chrome enterprise

Chrome 135 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 March 26, 2025.

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

Chrome 135 release summary

Current Chrome browser updates	Security / Privacy	User productivity / Apps	Management
3P profile enrollment migrates to OIDC auth code flow	✓		
Auto-deletion of downloads for Chrome on iOS	✓		
Better password form detection with ML	✓		
Client's LLM assistance in mitigating scams	✓		
Deprecate mutation events	✓		
Download file type extension-based warnings - documentation correction	✓		
Extensions improvements on Chrome Desktop	✓	✓	
Generic Device Trust Connector	✓		
Remove Private Network Access enterprise policies	✓		
Remove ThirdPartyBlockingEnabled policy	✓		
Settings, site shortcuts, and themes improvements on Chrome Desktop	✓		
Sunsetting the legacy Password Manager in Chrome on Android	✓		
Third-party cookies always blocked in Incognito mode	✓		

Create service worker client and inherit service worker controller for srcdoc iframe	✓		
HSTS tracking prevention	✓		
Remove deprecated navigator.xr.supportsSession method	✓		
New policies in Chrome browser			✓
Removed policies in Chrome browser			✓
Chrome Enterprise Core	**Security / Privacy**	**User productivity / Apps**	**Management**
Extensible SSO support for Chrome on macOS		✓	✓
Chrome Enterprise Premium	**Security / Privacy**	**User productivity / Apps**	**Management**
No updates in Chrome 135			
Upcoming Chrome browser updates	**Security / Privacy**	**User productivity / Apps**	**Management**
Remote debugging port custom data directory requirement	✓		
Blob URL Partitioning: Fetching/Navigation	✓		
Deprecate getters of Intl Locale Info API	✓		
FedCM updates			✓
Partitioning :visited links history	✓		
Strict Same Origin Policy for Storage Access API	✓		
Remove SwiftShader fallback	✓		
Disallow spaces in non-file:// URL host	✓		
Isolated Web Apps	✓		
SafeBrowsing API v4 to v5 migration	✓		

UI Automation accessibility framework provider on Windows		✓	
Upcoming Chrome Enterprise Core updates	**Security / Privacy**	**User productivity / Apps**	**Management**
Improved Admin console reporting performance and scalability			✓
New remote commands and CSV export for the Managed Profile List			✓
New Overview landing page for Chrome Enterprise Core			✓
IP Address logging and reporting	✓		
Inactive profile deletion in Chrome Enterprise Core	✓		✓
Upcoming Chrome Enterprise Premium updates	**Security / Privacy**	**User productivity / Apps**	**Management**
URL filtering on iOS and Android	✓		
Refactor DLP rules user experience	✓		
Reporting connector for mobile	✓		
Connectors API	✓		

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

3P profile enrollment migrates to OIDC auth code flow

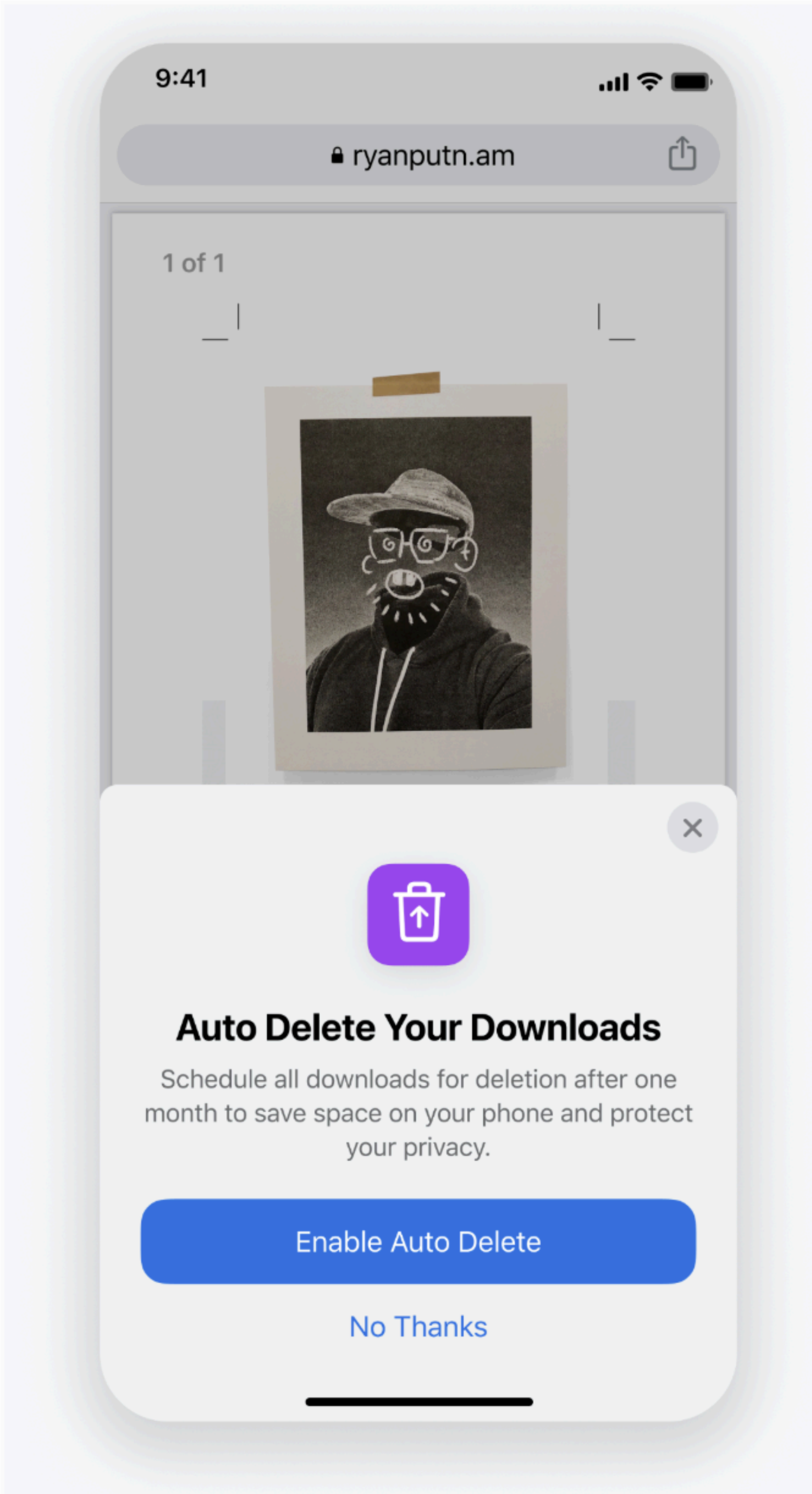
Chrome 135 migrates the landing page for profile registration from the marketing website to a dynamic website. This update also migrates the OpenID Connect (OIDC) implicit flow to an auth code flow. This aims to improve both the security and the user experience for third party (3P) managed profiles.

- **Chrome 135 on Windows**

Auto-deletion of downloads for Chrome on iOS

Users of Chrome browser on iOS can now choose to automatically delete their browser downloads on a scheduled basis.
This feature is likely to both improve device performance related to storage capacity, and to improve privacy by automating the deletion of files that users might otherwise forget to on their own.

- **Chrome 135 on iOS**
  Initial experiment at 1% in 135 for Chrome for iOS only. No planned rollout for other platforms.



Auto Delete Your Downloads

Schedule all downloads for deletion after one month to save space on your phone and protect your privacy.

Better password form detection with ML

Chrome 135 introduces a new client-side Machine Learning (ML) model to better parse password forms on the web to increase detection and filling accuracy. You can control this feature using the PasswordManagerEnabled policy.

- **Chrome 135 on Android, iOS, ChromeOS, Linux, macOS, Windows**

Client's LLM assistance in mitigating scams

Users on the web are facing significant amounts and varieties of scams on a daily basis. To combat these scams, Chrome 135 uses on-device Large Language Models (LLMs) to identify scam websites for **Enhanced protection** users. Chrome sends the page content to an on-device LLM to infer security-related signals for that page.Chrome then sends these signals to Safe Browsing server side for a final verdict. When turned on, Chrome might consume more bandwidth to download the LLM.

- Chrome 134 on Linux, macOS, Windows
  Gather the brand name and intent summary of the page that requested keyboard lock API to identify scam websites.
- **Chrome 135 on Linux, macOS, Windows**
  Show the warnings to the user based on the server verdict which uses the brand and intent summary of the page that requested keyboard lock API.

Deprecate mutation events

Synchronous mutation events, including DOMSubtreeModified, DOMNodeInserted, DOMNodeRemoved, DOMNodeRemovedFromDocument, DOMNodeInsertedIntoDocument, and DOMCharacterDataModified, negatively affect page performance, and also significantly increase the complexity of adding new features to the Web. These APIs were deprecated from the spec in 2011, and were replaced (in 2012) by the much better-behaved Mutation Observer API. Usage of the obsolete mutation events must be removed or migrated to Mutation Observer.
Since Chrome 124, a temporary enterprise policy, MutationEventsEnabled, is available to re-enable deprecated or removed mutation events. To read more, see this Chrome for Developers blog post. If you encounter any issues, you can file a Chromium bug.

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

- The Mutation Events Deprecation Trial can be used to re-enable the feature for a limited time on a given site. This can be used up until Chrome 135, ending March 25, 2025.
- A MutationEventsEnabled enterprise policy can also be used for the same purpose, also through Chrome 135.
- **Chrome 135 on Android, Linux, macOS, Windows:** The MutationEventsEnabled enterprise policy will be deprecated.

Download file type extension-based warnings - documentation correction

We've updated the policy documentation for ExemptDomainFileTypePairsFromFileTypeDownloadWarnings to correctly reflect its interaction with the DownloadRestrictions policy. The behavior in Chrome has not changed.
The behavior is: ExemptDomainFileTypePairsFromFileTypeDownloadWarnings can specify exemptions that override DownloadRestrictions settings for blocking dangerous file types. Other types of security measures specified by DownloadRestrictions, such as blocking malicious downloads, cannot be overridden by ExemptDomainFileTypePairsFromFileTypeDownloadWarnings.

- **Chrome 135 on ChromeOS, Linux, macOS, Windows**
  No Chrome changes - documentation change only.

Extensions improvements on Chrome Desktop

On Chrome 135 on Desktop, some users who sign in to Chrome when installing a new extension can now use and save extensions in their Google Account.
Relevant enterprise policies controlling extensions, as well as BrowserSignin, SyncDisabled or SyncTypesListDisabled, continue to work as before, so admins can configure whether users can use and save items in their Google Account.
For more information about how to use extensions on any computer, see Install and manage extensions in the Chrome Web Store Help Center.

Note: This change is a follow-up to the launch of the new identity model on Chrome Desktop. For more details, see Sign in and sync in Chrome.

- **Chrome 135 on Linux, macOS, Windows**

Generic Device Trust Connector

Integrations created through the Device Trust Connector allow customers to implement granular controls for authentication into enterprise resources, for example, SaaS apps or your corporation intranet, based on the properties of the end user's device and browser instance sent by Chrome. For more details, see Manage Chrome Enterprise device trust connectors.

- **Chrome 135 on Windows**

Remove Private Network Access enterprise policies

Private Network Access (PNA 1.0) is an unshipped security feature designed to limit website access to local networks. Due to deployability concerns, PNA 1.0 was never able to ship by default, as it was incompatible with too many existing devices.

PNA 1.0 required changes to devices on local networks. Instead, Chrome is implementing an updated proposal, Private Network Access 2.0 (PNA 2.0). PNA 2.0 only requires changes to sites that need to access the local network, rather than requiring changes to devices on the local network. Sites are much easier to update than devices, and so this approach should be much more straightforward to roll out.

The only way to enforce PNA 1.0 is via enterprise policy. To avoid regressing security for enterprise customers opting-in to PNA 1.0 prior to shipping PNA 2.0, we will maintain the PrivateNetworkAccessRestrictionsEnabled policy, which causes Chrome to send special preflight messages, until such time that it becomes incompatible with PNA 2.0.

Chrome 135 removes the InsecurePrivateNetworkRequestsAllowedForUrls and InsecurePrivateNetworkRequestsAllowed policies, which loosen PNA 1.0 restrictions. These policies currently have no effect, since PNA 1.0 is not shipped, and they will have no meaning once PNA 1.0 is removed.

PNA 2.0 is described in this explainer on GitHub.

- **Chrome 135 on Android, ChromeOS, Linux, macOS, Windows, Fuchsia**
  Removal of InsecurePrivateNetworkRequestsAllowedForUrls and InsecurePrivateNetworkRequestsAllowed policies.
- Chrome 137 on Android, ChromeOS, Linux, macOS, Windows, Fuchsia
  Removal of PrivateNetworkAccessRestrictionsEnabled.

Remove ThirdPartyBlockingEnabled policy

Due to unexpected issues, we plan to remove the ThirdPartyBlockingEnabled policy in Chrome 135. If you have feedback about this removal, you can file a Chromium bug.

- Chrome 132 on Windows
  Deprecation of ThirdPartyBlockingEnabled policy
- **Chrome 135 on Windows**
  Removal of ThirdPartyBlockingEnabled policy

Settings, site shortcuts, and themes improvements on Chrome Desktop

On Chrome 135 on Desktop, for users who newly sign in to Chrome or who have Sync enabled, settings, site shortcuts and themes synced to their Google Account will now be kept separate from the local ones, that is, settings from when they're signed out or when Sync is turned off.
This allows for strictly less data sharing than previously: local settings don't get automatically uploaded when signing in or turning on Sync, and no settings from the account are left behind on the device when Sync is turned off.
Existing enterprise policies SyncDisabled and SyncTypesListDisabled will continue to apply so admins can restrict or disable the Sync feature if they want to. For more details, see Manage who can sync browser settings.
Note: This change is a follow-up to the launch of the new identity model on Chrome Desktop. For more details, see Chrome Platform Status.

- **Chrome 135 on Linux, macOS, Windows**

Sunsetting the legacy Password Manager in Chrome on Android

Users with old versions of Google Play Services will lose Password Manager functionality in Chrome. This is a step towards sunsetting the legacy Password Manager in Chrome on Android. These users can download a CSV file with their passwords from Chrome Settings and import it to their preferred Password Manager. The new Google Password Manager is available on devices with a recent version of Google Play Services.

- **Chrome 135 on Android**

Third-party cookies always blocked in Incognito mode

Starting in Chrome 135, users have third-party cookies blocked in Incognito mode with no way to globally re-enable them. Site-level controls for allowing third-party cookies will not be changed. With this launch, the BlockThirdPartyCookies policy applies to regular mode only when set to false, not Incognito mode. There are no changes when the policy is true or unset. There are also no changes to the CookieAllowedForUrls policy, which continues to apply in both regular and Incognito modes, as it applies at the site level and not globally.

- **Chrome 135 on Android, ChromeOS, Linux, macOS, Windows**

Create service worker client and inherit service worker controller for srcdoc iframe

Srcdoc context documents were previously not service worker clients and were not covered by their parent page's service worker. This resulted in some discrepancies (for example, Resource Timing reports the URLs that these documents load, but the service worker doesn't intercept them).
To fix these discrepancies, Chrome 135 creates service worker clients for `srcdoc` iframes and makes them inherit the parent page's service worker controller.

- **Chrome 135 on Windows, macOS, Linux, Android**

HSTS tracking prevention

HTTP Strict Transport Security (HSTS) allows sites to declare themselves accessible through secure connections only.
In Chrome 135, HSTS tracking prevention mitigates user tracking by third-parties using the HSTS cache. It only allows HSTS upgrades for top-level navigations and blocks HSTS upgrades for sub-resource requests. This prevents third-party sites using the HSTS cache to track users across the web. For more information, see this HSTS Tracking Prevention explainer on Github.

- **Chrome 135 on Windows, macOS, Linux, Android**

Remove deprecated navigator.xr.supportsSession method

Chrome 135 removes the `navigator.xr.supportsSession` method, which was replaced in the WebXR spec by the `navigator.xr.isSessionSupported` method in September of 2019 after receiving feedback on the API shape from the TAG. It has been marked as deprecated in Chromium since then, producing a console warning redirecting developers to the updated API.
Usage of the call is very low, as shown by Chrome Status usage metrics. Additionally, all major frameworks that are used to build WebXR content have been confirmed to have been updated to use the newer call.

- **Chrome 135 on Windows, macOS, Linux, Android**

New policies in Chrome browser

Policy	Description
DownloadRestrictions	Blocks malicious downloads and dangerous file types
PartitionedBlobUrlUsage	Choose whether Blob URLs are partitioned during fetching and navigations
ExtensibleEnterpriseSSOBlocklist	Blocklist of identity providers that cannot use Extensible Enterprise SSO for the browser
EnterpriseSearchAggregatorSettings	Enterprise search aggregator settings (Beta)
ProfilePickerOnStartupAvailability	Profile picker availability on startup

Removed policies in Chrome browser

Policy	Description
ThirdPartyBlockingEnabled	Enable third party software injection blocking
KeyboardFocusableScrollersEnabled	Enable keyboard focusable scrollers

Current Chrome Enterprise Core updates

Extensible SSO support for Chrome on macOS

Chrome 135 on macOS enables seamless authentication for identity providers that are enabled via an OS-configured Enterprise Single Sign On (SSO) extension. For this initial release, Chrome allows end users on managed browsers to sign in to any Microsoft Entra-authenticated resources without the need to enter any credentials. Extensible SSO needs to be pre-configured in your environment and deployed with its respective enterprise device management solution.

- **As early as Chrome 135 on macOS**

Current Chrome Enterprise Premium updates

No updates for Chrome Enterprise Premium in Chrome 135.

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

Remote debugging port custom data directory requirement

Remote debugging via a TCP port or a pipe will no longer be possible in Google Chrome with the default data directory on Windows, Linux and macOS.
A custom data directory must be specified to remotely debug Google Chrome using the `--user-data-dir` switch, when using the `--remote-debugging-pipe` or `--remote-debugging-port` switches.
The motivation for this change is because these remote debugging switches are being abused by infostealers and malware to extract data from Google Chrome. A custom user data directory uses a different encryption key and so it becomes no longer possible for malware to steal encrypted data such as cookies.
This change does not affect Chrome for Testing and Chromium.

- **Chrome 136 on Linux, macOS, Windows**

Blob URL Partitioning: Fetching/Navigation

As a continuation of Storage Partitioning, Chromium will implement partitioning of Blob URL access by Storage Key (top-level site, frame origin, and the has-cross-site-ancestor boolean), with the exception of top-level navigations which will remain partitioned only by frame origin. This behavior is similar to what's currently implemented by both Firefox and Safari, and aligns Blob URL usage with the partitioning scheme used by other storage APIs as part of Storage Partitioning. In addition, Chromium will enforce noopener on renderer-initiated top-level navigations to Blob URLs where the corresponding site is cross-site to the top-level site performing the navigation. This aligns Chromium with similar behavior in Safari, and the relevant specs have been updated to reflect these changes.

This change can be temporarily reverted by setting the PartitionedBlobURLUsage policy. The policy will be deprecated when the other storage partitioning related enterprise policies are deprecated.

- **Chrome 136 on Windows, macOS, Linux, Android**

Deprecate getters of Intl Locale Info API

Intl Locale Info API is a Stage 3 ECMAScript TC39 proposal to enhance the `Intl.Locale` object by exposing locale information, such as week data (first day in a week, weekend start day, weekend end day, minimum day in the first week), and text direction hour cycle used in the locale.
We shipped our implementation in Chrome 99 but later on the proposal made some changes in Stage 3 and moved several getters to functions. We plan to remove the deprecated getters and relaunch the renamed functions.

- **Chrome 136 on Windows, macOS, Linux, Android**

FedCM updates

As early as Chrome 136, Federated Credential Management API (FedCM) will be able to show multiple identity providers in the same dialog. This will provide developers with a convenient way to present all supported identity providers to users. We are planning to first tackle the simple case of having all providers in the same get() call.
We plan to remove support for adding another account in FedCM passive mode. This feature allows showing a **Use another account** button alongside other IdP accounts in the chooser. The feature is currently unused, and UX conversations indicate that supporting this leads to a more complicated flow without much benefit. This feature will still work in FedCM active mode.

- **Chrome 136 on Windows, macOS, Linux, Android**

Partitioning :visited links history

To eliminate user browsing history leaks, anchor elements are styled as `:visited` only if they have been clicked from this top-level site and frame origin before. On the browser-side, this means that the VisitedLinks hashtable is now partitioned by triple-keying, or by storing the following for each visited link: `<link URL, top-level site, frame origin>`. By only styling links that have been clicked on this site and frame before, the many side-channel attacks that have been developed to obtain `:visited` links styling information are now obsolete, as they no longer provide sites with new information about users.

There is an exception for *self-links*, where links to a site's own pages can be styled as `:visited` even if they have not been clicked on in this exact top-level site and frame origin before. This exemption is only enabled in top-level frames or subframes, which are same-origin with the top-level frame. The privacy benefits above are still achieved because sites already know which of its subpages a user has visited, so no new information is exposed. This was a community-requested exception that improves user experience as well.

- **Chrome 136 on Windows, macOS, Linux, Android**

Strict Same Origin Policy for Storage Access API

Chrome 136 will adjust Storage Access API semantics to strictly follow the Same Origin policy, to enhance security. This means that using `document.requestStorageAccess()` in a frame will only attach cookies to requests to the iframe's origin (not site) by default.

Note: the CookiesAllowedForUrls policy or Storage Access headers can still be used to unblock cross-site cookies.

- **Chrome 136 on Windows, macOS, Linux, Android**

Remove SwiftShader fallback

As early as Chrome 137, we plan to deprecate automatic fallback to WebGL backed by SwiftShader. WebGL context creation will fail instead of falling back to SwiftShader. We plan to remove SwiftShader fallback for two primary reasons:

1. SwiftShader is a high security risk due to JIT-ed code running in Chromium's GPU process.
2. Users have a poor experience when falling back from a high-performance GPU-backed WebGL to a CPU-backed implementation. Users have no control over this behavior and it is difficult to describe in bug reports.

SwiftShader is a useful tool for web developers to test their sites on systems that are headless or do not have a supported GPU. This use case will still be supported by opting in but is not intended for running untrusted content.

To opt-in to lower security guarantees and allow SwiftShader for WebGL, run the chrome executable with the `--enable-unsafe-swiftshader` command-line switch.

During the deprecation period, a warning will appear in the JavaScript console when a WebGL context is created and backed with SwiftShader. Passing `--enable-unsafe-swiftshader` will remove this warning message.

Chromium and other browsers do not guarantee WebGL availability. You can test and handle WebGL context creation failure and fall back to other web APIs such as Canvas2D or an appropriate message to the user.

- **Chrome 137 on Windows, macOS, Linux, Android**

Disallow spaces in non-file:// URL host

As stated in the WhatWG.org spec, 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.

To read more, see the discussion on Github.

This feature will be part of the ongoing work to bring Chromium closer to spec compliance by forbidding spaces in non-file URLs only.

- **Chrome 138 on Android, ChromeOS, Linux, macOS, Windows, Fuchsia**

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, which 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 Getting started with Isolated Web Apps.
In the initial release, IWAs will only be installable through a policy on enterprise-managed ChromeOS devices.

- **Chrome 140 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.

- **Chrome 145 on Android, iOS, ChromeOS, Linux, macOS, Windows**
  This will be a gradual roll-out.

UI Automation accessibility framework provider on Windows

Starting in Chrome 126, Chrome started 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.

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

- Chrome 125 on Windows:The UiAutomationProviderEnabled policy is introduced so that admins 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 population, with pauses as needed to address compatibility issues that can be resolved in Chrome. Enterprise admins may continue to use the UiAutomationProviderEnabled policy to either opt-in early to the new behavior, or to temporarily opt-out through Chrome 136.
- **Chrome 147 on Windows:** The UiAutomationProviderEnabled policy will be removed from Chrome. All clients will use the browser's UI Automation accessibility framework provider.

Upcoming Chrome Enterprise Core updates

Improved Admin console reporting performance and scalability for large customers

Chrome Enterprise Core will roll out software infrastructure changes that aim to improve the performance, accuracy and scalability of many pages and reports in the Admin console. The pages and reports impacted in the Admin console include (but are not limited to):

- Versions report
- Apps & Extension Usage report
- Extension Details page
- Chrome Insights page for browsers

The changes are planned to gradually roll out between April and July 2025.

- **As early as April 2025, until July 2025**

New remote commands and CSV export for the Managed Profile List

We plan to add a **CSV export** action and **Clear cache** and **Clear cookies** remote commands on the Managed profile list. You will be able to select one or multiple profiles and perform a remote command.

- **CSV Export: As early as Chrome 135 on Android, Linux, macOS, Windows**
- Remote Commands: As early as Chrome 136 on Linux, macOS, Windows

New Overview landing page for Chrome Enterprise Core

This new overview page will be located in the Chrome browser section of the Admin console and it will display insightful information about your deployment, such as a summary of your browser and profiles deployment, a summary of Chrome versions reported and extensions installed. For example, those insights will allow you to quickly identify inactive browsers and browsers with a pending update. You will also be able to quickly see your queue of extension requests and review extensions that have been configured.

- **As early as Chrome 135 for early Trusted Testers access**

IP Address logging and reporting

Chrome Enterprise is enhancing its security monitoring and incident response capabilities by collecting and reporting local and remote IP addresses and sending those IP addresses to the Security Investigation Logs (SIT). In addition, Chrome Enterprise will allow admins to optionally send the IP addresses to both in-house and third-party Security and Information Event Management (SIEM) providers via the Chrome Enterprise Reporting connector.
This will be available for Chrome Enterprise Core customers.

- **Chrome 136 on Windows, macOS, Linux**

Inactive profile deletion in Chrome Enterprise Core

In April 2025 (Chrome 136), the inactive period for profile deletion policy will start rolling out. In June 2025 (Chrome 138), the policy will begin to automatically delete managed profiles in the Admin console that have been inactive for more than the defined inactivity period. When releasing the policy, the inactivity period of time has a default value of 90 days. Meaning that by default, all managed profiles that have been inactive for more than 90 days are deleted from your account. Administrators can change the inactive period value using this policy. The maximum value to determine the profile inactivity period is 730 days and the minimum value is 28 days.
If you lower the set policy value, it might have a global impact on any currently managed profiles. All impacted profiles will be considered inactive and, therefore, be deleted. This does not delete the user account. If an inactive profile is re-activated on a device, that profile will reappear in the console.

- **Chrome 138 on Android, ChromeOS, Linux, macOS, Windows**
  Policy will roll out in April (Chrome 136). Deletion will start in June (Chrome 138) and the initial wave of deletion will complete by the end of July (Chrome 139). After the initial deletion rollout, inactive profiles will continue to be deleted once they have reached their inactivity period.

Upcoming Chrome Enterprise Premium updates

URL filtering on iOS and Android

We will extend the existing URL filtering capabilities from desktop to mobile platforms, providing organizations with the ability to audit, warn, or block certain URLs or categories of URLs from loading on managed Chrome browsers or managed user profiles on mobile devices. This includes ensuring the functionality works seamlessly with Context-Aware Access (CAA) which allows admins to set access policies based on user context (for example, user role, location) and device state (for example, managed device, security compliance).

- **Chrome 136 on Android**
- **Chrome 137 on iOS**

Refactor DLP rules user experience

We aim to create a more user-friendly and efficient interface for Chrome-specific DLP rules. This involves redesigning the rule creation workflow in the Admin console to better accommodate existing and upcoming security features for Chrome Enterprise Premium customers.

- **Chrome 137 on Windows, macOS, Linux, ChromeOS**

Reporting connector for mobile

We are working towards feature parity with the desktop version, enabling organizations to monitor and respond to security events on mobile devices, such as unsafe site visits and potential data exfiltration attempts. This helps ensure consistent security and policy enforcement across different platforms.

- **Chrome 137 on Android, iOS**

Connectors API

We plan to simplify the setup process for third-party security connectors and enable providers to manage configurations directly from their own UI. This aims to make it easier for organizations to integrate their preferred security tools and services with Chrome, enhancing security and management across different platforms.

- **Chrome 137 on Windows, macOS, Linux, ChromeOS**

Previous release notes

Chrome version & targeted Stable channel release date
Chrome 134: February 26, 2025
Chrome 133: January 9, 2025
Chrome 132: January 8, 2025
Chrome 131: November 6, 2024
Archived release notes

Additional resources

- For emails about future releases, sign up here.
- To try out new features before they're released, sign up for the trusted tester program.
- Connect with other Chrome Enterprise IT admins through the Chrome Enterprise Customer Forum.
- How Chrome releases work—Chrome Release Cycle
- Chrome browser downloads and Chrome Enterprise product overviews—Chrome browser for enterprise
- Chrome version status and timelines—Chrome Platform Status | Google Update Server Viewer
- Announcements: Chrome Releases Blog | Chromium Blog
- Developers: Learn about changes to the web platform.

Still need help?

- Google Workspace, Cloud Identity customers (authorized access only)—Contact support
- Chrome browser Enterprise Support—Sign up to contact a specialist
- Chrome Administrators Forum
- Chrome Enterprise Help Center