Chrome 100 Enterprise release notes

For administrators who manage Chrome browser or Chrome devices for a business or school.

These release notes were last updated on March 29, 2022.

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

Chrome 100 release summary

Chrome browser updates	**Security**	**User productivity /Apps**	**Management**
Screen sharing fix for macOS		✓	
Chrome major version number reaches 100		✓	
Updates for Legacy Browser Support <open-in> rules			✓
Chrome 100 removes the AllowSyncXHRInPageDismissal policy			✓
New WebHID enterprise policies			✓
Chrome 100 removes Lite Mode on Android		✓	
Chrome Actions introduced on Android		✓	
Chrome on Android supports login using QR codes	✓		
Updates to the Certificate Transparency policy	✓		
Multi-Screen Window Placement API stable launch		✓	
Changes to tab-sharing blue border behavior		✓	
Chrome on iOS users can choose their default website view		✓	
Chrome adds Google Account-tied tokens to Enhanced Safe Browsing pings	✓		
Dismiss password alerts on Desktop	✓	✓	
Chrome expands SCT auditing to more users	✓		
Chrome no longer supports TLS 1.0/1.1 on Android WebView	✓		
New and updated policies in Chrome browser			✓
Chrome OS updates	**Security**	**User productivity /Apps**	**Management**

Chrome OS Dictation text editing		✓	
Chrome OS Flex	✓	✓	✓
Admin console updates	**Security**	**User productivity /Apps**	**Management**
Chrome Browser Cloud Management (CBCM) supports Chrome on Android		✓	✓
Remotely connect to any device from the Admin console			✓
New policies in the Admin console			✓
Upcoming Chrome browser changes	**Security**	**User productivity /Apps**	**Management**
Chrome 101 will remove setTimeout clamping to 1ms		✓	
Chrome 101 will add new CSV Export for some Chrome Admin console reports			✓
Deprecation Origin Trial for UA Reduction in Chrome 101	✓		
Chrome Browser Cloud Management will maintain compatibility with the most recent 12 versions of Chrome			✓
Chrome 101 will support Android 13 and above notification permission changes		✓	
MetricsReportingEnabled policy available in Chrome 101 on Android			✓
Privacy Sandbox updates in Chrome 101	✓		
WebSQLInThirdPartyContextEnabled will be removed in Chrome 101	✓		
Compare search results with new Side Search feature in Chrome 101		✓	
Legacy policies with non-inclusive names will be removed in Chrome 101			✓

Chrome apps will no longer work in Chrome 102		✓	✓
Chrome 102 to use case-matching on CORS preflight requests	✓		
Chrome 102 to send Private Network Access preflights for subresources	✓		
Chrome will use MiraclePtr to improve security	✓		
Network Service on Windows to be sandboxed in Chrome 102	✓		
Default to origin-keyed agent clustering in Chrome 106	✓		

The enterprise release notes are available in 8 languages. You can read about Chrome's updates in English, German, French, Dutch, Spanish, Portuguese, Korean, and Japanese. Please allow 1 to 2 weeks for translation for some languages.

Chrome browser updates

Screen sharing fix for macOS

If your users are having trouble sharing their screens on macOS, please see this guide for instructions on how to fix it.

Chrome major version number reaches 100

Chrome is now on a 3-digit version number. When browsers went from version 9 to 10, the increase in the number of digits uncovered many issues in User-Agent string parsing libraries.

An Enterprise policy ForceMajorVersionToMinorPositionInUserAgent is available to control whether the User-Agent string major version should be frozen at 99. If you have an app that is broken in version 100 due to a User-Agent parsing error, you can set the policy to 2 and the User-Agent string freezes the major version at 99 and includes the browser's major version in the minor position.

Updates for Legacy Browser Support <open-in> rules

When the BrowserSwitcherParsingMode policy is set to IE-compatible, Chrome updates the Legacy Browser Support rules:

- For v2 sitelists, <open-in> behavior is changed in the following ways:
  - `<open-in>None</open-in>` entries are treated as a greylist, and will open in any browser, rather than as inverted sitelist entries.
  - `<open-in>MSEdge</open-in>` entries will open in Chrome, as Windows treats this to mean the default, modern browser.
  - Anything unspecified opens in any browser, the same as greylist entries
- For v1 sitelists, `doNotTransition="true"` entries are treated as a greylist, and will open in any browser, rather than as inverted sitelist entries.

To mitigate disruption, this change only applies if you set BrowserSwitcherParsingMode policy is set to 1.

The documentation for Legacy Browser Support can be found here.

Chrome 100 removes the AllowSyncXHRInPageDismissal policy

The AllowSyncXHRInPageDismissal policy was introduced in Chrome 78 to give enterprises more time to adapt to the removal of synchronous XHR requests during page dismissal. Though this policy was originally planned to be removed in Chrome 93, the transition period was extended to allow developers more time to adapt. This transition period is now closed and Chrome 100 removes this policy.

New WebHID enterprise policies

As early as Chrome 100, Chrome adds new policies to manage the WebHID API. DefaultWebHidGuardSetting configures the default API behavior for all URLs and can be configured to allow origins to Ask for new device permissions or Block all permission requests. The WebHidAskForUrls and WebHidBlockedForUrls policies override the default policy for specific URLs.

Three new policies are added for automatically granting device permissions. URLs contained in the WebHidAllowAllDevicesForUrls policy will be automatically granted permissions for any connected device. The WebHidAllowDevicesForUrls and WebHidAllowDevicesWithHidUsagesForUrls policies can be used to grant narrower permissions by matching against vendor and product IDs or application collection usages in the HID report descriptor.

Chrome 100 removes Lite Mode on Android

Lite Mode was a way to reduce data usage on Android devices. Since its introduction, the cost of data has been reduced in many countries, and Chrome has invested in other ways to save data. As a result, Lite Mode is no longer available, including the DataCompressionProxyEnabled policy used to control it.

Chrome Actions introduced on Android

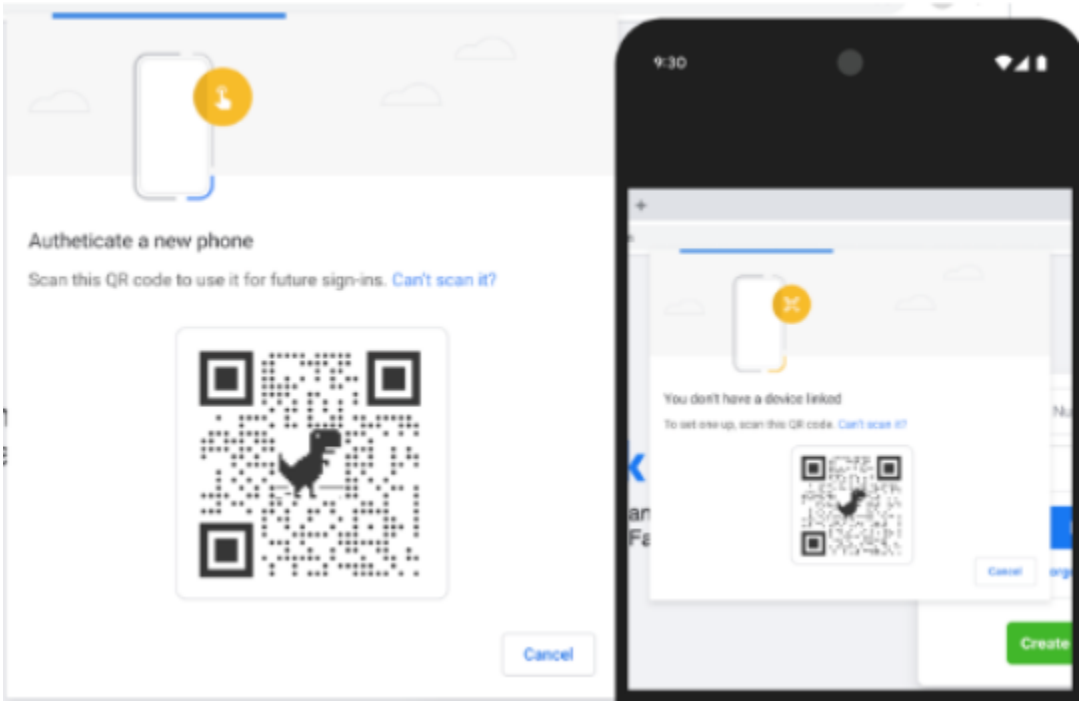
Chrome Actions help users get things done fast, directly from the address bar. We first released Chrome Actions on desktop a couple of years ago, with Actions like Clear browsing data. Now, we're bringing some of them to Chrome on Android, like:

- Manage passwords
- Open Incognito tab
- Clear browsing data
- And more!

Chrome on Android allows users to take actions directly from the address bar, like clearing browsing data, using a button that appears among auto-complete suggestions. This feature is already available on desktop platforms.

Chrome on Android supports login using QR codes

Chrome 100 allows users to use any Android phone as a security key by scanning a QR code. Previously, only phones that were syncing to the same Google account as the desktop could be used. Bluetooth is still required to show proximity.



Updates to the Certificate Transparency policy

In Chrome 100, the Certificate Transparency requirements in Chrome change; certificates are no longer required to include signed certificate timestamps (SCTs) from one Google operated and one non-Google operated log, and instead are required to include SCTs from at least two logs

from different operators. Additionally, the amount of SCTs required for certificates with a lifetime between 180 days and 15 months increase, from 2 to 3. The existing policies that allow selectively disabling CT enforcement (CertificateTransparencyEnforcementDisabledForCas, CertificateTransparencyEnforcementDisabledForLegacyCas, and CertificateTransparencyEnforcementDisabledForUrls) continue to work.

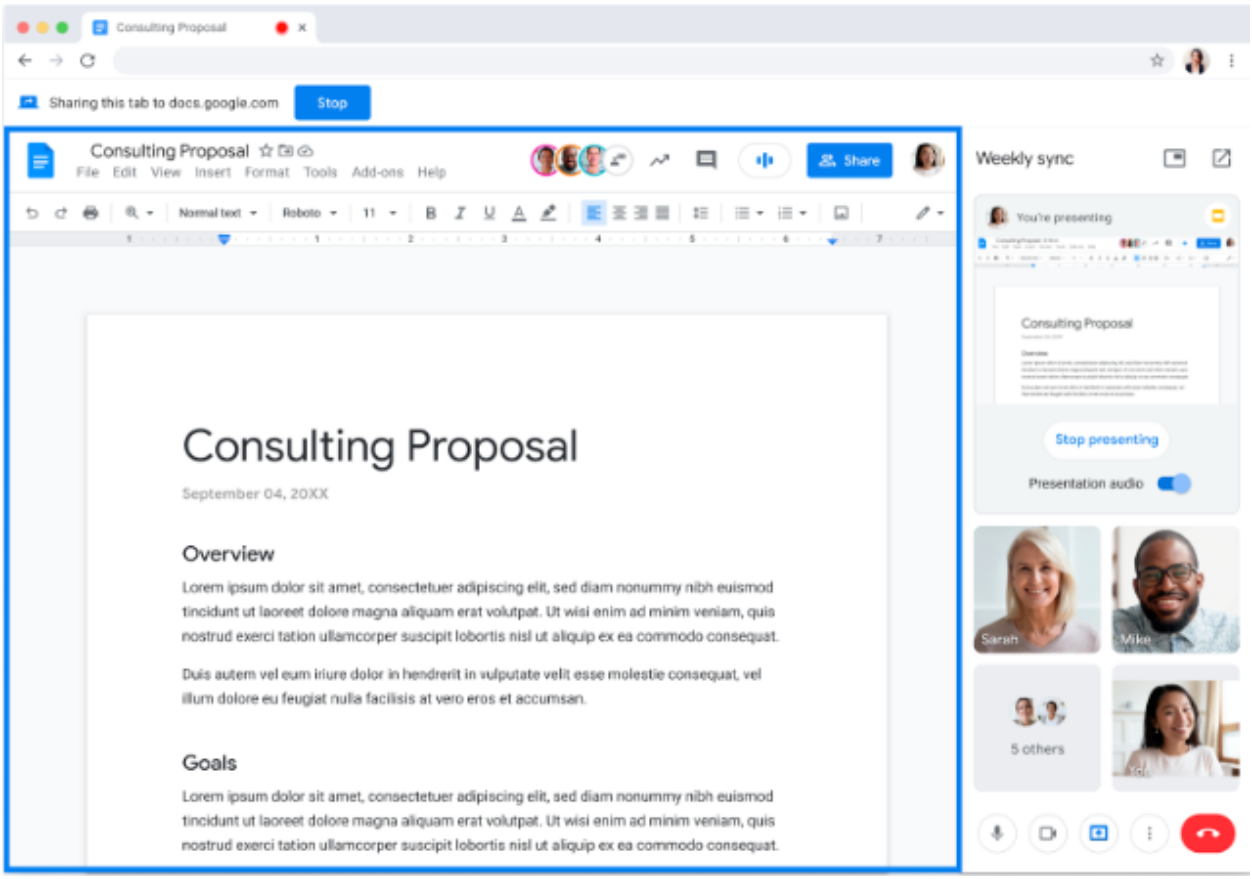
Multi-Screen Window Placement API stable launch

Multi-Screen Window Placement API adds new screen information APIs and makes incremental improvements to existing window placement APIs, allowing web applications to offer compelling multi-screen experiences. The existing singular `window.screen` offers a limited view of available screen space, and window placement functions generally clamp bounds to the current screen. This feature unlocks modern multi-screen workspaces for web applications.

A new set of policies, DefaultWindowPlacementSetting, WindowPlacementAllowedForUrls, and WindowPlacementBlockedForUrls, lets admins force their fleet to employ a default setting and automatically accept or deny the Window Placement permission without prompting the user, per origin.

Changes to tab-sharing blue border behavior

When a user shares their tab, the blue border used to indicate that a tab is being shared no longer appears around the whole tab. Instead, only the captured content has a blue border.



Chrome on iOS users can choose their default website view

In Chrome on iOS, users can choose the default view, Desktop or Mobile, in which the websites are requested. You can access this from **Settings**.

Chrome adds Google Account-tied tokens to Enhanced Safe Browsing pings

For users who consented to Enhanced Safe Browsing and are signed in to their Google accounts, Chrome adds Google Account-tied tokens to various incident reporting pings, except when in Incognito mode. This enables better tailored protection after encountering Safe Browsing warnings.

You control this feature on your environment using the SafeBrowsingProtectionLevel enterprise policy.

Dismiss password alerts on Desktop

To reduce noise from unnecessary alerts, Chrome Desktop users can now dismiss password alerts for compromised passwords. You can prevent end users from dismissing password alerts with the PasswordDismissCompromisedAlertEnabled policy.

Chrome expands SCT auditing to more users

As part of Chrome's Certificate Transparency protections, Chrome expands the existing signed certificate timestamp (SCT) auditing to all users that have Safe Browsing enabled. With this change, Chrome makes rare — less than one in 10,000 TLS connections — privacy-preserving queries to Google to ensure that Certificate Transparency logs are operating correctly. If a query detects a misbehaving log, the client will provide evidence of that misbehavior (the certificate chain and all SCTs) to Google. Chrome does not share certificates that are not issued by publicly trusted root certificates. CT ensures that all certificates or SCTs from publicly trusted roots are already public information, and no additional data is collected.

Chrome no longer supports TLS 1.0/1.1 on Android WebView

In Chrome 98, TLS 1.0/1.1 support was fully removed from Chrome on Windows, Mac, Linux, Android, and iOS. Starting in Chrome 100, TLS 1.0/1.1 is no longer supported on Android WebView. This might affect Android Apps using WebView which rely on connecting to a server that does not support TLS 1.2 or higher. Please update any servers to support modern TLS versions.

New and updated policies in Chrome browser

Policy	Description
PasswordDismissCompromisedAlertEnabled	Enable dismissing compromised password alerts for entered credentials
AllHttpAuthSchemesAllowedForOrigins	List of origins allowing all HTTP authentication
DefaultWebHidGuardSetting	Control use of the WebHID API
WebHidAskForUrls	Allow the WebHID API on these sites
WebHidBlockedForUrls	Block the WebHID API on these sites
WebHidAllowAllDevicesForUrls	Automatically grant permission to sites to connect to any HID device.
WebHidAllowDevicesForUrls	Automatically grant permission to these sites to connect to HID devices with the given vendor and product IDs.
WebHidAllowDevicesWithHidUsagesForUrls	Automatically grant permission to these sites to connect to HID devices containing top-level collections with the given HID usage.
OriginAgentClusterDefaultEnabled	Allows origin-keyed agent clustering by default.
DefaultWindowPlacementSetting	Default Window Placement permission setting
WindowPlacementAllowedForUrls	Allow Window Placement permission on these sites
WindowPlacementBlockedForUrls	Block Window Placement permission on these sites
ExemptDomainFileTypePairsFromFileTypeDownloadWarnings	Disable download file type extension-based warnings for specified file types on domains

Chrome OS updates

Chrome OS Dictation text editing

Dictation lets you use your voice to dictate text anywhere you would usually type on your Chromebook. Now, you can also edit text with your voice using commands like *delete*, *undo*, or *select all*. This feature is particularly useful for those who have motor impairments or anyone who prefers to use their voice to type.

We're initially launching with a small number of commands; we plan to add more in the future. Try it out by turning on dictation under **Settings** > **Accessibility** > **Keyboard and text input**. Whenever you are in a text area, you can select **Search + d** to activate dictation.

Chrome OS Flex

We announced early access to a new version of Chrome OS bringing the benefits of Chrome OS to PCs and Macs. Chrome OS Flex is the cloud-first, fast, easy-to manage, and secure operating system for PCs and Macs. Chrome OS Flex is now on the beta channel and since launch, 100+ more devices have been verified to work with Chrome OS Flex. Try it out and share your feedback to help us shape this product.

Admin console updates

Chrome Browser Cloud Management (CBCM) supports Chrome on Android

CBCM now supports enrolling Chrome-on-Android and sends reporting information back to the Admin console. Admins can get reporting information on policies that have been enabled, the OS version, model name, and other important data. More details are in our help center.

Remotely connect to any device from the Admin console

Admins can now establish a remote Chrome Remote Desktop (CRD) connection using a remote command under **Device details** for any device with an affiliated user or managed guest session. Previously, this feature was only available for devices in kiosk mode. More details are in our help center.

New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
SandboxExternalProtocolBlocked	User & Browser Settings; Managed Guest Session	Chrome Chrome OS	Content > iframe navigation
NetworkServiceSandboxEnabled	User & Browser Settings	Browser	Network > Network service sandbox
UserAgentReduction	User & Browser Settings; Managed Guest Session	Chrome Chrome OS Android	Network > User-Agent Reduction

UserAgentClientHintsGREASEUpdateEnabled	User & Browser Settings; Managed Guest Session	Chrome Chrome OS Android	Network > User-Agent client hints
DeviceI18nShortcutsEnabled	Device Settings	Chrome OS	Other settings > International keyboard shortcuts mapping
QuickAnswersEnabled	User & Browser Settings; Managed Guest Session	Chrome OS	User experience > Quick Answers > Enable Quick Answers
QuickAnswersDefinitionEnabled	User & Browser Settings; Managed Guest Session	Chrome OS	User experience > Quick Answers > Enable Quick Answers definition
QuickAnswersTranslationEnabled	User & Browser Settings; Managed Guest Session	Chrome OS	User experience > Quick Answers > Enable Quick Answers translation
QuickAnswersUnitConversionEnabled	User & Browser Settings; Managed Guest Session	Chrome OS	User experience > Quick Answers > Enable Quick Answers unit conversion

Coming soon

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

Upcoming Chrome browser changes

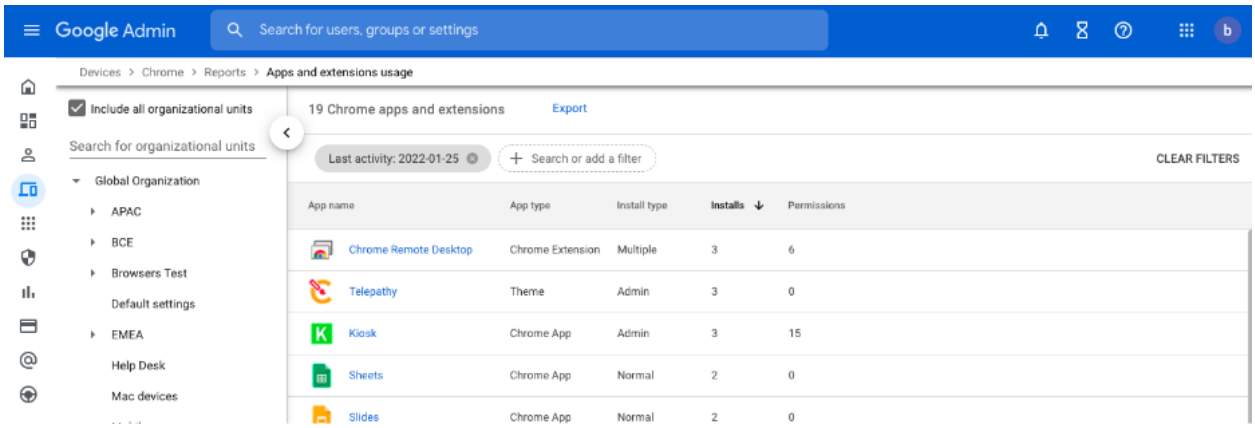
Chrome 101 will remove setTimeout clamping to 1ms

Chrome 101 removes a web intervention for some users that clamped `setTimeout(function,0)` timers to 1ms. In Chrome 101, those users will see timers fire immediately. Note that nested timer calls will clamp to 4ms after repeated nested calls. This change brings Chrome in line with web specifications and may improve performance on some pages.

It's possible that this change will introduce bugs in web applications that rely on the current clamped behavior. If you have any apps affected by this change, you can use the **SetTimeoutWithout1MsClampEnabled** policy to revert to the Chrome 100 behavior.

Chrome 101 will add new CSV Export for some Chrome Admin console reports

As early as Chrome 101, Chrome will introduce a new CSV download option for the Apps & Extensions Usage report data and the Versions report data.



Deprecation Origin Trial for UA Reduction in Chrome 101

As previously announced, Chrome 101 protects user privacy by reducing the granularity of information in the User-Agent string. In this phase, the MINOR.BUILD.PATCH version info is reduced to "0.0.0". If a site needs this information, it should migrate to the User Agent Client Hints API. Sites that need more time to test or migrate can take advantage of a Deprecation Trial, starting in Chrome 100.

You can also control this using the UserAgentReduction Enterprise policy. You can test the new reduced-granularity User-Agent string by setting the policy to 2, or you can delay the change while you update your apps by setting it to 1.

Chrome Browser Cloud Management will maintain compatibility with the most recent 12 versions of Chrome

Starting with Chrome 101, Chrome Browser Cloud Management will maintain compatibility with the most recent 12 versions of Chrome. Older versions may lose some CBCM features without notice, or behave unexpectedly. For your security, you should keep Chrome auto-update enabled, which will keep your fleet on the most recent version of Chrome. If you manage Chrome updates manually, staying close to the most recent version will both keep your users safer, and ensure you stay within the CBCM compatibility window.

Chrome 101 will support Android 13 and above notification permission changes

Android 13 is changing the way push notification permissions behave by default. All Android apps will require users to explicitly allow OS notification permissions (as opposed to Android 12 and earlier where it was granted by default). Chrome running on this version of Android will prompt the user for permission at app launch up to two times.

MetricsReportingEnabled policy available in Chrome 101 on Android

Chrome-on-Android will be slightly modifying the First Run Experience to support the MetricsReportingEnabled policy. If the admin has disabled metrics reporting, there will be no change. If the admin has enabled metrics, users will still be able to disable it.

Privacy Sandbox updates in Chrome 101

The Privacy Sandbox release in Chrome 101 provides controls for the new Topics & Interest Group APIs. It also introduces a one-time dialog that explains Privacy Sandbox to users and allows them to manage their preferences. This dialog is not shown for Guest users or managed EDU users.

Admins can prevent the dialog from appearing for their managed users by controlling third party cookies explicitly via policy:

- To allow third party cookies and Privacy Sandbox features, set BlockThirdPartyCookies to disabled
- To disallow third party cookies and Privacy Sandbox features, set BlockThirdPartyCookies to enabled. This may cause some sites to stop working.

Privacy Sandbox features will also be disabled (and no dialog shown) if DefaultCookiesSetting is set to *Do not allow any site to set local data*.

WebSQLInThirdPartyContextEnabled will be removed in Chrome 101

WebSQLInThirdPartyContextEnabled was introduced to give admins additional time to react to the removal of WebSQL in a third-party context. As planned, it is removed in Chrome 101.

Compare search results with new Side Search feature in Chrome 101

Side Search allows users to compare search results via a side panel UI to get the right answer faster. This means users can view a page and the search results at the same time, without needing to navigate back and forth or losing their search results. This is helpful for users who are actively searching for something and need more than one site, for example, planning an employee dinner, putting together presentations, and so on. This feature can be controlled using the SideSearchEnabled policy.

Legacy policies with non-inclusive names will be removed in Chrome 101

Chrome 86 through Chrome 90 introduced new policies to replace policies with less inclusive names (for example, whitelist, blacklist). In order to minimize disruption for existing managed users, both the old and the new policies currently work.

This transition period was originally planned for Chrome 95, but was extended to Chrome 101 to give admins more time to transition their policies. In Chrome 101, the policies in the left column of the following table will no longer function. Please ensure you're using the corresponding policy from the right column instead:

Legacy Policy Name	New Policy Name
NativeMessagingBlacklist	NativeMessagingBlocklist
NativeMessagingWhitelist	NativeMessagingAllowlist
AuthNegotiateDelegateWhitelist	AuthNegotiateDelegateAllowlist
AuthServerWhitelist	AuthServerAllowlist
SpellcheckLanguageBlacklist	SpellcheckLanguageBlocklist
AutoplayWhitelist	AutoplayAllowlist
SafeBrowsingWhitelistDomains	SafeBrowsingAllowlistDomains
ExternalPrintServersWhitelist	ExternalPrintServersAllowlist
NoteTakingAppsLockScreenWhitelist	NoteTakingAppsLockScreenAllowlist
PerAppTimeLimitsWhitelist	PerAppTimeLimitsAllowlist
URLWhitelist	URLAllowlist
URLBlacklist	URLBlocklist
ExtensionInstallWhitelist	ExtensionInstallAllowlist

ExtensionInstallBlacklist	ExtensionInstallBlocklist
UserNativePrintersAllowed	UserPrintersAllowed
DeviceNativePrintersBlacklist	DevicePrintersBlocklist
DeviceNativePrintersWhitelist	DevicePrintersAllowlist
DeviceNativePrintersAccessMode	DevicePrintersAccessMode
DeviceNativePrinters	DevicePrinters
NativePrinters	Printers
NativePrintersBulkConfiguration	PrintersBulkConfiguration
NativePrintersBulkAccessMode	PrintersBulkAccessMode
NativePrintersBulkBlacklist	PrintersBulkBlocklist
NativePrintersBulkWhitelist	PrintersBulkAllowlist
UsbDetachableWhitelist	UsbDetachableAllowlist
QuickUnlockModeWhitelist	QuickUnlockModeAllowlist
AttestationExtensionWhitelist	AttestationExtensionAllowlist
PrintingAPIExtensionsWhitelist	PrintingAPIExtensionsAllowlist
AllowNativeNotifications	AllowSystemNotifications
DeviceUserWhitelist	DeviceUserAllowlist
NativeWindowOcclusionEnabled	WindowOcclusionEnabled

If both the legacy policy and the new policy are set for any row in the table below, the new policy will override the legacy policy.

If you're managing Chrome via the Google Admin console (for example, Chrome Browser Cloud Management), no action is required; the Google Admin console will manage the transition automatically.

Chrome apps will no longer work in Chrome 102

As previously announced, Chrome apps are being phased out in favor of Progressive Web Apps and web-standard technologies. The deprecation schedule was adjusted to provide enterprises who used Chrome apps additional time to transition to other technologies, and Chrome apps will now stop functioning in Chrome 102. If you need additional time to adjust, a policy **ChromeAppsEnabled** will be available to extend the lifetime of Chrome Apps for an additional 2 releases.

Chrome 102 to use case-matching on CORS preflight requests

Chrome 101 and previous releases uppercase request methods when matching with Access-Control-Allow-Methods response headers in CORS preflight. Chrome 102 no longer uppercases request methods, except for those normalized in the spec. So, Chrome 102 and later will require exact case-sensitive matching.

Previously accepted, but now rejected:

```
Request: fetch(url, {method: 'Foo'})
Response Header: Access-Control-Allow-Methods: FOO
```

Previously rejected, but now accepted:

```
Request: fetch(url, {method: 'Foo'})
Response Header: Access-Control-Allow-Methods: Foo
```

Note: `post` and `put` methods are not affected because they are in the spec, while `patch` is affected.

Chrome to send Private Network Access preflights for subresources

As early as Chrome 102, Chrome plans to send a CORS preflight request ahead of any private network requests for subresources, asking for explicit permission from the target server. This request carries a new `Access-Control-Request-Private-Network: true` header. In this initial phase, this request is sent, but no response is required from network devices.

In a future release of Chrome, the response must carry a matching `Access-Control-Allow-Private-Network: true` header.

A private network request is any request from a public website to a private IP address or localhost, or from a private website, for example, an intranet, to localhost. Sending a preflight request mitigates the risk of cross-site request forgery attacks against private network devices such as routers, which are often not prepared to defend against this threat.

Chrome to use MiraclePtr to improve security

MiraclePtr is a technology that reduces the risk of security vulnerabilities relating to memory safety. Chrome is currently testing the impacts of MiraclePtr for some users. A full release is planned as early as Chrome 102.

Network Service on Windows will be sandboxed in Chrome 102

As early as Chrome 102, to improve security and reliability, the network service, already running in its own process, will be sandboxed on Windows. As part of this, third-party code that is currently able to tamper with the network service may be prevented from doing so. This might cause interoperability issues with software that injects code into Chrome's process space, such as Data Loss Prevention software. The NetworkServiceSandboxEnabled policy allows you to disable the sandbox if incompatibilities are discovered. You can test the sandbox in your environment using these instructions and report any issues you encounter.

Default to origin-keyed agent clustering in Chrome 106

As early as Chrome 106, websites will be unable to set *document.domain*. Websites will need to use alternative approaches such as `postMessage()` or Channel Messaging API to communicate cross-origin. If a website relies on same-origin policy relaxation via *document.domain* to function correctly, it will need to send an `Origin-Agent-Cluster: ?0` header along with all documents that require that behavior.

Note: *document.domain* has no effect if only one document sets it.

An enterprise policy will be available to extend the current behavior.

Previous release notes

Chrome version & targeted Stable channel release date	PDF
Chrome 99: March 01, 2022	PDF
Chrome 98: February 01, 2022	PDF
Chrome 97: January 04, 2022	PDF
Chrome 96: November 16, 2021	PDF
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 and features planned for upcoming releases.

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