chrome enterprise

Chrome 143 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 November 19, 2025, last updated December 3, 2025.

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

Chrome 143 release summary

Current Chrome browser updates	Security / Privacy	User productivity / Apps	Management
Deprecate and remove XSLT	✓	✓	✓
AI Mode enhancements		✓	
ICU version 77.1 (supporting Unicode 16)			✓
New policies in Chrome browser			✓
Chrome Enterprise Core updates	**Security / Privacy**	**User productivity / Apps**	**Management**
Dynamic Recommendations in the Admin console			✓
Enterprise-managed shortcuts on the New tab page		✓	✓
Profile reporting for Chrome on iOS			✓
Chrome Enterprise Premium updates	**Security / Privacy**	**User productivity / Apps**	**Management**
Client certificates support on Chrome for Android	✓		
Upcoming Chrome browser updates	**Security / Privacy**	**User productivity / Apps**	**Management**
Gemini in Chrome		✓	
Bundled security settings	✓		

Deprecating savedTabGroups as individual value in SyncTypesListDisabled			✓
Happy Eyeballs V3	✓		✓
Multicast support for Direct Sockets API.			✓
On-device scam detection on Android	✓		
ServiceWorkerAutoPreload			✓
Update to *No HTTPS* warning design	✓		
2SV enforcement for admins			✓
CSS find-in-page highlight pseudos			✓
Change in launch schedule starting in Chrome Early Stable 145			✓
Disable force-installed extensions with non-malware violations	✓		
Origin-bound cookies (by default)			✓
Remove third-party storage partitioning policies	✓		
X25519Kyber768 key encapsulation for TLS	✓		
Disallow spaces in non-file:// URL hosts	✓		
UI Automation accessibility framework provider on Windows		✓	
SafeBrowsing API v4 → v5 migration	✓		
Isolated Web Apps			✓
PostQuantum cryptography for DTLS in WebRTC	✓		

Local network access restrictions	✓		✓
Upcoming Chrome Enterprise Core updates	**Security / Privacy**	**User productivity / Apps**	**Management**
No upcoming feature announcements			
Upcoming Chrome Enterprise Premium updates	**Security / Privacy**	**User productivity / Apps**	**Management**
Copy and Paste rules protection	✓		✓
Proxy override rules	✓		✓
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

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, but libxslt has been unmaintained for approximately 6 months of 2025. `Libxslt` is a complex, aging, C codebase that is 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.

AI Mode enhancements

Chrome 143 integrates new AI Mode capabilities into Chrome on macOS and Windows. Users will be able to access AI Mode directly from the **New tab** page and the omnibox, allowing users to ask complex questions directly from where they start browsing. This will start rolling out in Chrome 143 on macOS and Windows. Admins can turn off these features (value 1) using the AIModeSettings policy or by using the GenAiDefaultSettings (value 2). For more details, see the relevant section in the Help Center.
Also coming in Chrome 144 is the multi-tab context feature. Users can choose to share the contents of one or more of their open tabs with AI Mode, helping them ask questions, compare, summarize, and find information more efficiently. Admins will be able to turn off these features (value 1) using the **SearchContentSharingSettings** policy (available in Chrome 144) or by using the GenAiDefaultSettings (value 2).

- **Chrome 143 on MacOS, Windows**: New AI Model capabilities 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

ICU version 77.1 (supporting Unicode 16)

The Unicode support library, International Components for Unicode (ICU), is upgraded from version 74.2 to version 77.1, adding support for Unicode 16 and updating locale data.
Two changes could pose some risk for web applications that assume a specific format from the Intl JS APIs:

1. The default Italian number formatting changed to omit the thousand separator for 4-digit numbers. For example new Intl.NumberFormat("it").format(1234) will return *1234* instead of *1.234*. The old behavior can be achieved with the `useGrouping` parameter for the `Intl.NumberFormat` constructor.
2. In some English locales (en-AU, en-GB, and en-IN), a comma was added after full-length weekdays, for example, changing Saturday 30 April 2011 to Saturday, 30 April 2011. Web applications should avoid relying on the precise formatting of dates and they may change again in future.

- **Chrome 143 on Windows, MacOS, Linux, Android**

New policies in Chrome browser

Policy	Description
DisableScreenshots	Disable taking screenshots *(now available on Android)*
GeminiActOnWebSettings	Allows Gemini app integrations to directly act on web pages
AutoSelectCertificateForUrls	Automatically select client certificates for these sites *(now available on Android)*
CloudProfileReportingEnabled	Enable profile reporting to the admin console *(now available on iOS)*
ProvisionManagedClientCertificateForUser	Enables the provisioning of client certificates for a managed user or profile *(now available on Android)*
ProvisionManagedClientCertificateForBrowser	Enables the provisioning of client certificates for managed browsers *(now available on Android)*

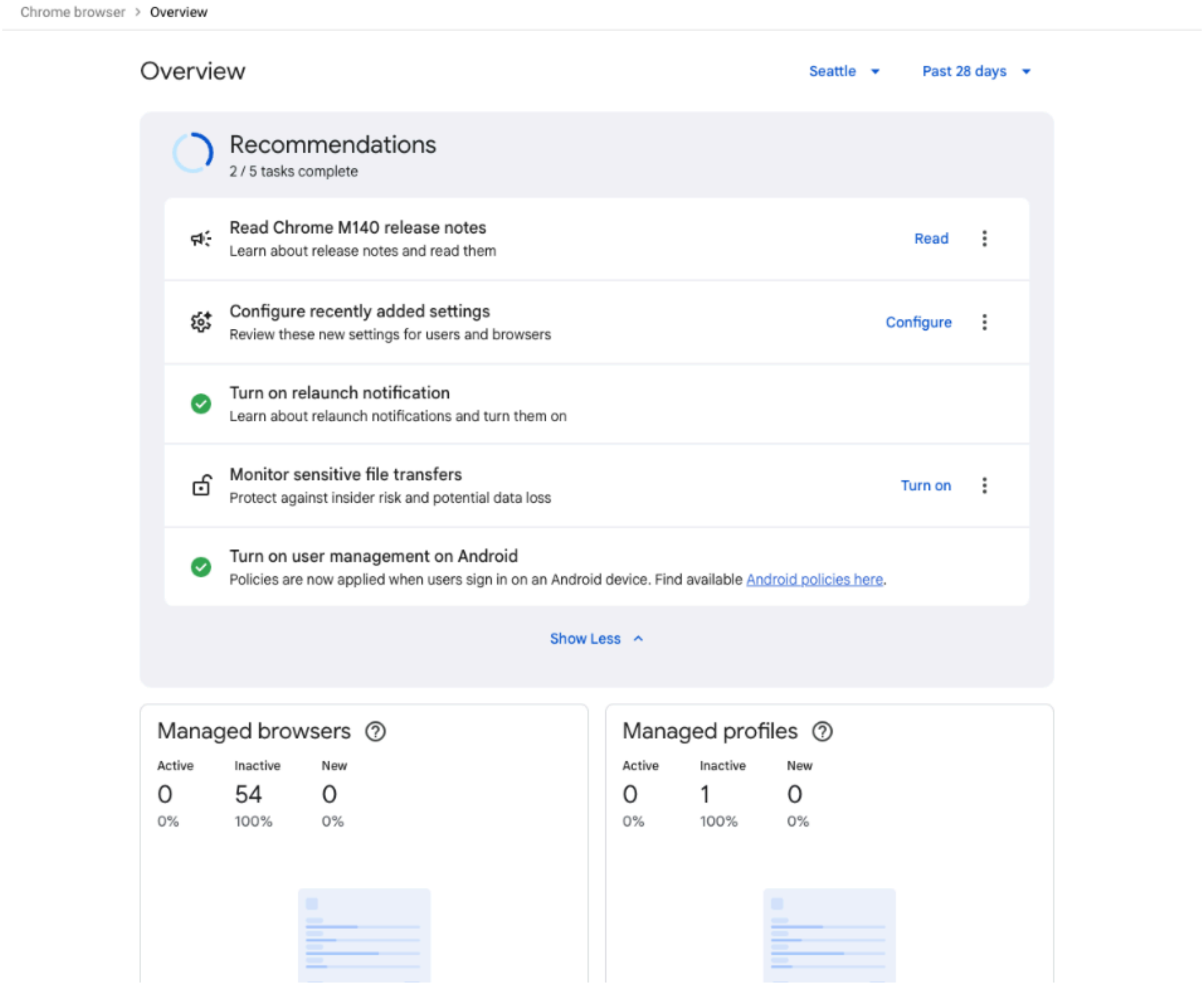
Current Chrome Enterprise Core updates

Dynamic Recommendations in the Admin console

Chrome Enterprise is launching a new dynamic recommendations list on the Overview page of the Chrome Enterprise in the Google Admin console.
This Recommendation list helps IT admins understand what to do next, get alerts on important changes, discover what's new via the release notes, configure popular settings, and more. The list dynamically changes based on admins configurations for each organization unit.

Admins can try this feature directly on the **Admin console** Chrome Overview page by navigating to **Chrome browser > Overview**.

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


Chrome browser > Overview

Overview

Seattle ▾ Past 28 days ▾

Recommendations
2 / 5 tasks complete

Read Chrome M140 release notes
Learn about release notes and read them
Read

Configure recently added settings
Review these new settings for users and browsers
Configure

✓ Turn on relaunch notification
Learn about relaunch notifications and turn them on

Monitor sensitive file transfers
Protect against insider risk and potential data loss
Turn on

✓ Turn on user management on Android
Policies are now applied when users sign in on an Android device. Find available Android policies here.

Show Less ^

Managed browsers

Active	Inactive	New
0	54	0
0%	100%	0%

Managed profiles

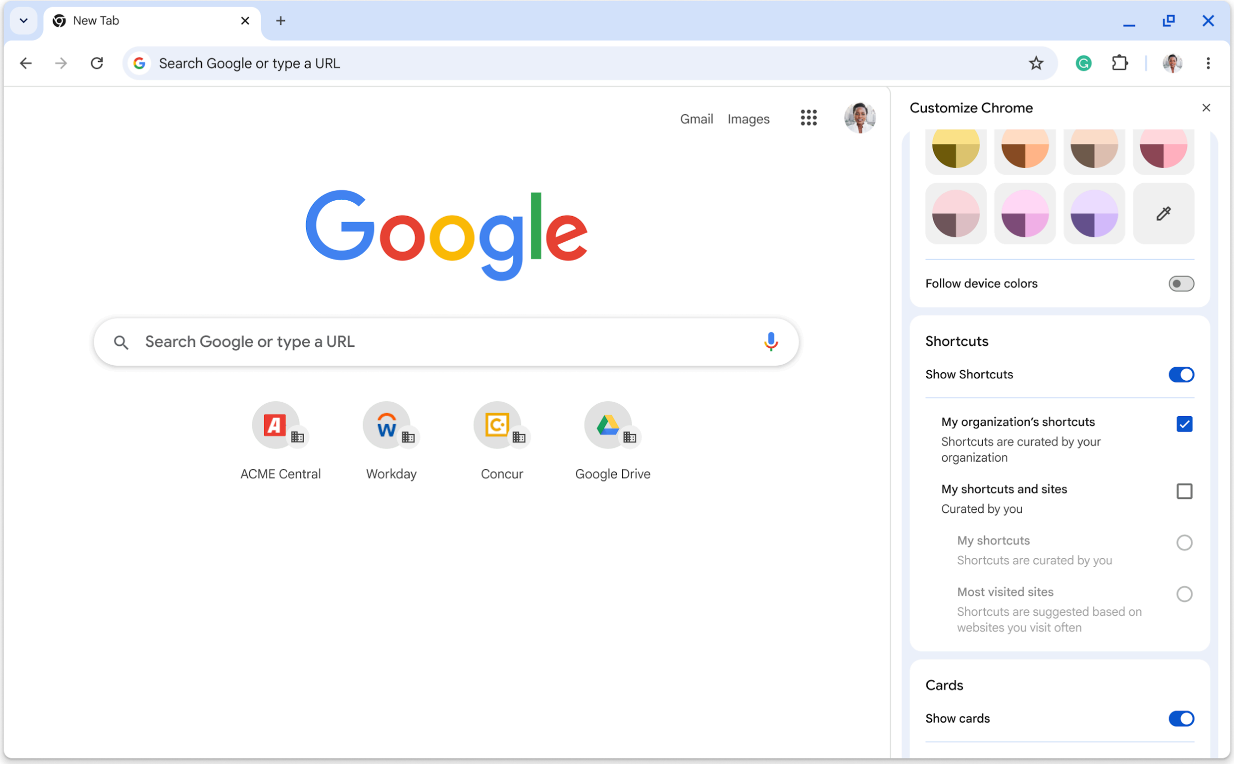
Active	Inactive	New
0	1	0
0%	100%	0%

Enterprise-managed shortcuts on the New tab page

Shortcuts on the **New tab** page can provide quick access to internal resources and applications. Admins can set up to 10 shortcuts on the user's **New tab** page using the NTPShortcuts policy.

As early as Chrome 141, this feature will be available to Chrome Enterprise Core Trusted Testers.

- Chrome 141 on ChromeOS, Linux, macOS, Windows: Early preview of policy is available for Trusted Testers. Admins can set up to 10 shortcuts and users can switch to My organizations shortcuts by navigating to **Customize Chrome**.
- **Chrome 143 on ChromeOS, Linux, macOS, Windows:** Policy will be generally available. Shortcuts set by admins will be shown in addition to user-set shortcuts (My shortcuts or Most visited sites). Users can control visibility of shortcuts by navigating to the **Customize Chrome** panel.



Customize Chrome

Follow device colors ○

Shortcuts

Show Shortcuts ●

☑ My organization's shortcuts
Shortcuts are curated by your organization

☐ My shortcuts and sites
Curated by you

○ My shortcuts
Shortcuts are curated by you

○ Most visited sites
Shortcuts are suggested based on websites you visit often

Cards

Show cards ●

Profile reporting for Chrome on iOS

Chrome Enterprise Core is launching cloud profile reporting for Chrome on iOS. To turn on profile reporting on iOS, IT administrators will need to enable the Managed profile reporting policy in the **Chrome browser > Settings** section of the Google Admin console. If you have already turned on

Managed profile reporting, you will automatically receive profile reporting on Chrome on iOS. Admins can control this feature using the CloudProfileReportingEnabled policy.
The profile reporting data can be found on the **Google Admin console > Chrome browser > Managed profiles**. The reporting information includes profile information, browser information (browser versions, OS, channel, and so on), the policies that are applied, and more.

- **Chrome 143 on iOS**: Feature would roll out gradually

Experimental cryptographic compliance policies

PreferSlowKEXAlgorithms and PreferSlowCiphers are two new, experimental enterprise policies that configure Chrome to order its preferred key agreement algorithms (supported groups) and encryption cipher algorithms, in TLS 1.3, to reflect a preference for algorithms that have been approved by a specific compliance regime. As of now, 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.

Current Chrome Enterprise Premium updates

Client certificates support on Chrome for Android

Enterprise client certificate provisioning is now available on Chrome on Android, extending the existing support already available on desktop platforms. Administrators using Chrome Enterprise Core can now deploy client certificates to both managed browsers and managed profiles on Android devices, enabling seamless authentication to enterprise resources. This integration enhances security by leveraging hardware-backed key storage, like Android Keystore and StrongBox, which makes private keys non-exportable and highly resistant to compromise.

- **Chrome 143 on Android**

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

Gemini in Chrome

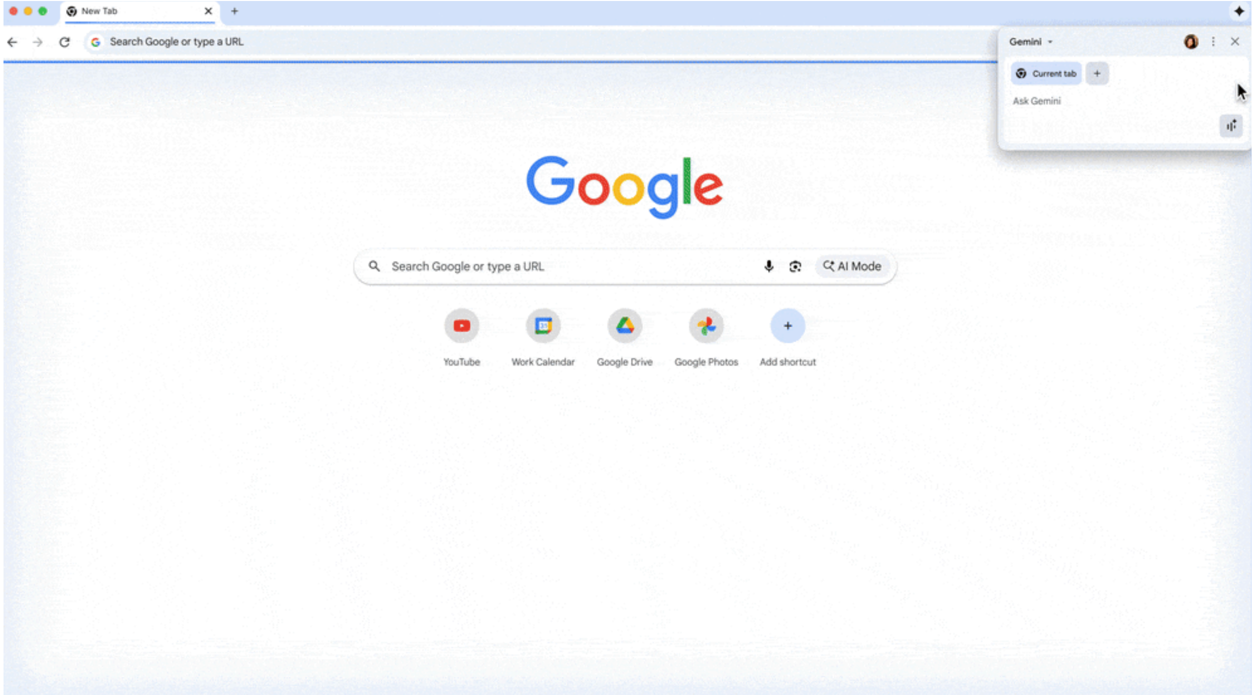
Gemini is now integrated into Chrome on macOS and Windows, and can understand the content of your current page. Users can now seamlessly get key takeaways, clarify concepts, and find answers, all without leaving their Chrome tab. This integration includes both chat—where users can interact with Gemini via text, and **Gemini Live**, with which users can interact with Gemini via voice.

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

Also coming in Chrome 143 is the multi-tab context feature. Gemini in Chrome can now see more of your opened tabs (10 max) so you can ask questions across multiple pages to help you compare or find information more efficiently. Gemini in Chrome also serves as a productivity agent by enabling YouTube, Maps, Gmail, Drive, Keep, Calendar, and Tasks tools.

- 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.
- **As early as Chrome 144 on macOS, Windows:**
    - Agentic capabilities in Gemini in Chrome available to some users (non-enterprise). An enterprise policy, GeminiActOnWebSettings, will be available at launch and can be set using custom configurations. Non-enterprise users will also 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.

    - Image upload context menu item available to enterprise users. This feature will respect rules set via the DataControlsRules policy and the OnBulkDataEntryEnterpriseConnector settings.
- As early as Chrome 148 on macOS, Windows: Agentic capabilities in Gemini in Chrome available to enterprise users.



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 144 on ChromeOS, Linux, macOS, Windows**

Deprecating savedTabGroups as individual value in SyncTypesListDisabled

Currently, the SyncTypesListDisabled enterprise policy allows administrators to disable the synchronization of savedTabGroups datatype on desktop platforms. On mobile platforms, however, Tab Groups synchronization is already managed by the tabs datatype. To align desktop behavior with mobile and simplify sync management, the individual savedTabGroups datatype will be deprecated and will no longer be an individually customizable value within the SyncTypesListDisabled policy.
Action required by administrators:

> Starting with Chrome 144, if your SyncTypesListDisabled policy disables either tabs or `savedTabGroups`, both data types will now be considered disabled. This means that disabling tabs will also disable saved tab groups, and vice-versa. The `savedTabGroups` value will be entirely removed from the list of supported datatypes for this policy. Administrators who have saved tab groups disabled and intend to keep this behavior must explicitly disable the tabs datatype. This will ensure the desired behavior before the `savedTabGroups` value is fully removed.

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

Happy Eyeballs V3

This launch is an internal optimization in Chrome that implements Happy Eyeballs V3 to achieve better network connection concurrency. Happy Eyeballs V3 performs DNS resolutions asynchronously and staggers connection attempts with preferable protocols (H3/H2/H1) and address families (IPv6 or IPv4) to reduce user-visible network connection delay. This feature is gated by a temporary policy HappyEyeballsV3Enabled.

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

Multicast support for Direct Sockets API

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

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

On-device scam detection on Android

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

- **Chrome 144 on Android**

ServiceWorkerAutoPreload mode

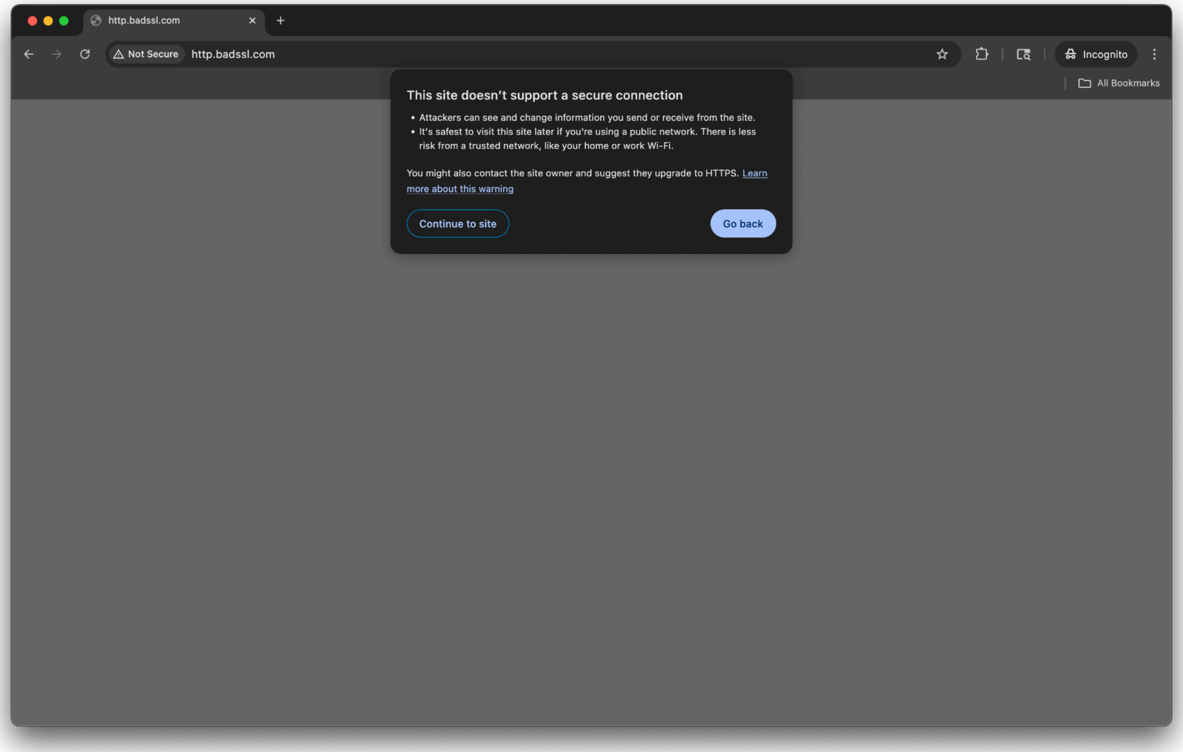
ServiceWorkerAutoPreload is a mode where the browser issues the network request in parallel with the service worker bootstrap, and consumes the network request result inside the fetch handler if the fetch handler returns the response with respondWith(). If the fetch handler result is fallback, it passes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

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

Update to *No HTTPS* warning

Chrome 140 updated the warning displayed when a user opts in to the **Always use secure connections** on chrome://settings/security from an interstitial to a dialog. The URL content security indicator on the warning changes from an asterisk to a broken lock, while the full page load remains blocked and the functionality remains unchanged. Some users might see this warning automatically when visiting HTTP sites. Users can opt in to the warning on chrome://settings/security.

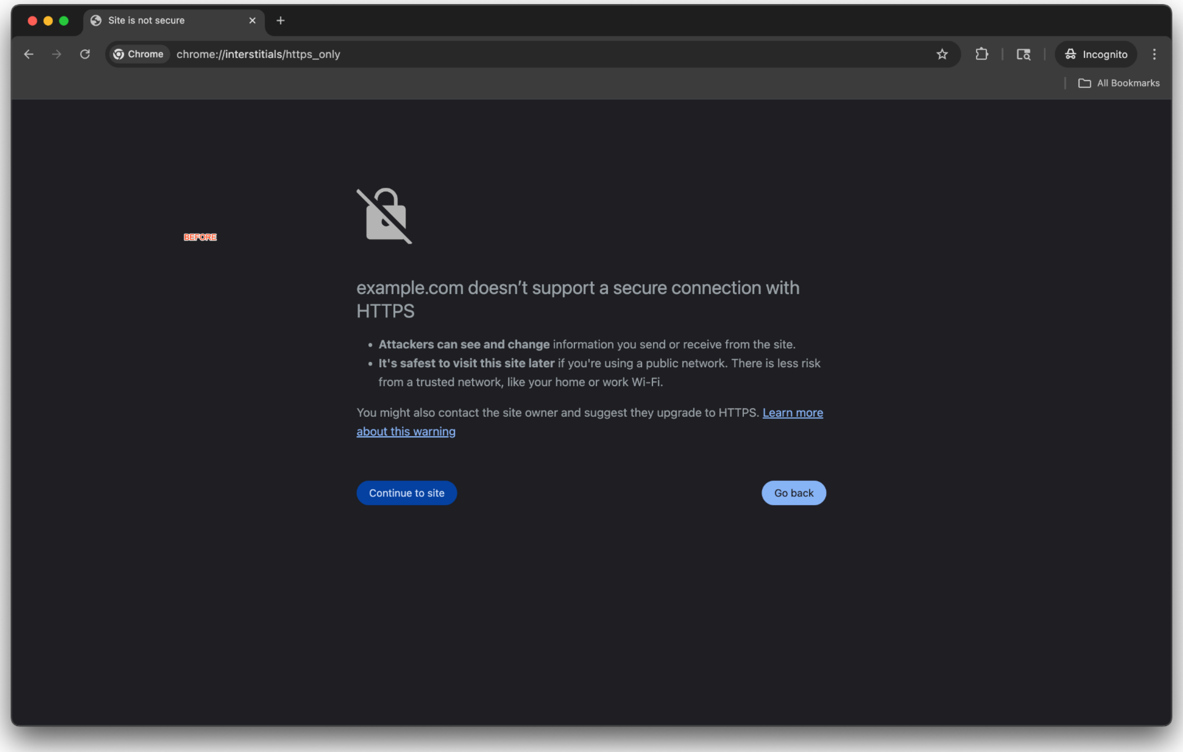
- Chrome 141 on ChromeOS, Linux, macOS, Windows: New warning design on desktop platforms
- **Chrome 143 on Android:** New warning design on Android



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

2SV enforcement for admins

To better protect your organization’s information, Google will soon require all accounts with access to `admin.google.com` to have 2-Step Verification (2SV) enabled. As a Google Workspace administrator, you need to confirm your identity with 2SV, which requires your password plus something additional, such as your phone or a security key.

The enforcement will be rolled out gradually over the coming months. You should enable 2SV for the admin accounts in your organization before Google enforces it. For more information, see this About 2SV enforcement for admins.

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

CSS find-in-page highlight pseudos

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

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

Change in launch schedule starting in Chrome *Early Stable* 145

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

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

Disable force-installed extensions with non-malware violations

This feature silently will disable force-installed extensions exhibiting violations of Chrome Web Store policies (CWS) 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 switch these extensions on or off, but will not be able to remove them.

A new enterprise policy, ExtensionForceInstallWithNonMalwareViolationEnabled, will be added in 142 to preserve the existing behavior for unmanaged browser environments, but will be removed in 145.

This change does not affect managed instances of Chrome that are joined to a Microsoft Active Directory domain, joined to Microsoft Azure Active Directory or enrolled in Chrome Enterprise Core. On macOS, this change does not affect instances of Chrome that are managed via MDM, joined to a domain or enrolled in Chrome Enterprise Core.

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

Origin-Bound cookies (by default)

In Chrome 145, cookies will be bound to their setting origin (by default) such that they're only accessible by that origin, that is, 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** are available to revert this change. These policies will stop working in Chrome 150.

- **Chrome 145 on Android, iOS, Linux, macOS, Windows**: Enterprise policies will be available
- Chrome 150 on Android, iOS, Linux, macOS, Windows: Enterprise policies would be removed

Remove third-party storage partitioning policies

Third-party storage partitioning became the default in Chrome 115. The `chrome://` flag that allowed users to disable this feature was removed in Chrome 128, and the deprecation trial ended with Chrome 139.
In Chrome 145, 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 in the Chromium bug.

- **Chrome 145 on Android, ChromeOS, Linux, macOS, Windows, Fuchsia:** Removal of DefaultThirdPartyStoragePartitioningSetting and ThirdPartyStoragePartitioningBlockedForOrigins

X25519Kyber768 key encapsulation for TLS

Chrome 124 enabled by default on all desktop platforms a new post-quantum secure TLS key encapsulation mechanism X25519Kyber768, based on a NIST standard (ML-KEM). This protects network traffic from Chrome with servers that also support ML-KEM from decryption by a future quantum computer. This change should be transparent to server operators. This cipher will be used for both TLS 1.3 and QUIC connections.
However, some TLS middleboxes might be unprepared for the size of a Kyber (ML-KEM) key encapsulation, or a new TLS ClientHello cipher code point, leading to dropped or hanging connections. This can be resolved by updating your middlebox, or disabling the key encapsulation mechanism via the temporary PostQuantumKeyAgreementEnabled enterprise policy, which will be available through the end of 2024. However, long term, post-quantum secure ciphers will be required in TLS and the enterprise policy will be removed. Post-quantum cryptography is required for CSNA 2.0. To learn more, see Protect Chrome Traffic with Hybrid 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:** Enterprise policy PostQuantumKeyAgreementEnabled 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 (Github).

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

UI Automation accessibility framework provider on Windows

Starting in Chrome 126, Chrome will start directly supporting accessibility client software that uses Microsoft Windows's UI Automation accessibility framework. Prior to this change, such software interoperated with Chrome by way of a compatibility shim in Microsoft Windows. This change is being made to improve the accessible user experience for many users. It provides complete support for Narrator, Magnifier, and Voice Access; and will improve third-party apps that use Windows's UI Automation accessibility framework. Users of Chrome will find reduced memory usage and processing overhead when used with accessibility tools. It will also ease development of software using assistive technologies.

Administrators 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 may fix any incompatibilities resulting from the switch from Microsoft's compatibility shim to Chrome's UI Automation provider.

- Chrome 125 on Windows: The UiAutomationProviderEnabled policy is introduced so that administrators can enable Chrome's UI Automation accessibility framework provider and validate that third-party accessibility tools continue to work.
- Chrome 126 on Windows: The Chrome variations framework will be used to begin enabling Chrome's UI Automation accessibility framework provider for users. It will be progressively enabled to the full stable population, with pauses as needed to address compatibility issues that can be resolved in Chrome. Enterprise administrators may continue to use the UiAutomationProviderEnabled policy to either opt-in early to the new behavior, or to temporarily opt-out through Chrome 146.

- **Chrome 147 on Windows:** The UiAutomationProviderEnabled policy will be removed from Chrome. All clients will use the browser's UI Automation accessibility framework provider.

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 148 on Android, iOS, ChromeOS, Linux, macOS, Windows:** Feature would gradually roll-out

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.
In the initial release, 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.

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
- **Chrome 152 on Android, ChromeOS, Linux, macOS, Windows, Fuchsia**: Remove Enterprise Policy

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 address, or from a local website (for example, an 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 permission 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 152 on Android, ChromeOS, Linux, MacOS, Windows:** LocalNetworkAccessRestrictionsTemporaryOptOut will be removed

Upcoming Chrome Enterprise Core updates

There are no Upcoming Chrome Enterprise Core updates.

Upcoming Chrome Enterprise Premium updates

Copy and Paste rules protection

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

- Chrome 140 on Android: Copy/Paste Rules Protection becomes available on Android
- **Chrome 144 on iOS:** Copy/Paste Rules Protection becomes available on Android

Proxy Override rules

To simplify proxy management in complex enterprise environments, Chrome 144 will introduce two new policies: **ProxyOverrideRules** and **EnableProxyOverrideRulesForAllUsers**. Currently, organizations that use multiple proxy solutions (for example, a general proxy and a specific one for Google's Secure Gateway) or have different admin teams (for example, for GPO and the Google Admin console) must manually merge complex PAC files. This process is error-prone and creates significant administrative friction.
The new **ProxyOverrideRules** policy allows administrators to configure a list of routing rules that are evaluated before any existing proxy configuration, including PAC files set by the ProxySettings policy. This enables admins to easily prepend specific routes (for example, to send traffic for private web apps to a secure gateway) without modifying the primary, company-wide PAC script. The **EnableProxyOverrideRulesForAllUsers** policy provides additional control over how these override rules apply to unaffiliated users on a device. End users will see a notification in their `chrome://settings` page to inform them when these administrative proxy rules are active.

- **Chrome 144 on ChromeOS, Linux, MacOS, Windows**
  Proxy Override Rules becomes available on Windows, MacOS, ChromeOS and Linux

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 will close 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 the 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 145 on Linux, macOS, Windows:** This stage enables the collection of large (>50 MB) and encrypted files for the Evidence Locker, closing a key DLP 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.