaaS tool inside of a different SaaS tool. This includes certain locally hosted documentation and knowledgebase softwares.
- 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.

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.



Security

Browsing protection

● Standard
- Protects against threats known to Google
- Warns you about insecure connections on the open internet
- Prioritizes site speed over enhanced security features

○ Enhanced
- Sends the URL and page content to Google for real-time protection
- Warns you about *all* insecure connections
- Slows some unfamiliar sites to block common attacks

Google Safe Browsing — Standard
Protects you from dangerous sites, downloads, and extensions

JavaScript guardrails — Standard
Better protects you from attacks by turning off Javascript optimization

Accounts protection

Compromised password detection
Get warned if Chrome finds one of your passwords in a public data breach

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

Remove third-party storage partitioning policies

Third-party storage partitioning became the default in Chrome 115. Chrome 128 removed the chrome:// flag that allowed users to disable this feature, and the deprecation trial ended with Chrome 139. In Chrome 146, we remove the enterprise policies

DefaultThirdPartyStoragePartitioningSetting and ThirdPartyStoragePartitioningBlockedForOrigins. We advise users 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

New policies in Chrome browser

Policy	Description
BlockExternalExtensions	Blocks external extensions from being installed
CacheEncryptionEnabled	This policy allows administrators to encrypt http cache on disk.
DefaultIdleDetectionSetting	Default idle detection setting
ExtensibleEnterpriseSSOBlocklist	Blocklist of identity providers that cannot use Extensible Enterprise SSO for the browser
ExtensionAllowedTypes	Configure allowed app/extension types
ExtensionDeveloperModeSettings	Control the availability of developer mode on extensions page
ExtensionInstallAllowlist	Configure extension installation allow list
ExtensionInstallBlocklist	Configure extension installation blocklist
ExtensionInstallForcelist	Configure the list of force-installed apps and extensions
ExtensionInstallSources	Configure extension, app, and user script install sources
ExtensionSettings	Extension management settings

Policy	Description
ForceForegroundPriorityForAllTabs	Force foreground priority for all tabs
GeminiActOnWebAllowedForURLs	Allow Gemini app integrations to directly act on specified sites
GeminiActOnWebBlockedForURLs	Block Gemini app integrations to directly act on specified sites
IdleDetectionAllowedForUrls	Allow idle detection on these sites
IdleDetectionBlockedForUrls	Block idle detection on these sites
LocalNetworkAccessIpAddressSpaceOverrides	Override IP address space mappings
LocalNetworkAccessPermissionsPolicyDefaultEnabled	Allow Local Network Access (LNA) requests in subframes without explicit delegation
LocalNetworkAllowedForUrls	Allow sites to make network requests to local network endpoints.
LocalNetworkBlockedForUrls	Block sites from making network requests to local network endpoints.
LoopbackNetworkAllowedForUrls	Allow sites to make network requests to the local device.
LoopbackNetworkBlockedForUrls	Block sites from making network requests to the local device.
PreferSlowCiphers	Prefer specific encryption cipher algorithms for TLS
PreferSlowKexAlgorithms	Prefer specific key exchange algorithms for TLS
XSLTEnabled	Control the availability of the XSLT feature

Removed policies in Chrome browser

Policy	Description
DefaultThirdPartyStoragePartitioningSetting	Default third-party storage partitioning setting
ThirdPartyStoragePartitioningBlockedForOrigins	Disable third-party storage partitioning for specific top-level origins

Current Chrome Enterprise Core updates

Spin.AI Risk score update in the Admin console

As early as Chrome 146, the risk assessment scores for Spin.AI in the **Admin console** will reflect recent changes made by Spin.AI. The scoring still follows the 0 to 100 scale, however, a score of 0 will reflect low risk, while a score of 100 will reflect a high risk.

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.

Seamless Okta Single Sign-On on macOS

Chrome on macOS now provides an enhanced Single Sign-On (SSO) experience for organizations using Okta. When a macOS device is managed and configured with the appropriate Extensible Enterprise SSO Mobile and Device Management (MDM) profile for Okta, users will benefit from a seamless authentication flow.

Specifically, prompts that previously asked for user permission to open the Okta Verify application or to allow local network communications during Okta FastPass authentication will no longer appear. Chrome will use Apple's built-in Extensible SSO mechanism to handle these authentications.

Requirements:

- The device must be running macOS.
- The device must be managed and have the correct ExtensibleEnterpriseSSO MDM profile configured by an administrator.
- The organization's Okta environment must be set up to support this flow.
- The Okta Verify application must be installed on the device.

Admins can manage this feature using the ExtensibleEnterpriseSSOBlocklist policy. To prevent Chrome from using the built-in Okta SSO integration, add okta to the policy's list of strings. To disable this built-in integration for all supported identity providers, add the value all.

This update aims to reduce user interruption and streamline access to Okta-protected resources.

- **Chrome 146 on macOS** - Feature rolls out gradually

Current Chrome Enterprise Premium updates

Enterprise cache encryption

Chrome Enterprise Premium offers 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

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 bring-your-own-device (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

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 will also reflect the specified values.

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

- **Chrome 147 on Windows, macOS, Linux, Android**: No rollout step

Device Bound Session Credentials

To enhance user security and combat session cookie 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 - Feature rolls out gradually
- **Chrome 147 on macOS** - Feature rolls out gradually

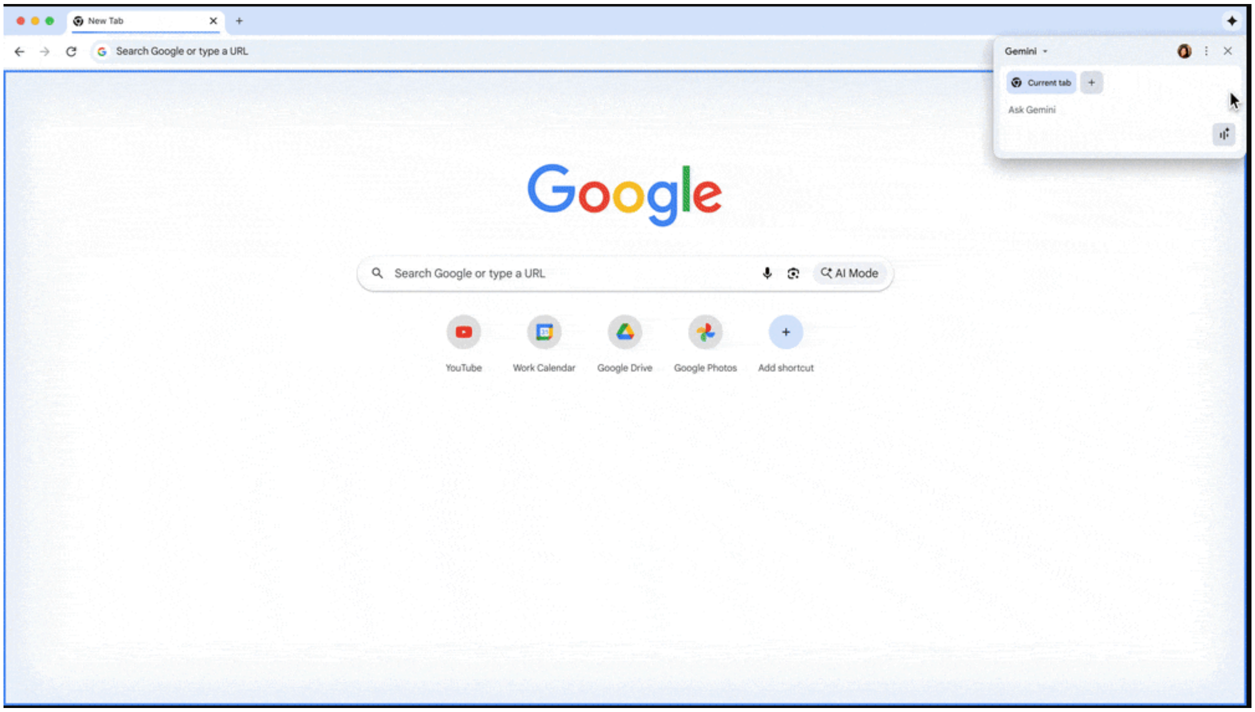
Gemini in Chrome

Gemini is now integrated into Chrome on macOS, Windows and selective ChromeOS devices, 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. Gemini in Chrome automatically uses public information from these Google services: Google Search, Google Maps, YouTube. With your permission, Gemini in Chrome can help you connect your personal information and content in Google Workspace services (Gmail, Drive, Keep, Calendar, and Tasks).

In Chrome 144, auto browse in Gemini in Chrome was made available to some users (non-enterprise). An enterprise policy GeminiActOnWebSettings will be available at launch.



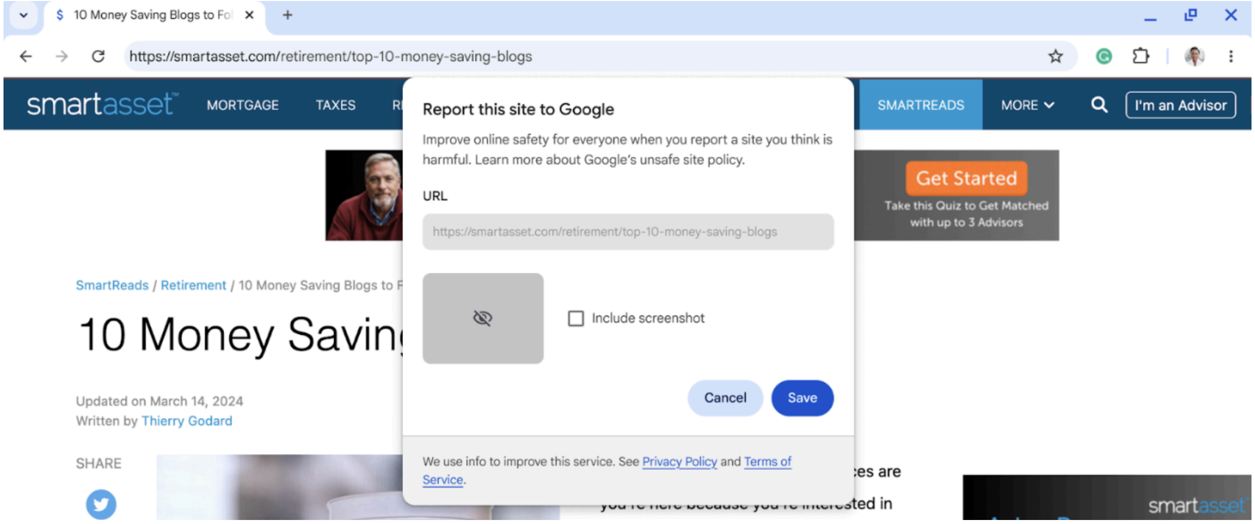
- Chrome 137 on macOS, Windows: Feature is available for some Google AI Pro and Ultra subscribers in the US and on pre-Stable (Dev, Canary, Beta) channels in the US.
- Chrome 144 on macOS, Windows: Auto browse in Gemini in Chrome available to some users (non-enterprise). Enterprise policy GeminiActOnWebSettings 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 ChromeOS: Gemini in Chrome rolled out to selective ChromeOS devices
- Chrome 144 on macOS, Windows: Gemini in Chrome allows 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... The US rollout will also support the same languages.
- **Chrome 147 on macOS, Windows**: Auto browse in Gemini in Chrome available to enterprise users. Enterprise policies GeminiActOnWebSettings,

GeminiActOnWebAllowedForURLs and GeminiActOnWebBlockedForURLs are available to control auto browse.
- **Chrome 147 on ChromeOS, macOS, Windows**: Gemini in Chrome will be able to use Chrome Autofill to fill credit card and address forms (with user permission). This will respect the AutofillAddressEnabled and AutofillCreditCardEnabled enterprise policies, as well as the general GeminiActOnWebSettings, GeminiActOnWebAllowedForURLs and GeminiActOnWebBlockedForURLs policies for agentic Gemini in Chrome.
- Chrome 148 on macOS, Windows: As early as Chrome 148 on macOS, Windows: auto browse in Gemini in Chrome available to enterprise users.

Report-a-Scam

With Safe Browsing switched on, users can report web pages directly to Safe Browsing from Chrome via the Help menu.

Admins can opt out of this feature by turning off Safe Browsing using SafeBrowsingProtectionLevel or by disallowing user feedback via UserFeedbackAllowed.


10 Money Saving Blogs to Fo
https://smartasset.com/retirement/top-10-money-saving-blogs
smartasset
MORTGAGE
TAXES
SMARTREADS
MORE
I'm an Advisor
Get Started
Take this Quiz to Get Matched with up to 3 Advisors
SmartReads / Retirement / 10 Money Saving Blogs to F
10 Money Savin
Updated on March 14, 2024
Written by Thierry Godard
SHARE

Report this site to Google

Improve online safety for everyone when you report a site you think is harmful. Learn more about Google's unsafe site policy.

URL

https://smartasset.com/retirement/top-10-money-saving-blogs

☐ Include screenshot

Cancel Save

We use info to improve this service. See Privacy Policy and Terms of Service.

- **Chrome 147 on 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 146 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 might 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.

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 in Chrome 147. 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 147 on Linux, macOS, Windows**: PostQuantumKeyAgreementEnabled enterprise policy will be removed

Enhanced autofill

From Chrome 137 onwards, some users can turn on Enhanced Autofill, a feature that helps users fill out online forms more easily. On relevant forms, Chrome can use AI to better understand the form and offer users to automatically fill in previously saved info. Admins can control the feature using the existing GenAiDefaultSettings policy and a new AutofillPredictionSettings policy.

- Chrome 137 on ChromeOS, Linux, macOS, Windows - Feature rolls out gradually
- Chrome 140 on ChromeOS, Linux, macOS, Windows: The existing "Autofill with AI" feature will be renamed to "Enhanced autofill", allow users to save and fill additional types of info, and become available in more countries and languages.

- **Chrome 148 on Android**: Enhanced autofill will be made available to users of Chrome on Android.

Origin-Bound cookies (by default)

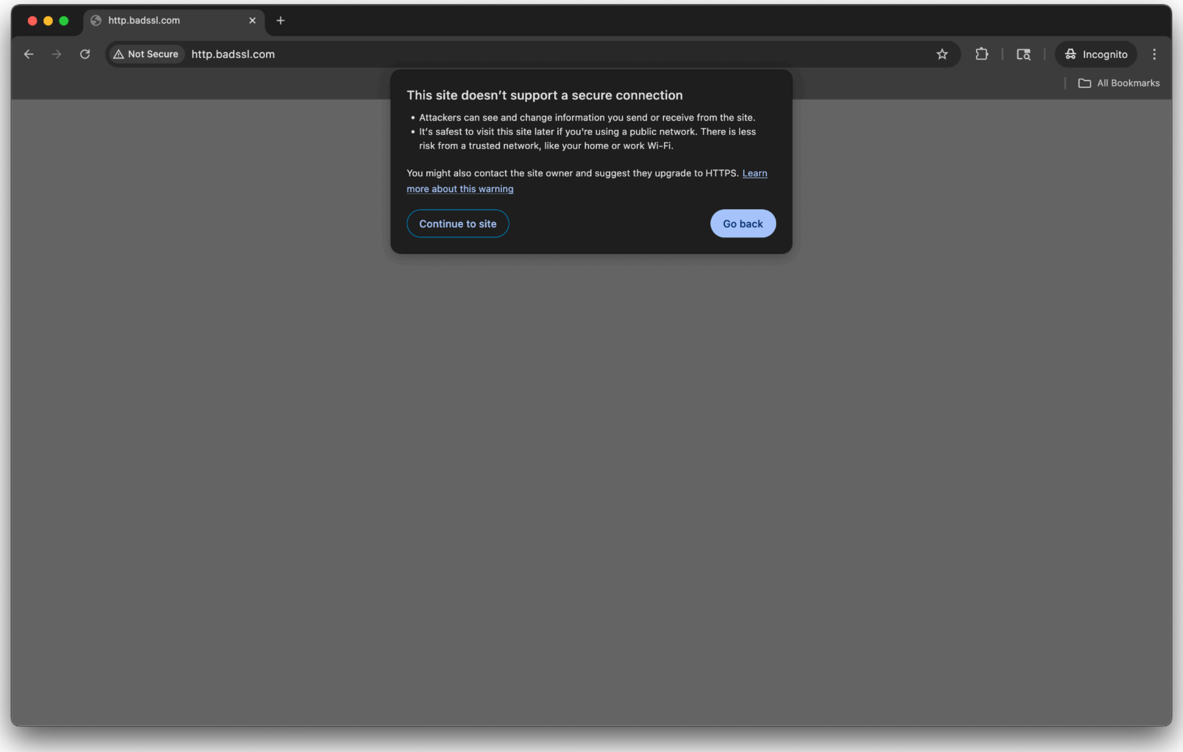
In Chrome 148, cookies are bound to their setting origin (by default) such that they're only accessible by that origin, that is, they are sent on a request or visible through document.cookie. Cookies might ease the host and port binding restrictions through use of the Domain attribute but all cookies 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.

Update to No HTTPS warning

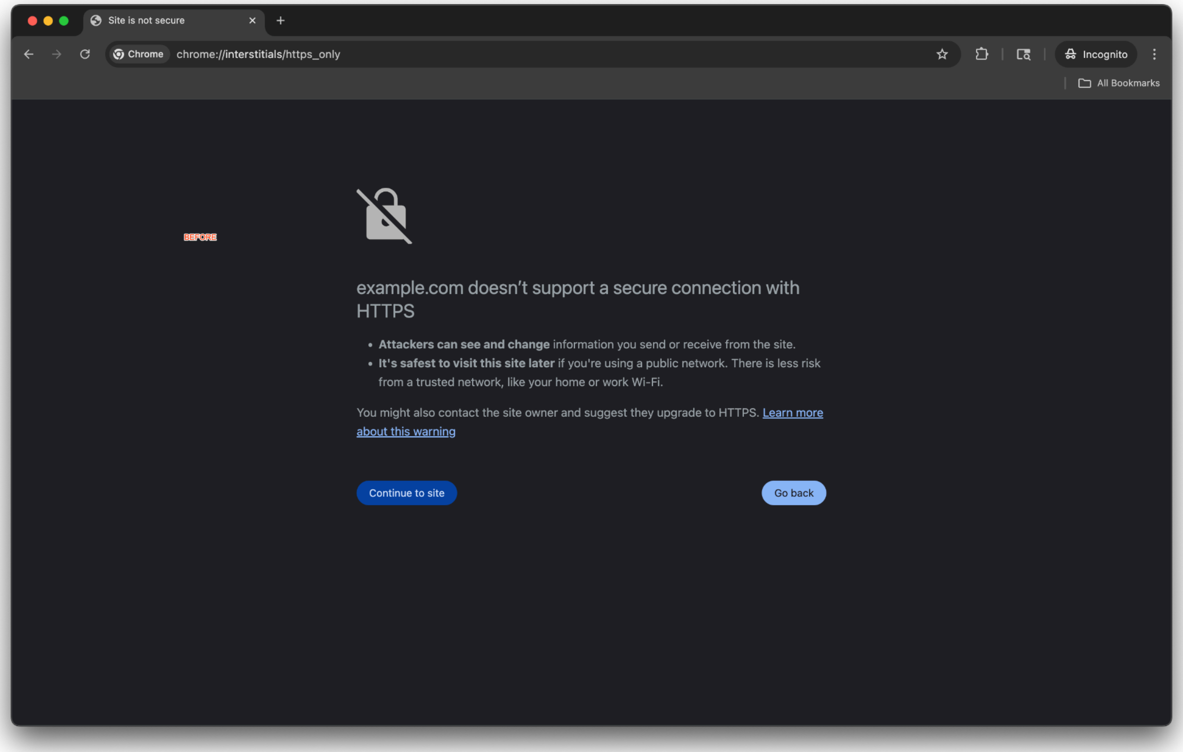
The warning displayed when a user opts-in to the **Always Use Secure Connections** on chrome://settings/security is changing from an interstitial to a dialog. Full page load remains blocked, and the functionality remains the same. The URL content security indicator on the warning is changing from the *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.



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



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

- Chrome 141 on ChromeOS, Linux, macOS, Windows: New warning design on desktop platforms.
- **Chrome 148 on Android**: Similar updated warning design on Android, using a warning bubble instead of a full interstitial.

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, and so on), 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** - Feature rolls out gradually: Enable "Always Use Secure Connections" for users who have opted in to Enhanced Safe Browsing.
- Chrome 154 on Android, ChromeOS, Linux, macOS, Windows, Fuchsia - Feature rolls out gradually: 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.

SafeBrowsing API v4 to v5 migration

Chrome calls into the SafeBrowsing v4 API will be migrated to call into the v5 API instead. The method names are also different between v4 and v5. If admins have any v4-specific URL allowlisting to allow network requests to https://safebrowsing.googleapis.com/v4*, these should be modified to allow network requests to the whole domain instead: safebrowsing.googleapis.com. Otherwise, rejected network requests to the v5 API will cause security regressions for users. For more details, see Migration From V4 - Safe Browsing.

- **Chrome 150 on Android, iOS, ChromeOS, Linux, macOS, Windows -** Feature rolls out gradually

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**: No rollout step

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

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 157 on Android, ChromeOS, LaCrOS, Linux, macOS, Windows, Fuchsia**

Upcoming Chrome Enterprise Core updates

There are no Upcoming Chrome Enterprise Core updates.

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 147 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.

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.

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 147 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 147 on Android, iOS, ChromeOS, Linux, macOS, Windows -** Feature rolls out gradually: Introduces the **IncognitoModeUrlBlocklist** and **IncognitoModeUrlAllowlist** policies.

Enterprise extension DOM activity telemetry

This enterprise-only feature provides security auditing for Chrome Extensions by creating a high-fidelity pipeline that monitors risky behavior. It specifically focuses on identifying Code Injection (execution risks) and Data Access (theft risks) occurring between web pages and extensions. Verified signals are filtered to ensure browser performance is not impacted, and they are ultimately transmitted using the Chrome real-time reporting pipeline for Security Information and Event Management (SIEM) system analysis. This feature can be enabled by admins using the **ExtensionDOMActivityLoggingEnabled** policy.

- **Chrome 148 on ChromeOS, Linux, macOS, Windows** - Early preview available to Chrome Enterprise Trusted Testers

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.