chrome enterprise

M93 Enterprise Release Notes

Each new Chrome release contains thousands of improvements. Here, you can review new features and changes that might be of interest to you and other administrators who manage Chrome Browser and device deployments.

These release notes were last updated on August 31, 2021.

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

Sign up here for our email distribution for future releases.

Chrome 93

Chrome browser updates

SyncXHR policy is no longer available

Chrome 93 removes the AllowSyncXHRInPageDismissal enterprise policy. Before updating to Chrome 93, web application owners must update all apps that previously relied on legacy platform behavior. This change was previously planned for Chrome 88, but delayed to provide more time for enterprises to update legacy applications.

New RelaunchWindow policy

The RelaunchWindow enterprise policy allows admins to specify a window of time when Chrome relaunches to force an update to apply. You can use this policy, in conjunction with RelaunchNotification, RelaunchNotificationPeriod, and RelaunchHeadsUpPeriod to control when Chrome relaunches to apply an update. **RelaunchWindow** helps you to minimize disruption and to force a relaunch outside of business hours. In Chrome 93, these policies are available in Group Policy. These policies will become available in the Admin console at a later date.

New JavaScript JIT setting policies

Chrome 93 introduces three new policies:

- DefaultJavaScriptJitSetting
- JavaScriptJitAllowedForSites
- JavaScriptJitBlockedForSites

These policies allow Chrome's JavaScript engine to default to using the Ignition interpreter in a JIT-less mode for a set of enterprise-defined sites.

Disabling the JavaScript JIT in this way may allow Chrome to render web content in a more secure configuration, as no executable permissions are needed for memory regions. However, disabling JIT has performance costs and currently disables some parts of JavaScript, including WebAssembly.

Full launch of Drive priority launchpad on New tab page

To help users get work done faster, Chrome 93 shows the Drive files the user is more likely to need on the **New tab** page. This feature uses Drive’s existing priority API, which powers the Priority section of drive.google.com. Some users see this change in Chrome 93.

Publishing updates to extensions requires 2-Step Verification

As part of the rollout of a set of updates and clarifications to the Chrome Web Store extension policies, the Chrome Web Store now requires 2-Step Verification on developer accounts *before* adding a new extension or updating an existing extension. This does not impact extensions that are self-hosted, sideloaded, or that are no longer being updated.

Developer accounts belonging to organizations where the admin has disabled 2-Step Verification for their organization are exempt from this requirement.

Updates to the lock icon in the address bar

Some users might see a new icon replacing the lock in the address bar, which is shown on sites that support HTTPS. The new icon aims to improve the discoverability of the *Page Info* surface, which includes site-level security and privacy information and controls. A *Not Secure* indicator continues to appear on sites without HTTPS support. An enterprise policy, LockIconInAddressBarEnabled, is available to revert to the original lock icon. See our blog post Increasing HTTPS Adoption for more information.

New feature changes to the User-Agent Client Hints API updates

Chrome 93 adds four feature changes to the User-Agent client hints API:

- Adding a Sec-CH-UA-Bitness User Agent Client Hint to return the bitness of the platform, which might be useful, for example, for sending optimized binaries during a download.
- Making Sec-CH-UA-Platform a low-entropy hint that is sent by default. Prior to this change, this hint would need to be requested.
- Including low-entropy hints by default in UADataValues (returned by `getHighEntropyValues()`): if a hint moves from high to low-entropy, this prevents site compatibility issues.
- Adding a toJSON method to NavigatorUAData. Instead of returning {}, `JSON.stringify(navigator.userAgentData)` is now useful.

An enterprise policy UserAgentClientHintsEnabled is available to control this feature. This policy will be removed in Chrome 94. Developers can leave feedback at crbug.com/1241062 on any issues related to this feature.

Chrome on iOS adds a new way to sign in

On iOS, when a user signs in to their Google Account on the web, they can sign in to Chrome with a Google Account that's already saved on their device. This does not enable Chrome sync by default; the user can opt into that separately if they want sync enabled. You can control the behavior of sign-in on Chrome on iOS and other platforms using the BrowserSignIn policy.

Chrome performs sentiment measurement

Chrome 93 performs sentiment measurement of users of Trusted Surface, Privacy Settings and Transactions. These surveys are delivered on the **New tab** page after the user has engaged with the feature. The delivery of these surveys can be disabled by disabling metrics via the MetricsReportingEnabled policy.

Chrome redesigns desktop *page info* surface

Chrome 93 continues to redesign the desktop *page info* surface. The purpose of this redesign is to improve scalability by introducing modular subpages, toggles for permissions and restructuring the main view to surface the important information first.

Tab Groups in desktop Recently closed menu

Chrome 93 allows users to see their tab groups in the **Recently closed** menu and helps alleviate worry about permanent loss of groups. This launch enables the whole group and individual tabs inside a group to restore from the Chrome desktop recently closed menu.

Save payment information to a Google Account

In Chrome 93, users who are signed in to their managed Google Account see an option to save their payment information to their Google Account. As an administrator, you can turn off this feature (Sync Service setting) in the Admin console or by using the AutofillCreditCardEnabled policy. This was previously available on Android and desktop and is now also available on iOS.

URL protocol handlers in web manifests

Chrome 93 is running an Origin Trial for URL protocol handlers in web manifests. This Origin Trial started in Chrome 92 and will end in Chrome 94. The handlers follow the PWA's lifecycle -- they are set up on PWA install, and removed on PWA uninstall. You can find out more in this article.

Note: The Origin Trial started in Chrome 92 but was initially not part of the Chrome 92 blog post.

New Incognito Exit Point on Clear browsing data

Chrome 93 introduces a new Close windows confirmation dialog which is displayed when a user selects **Clear browsing data** from the overflow menu or Chrome Actions on Omnibox while on Incognito mode. This dialog contains text explaining that **Clear browsing data** ends the Incognito session, and two call-to-action buttons: **Close windows** and **Cancel**.

Pausing quantum computer resistant security

Some devices behaved unexpectedly when Chrome offered quantum-resistant cryptography for TLS connections. We're working with those companies to provide fixed firmware for their devices and have temporarily disabled this technology.

For more details, see the Chromium Open Source Project.

LegacySameSiteCookieBehaviorEnabled is no longer available

When same-site cookie behavior was introduced, Chrome included policies to give admins extra time to adjust the implementation of any enterprise apps that relied on the legacy cookie behavior.

The first phase of the transition plan ends in Chrome 93, and LegacySameSiteCookieBehaviorEnabled is no longer taking effect. You will still be able to opt specific sites into the legacy cookie behavior using LegacySameSiteCookieBehaviorEnabledForDomainList until December 31st, 2022.

3DES TLS cipher suites are no longer supported

Chrome 93 removes support for 3DES TLS cipher suites. The TripleDESEnabled enterprise policy was made available in Chrome 92 to test this change, and will be available temporarily until Chrome 95, to give enterprises additional time to adjust.

Ubuntu 16.04 is no longer supported

Ubuntu 16.04 is past the end of standard support, and is no longer supported. The updated system requirements for Chrome are available here.

New and updated policies in Chrome browser

Policy	Description
DefaultJavaScriptJitSetting	Allows you to set whether Google Chrome runs the v8 JavaScript engine with JIT (Just In Time) compiler enabled or not.
DesktopSharingHubEnabled	Enable the sharing icon from the omnibox and the entry from the 3-dot menu.
JavaScriptJitAllowedForSites	Allows you to set a list of site URL patterns that specify sites which are allowed to run JavaScript with JIT (Just In Time) compiler enabled.

JavaScriptJitBlockedForSites	Allows you to set a list of site URL patterns that specify sites which are not allowed to run JavaScript JIT (Just In Time) compiler enabled.
LockIconInAddressBarEnabled	Controls the treatment for lock icon in the omnibox. From Chrome 93, there is a new omnibox icon for secure connections. If the policy is Enabled, Chrome uses the existing lock icon for secure connections. If the policy is Disabled or not set, Chrome uses the default icon for secure connections.
RelaunchWindow	Specify a target time window for the end of the relaunch notification period.
RemoteDebuggingAllowed	Controls whether users may use remote debugging.

Chrome OS updates

Enable Android applications to access Chrome OS certificates

Previously Android applications could only access certificates provisioned within Android, but not those in Chrome OS. Admins can now enable Android apps to access Chrome OS user and device certificates.
For more information, see the Help Center.

Regular online re-authentication for identity providers on the login and lock screen

Regular online authentication provides additional security for organizations that require 2FA or MFA authentication and organizations that use third-party identity providers like Okta.
As an admin, you can require regular online re-authentication on the login screen for users of third-party identity providers. Chrome OS 93 expands this capability to re-authenticate using the lock screen and also extends re-authentication support to users of Google identity, including those using 2FA like Yubikeys or SMS.
There are now three new controls to help manage online re-authentication:

1. SAML single sign-on unlock frequency
2. Google online login frequency
3. Google online unlock frequency

Admin console updates

Sending Extension Requests for Chrome browser Desktop and Chrome OS

As an admin, you can block users from installing extensions and the Chrome Web Store will now have a Request button so that you can see their requests from within the Admin console and take an action to allow or to block the extensions. To enable the feature, please follow the steps in the Help Center.

Chrome Browser Cloud Management is available for Chrome-on-iOS

Chrome Browser Cloud Management now supports Chrome-on-iOS. The policies for Chrome-on-iOS can be seen at https://chromeenterprise.google/policies (then filter for iOS platform). To get started, please visit the Help Center.

Chrome Browser Cloud Management Release Channel selector

Admin console now has a release channel selector (Stable, Beta, Dev) for Chrome Browser Cloud Management on Windows, Mac, or Linux. For more details, see the Help Center.

New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
SamlLockScreenOfflineSigninTimeLimitDays	User & Browser Settings	Chrome OS	Security/SAML single sign-on unlock frequency
GaiaLockScreenOfflineSigninTimeLimitDays	User & Browser Settings	Chrome OS	Security/Google online unlock frequency
ForcedLanguages	User & Browser Settings	Chrome Win/Mac/Linux	User experience/Preferred languages

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.

Chrome 94 is moving to a 4-week stable channel and introducing an 8-week extended stable channel

Chrome on mobile, Windows, Mac, and Linux will move from its current 6-week release cycle to a 4-week release cycle, allowing security features, new functionality and bug fixes to reach users more quickly. Note that Chrome 94’s shorter development cycle means Chrome 93 will be live in the stable channel for less time as well; specific release dates for both milestones can be found on our schedule.

No action is required for most enterprises, but if you manually update or test new releases of Chrome and prefer a slower release cadence, you'll be able to use the **TargetChannel** policy to switch Chrome on Mac and Windows to an extended stable channel, with a new release every 8 weeks instead. The option of Extended Stable will be added to the Target Channel

Control in the Admin console in Chrome 94. You can find more details in our blog post at blog.chromium.org.

To ensure continuous improvements to the Chrome OS platform, Chrome OS will move to a 4-week stable channel starting with Chrome 96. To bridge the gap between Chrome 94 and Chrome 96, Chrome OS will skip Chrome 95 (see the updated Chrome schedule page for milestone-specific details).

To provide commercial users with another dependably secure stable platform, Chrome OS will also introduce a new channel with a 6-month update cadence by Chrome 96. More details to be announced soon.

Upcoming Chrome browser changes

As early as Chrome 94, the browser list data will be available for download in CSV format in the Admin console

Chrome will introduce the CSV format as an option to download the browser list data from the Admin console.

Chrome 94 on iOS will be able to apply .mobileconfig files

A `.mobileconfig` file can be used to configure an iPhone, iPod touch, and iPad to work with certain enterprise systems. Since iOS 12.2, mobileconfig files can be downloaded and installed from Safari and Mail apps. Chrome will be able to download these files and continue to settings so the user can apply them.

Chrome 94 will support usage of Android phones as security keys

When Chrome on a desktop or laptop is signed into the same account as Chrome on an Android phone, that phone can be used as a security key.

This feature requires that the desktop has a Bluetooth Low Energy (BLE) adaptor. Communication between the devices is end-to-end encrypted with keys exchanged over BLE to prove proximity with the phone.

Chrome 94 will launch What's New in Chrome

What's New will be an effortless way for users to discover new features. Starting in Chrome 94 some users will see a page that highlights a few features. What's New will automatically show as the focused tab. You can disable this feature by using the existing PromotionalTabsEnabled enterprise policy.

Chrome 94 will no longer allow insecure public pages to make requests to private or local URLs

Non-secure contexts served from public IP addresses will no longer be able to make subresource requests to IP addresses belonging to a more private address space (as defined in Private Network Access). For example, **http**://public.example served on IP 1.2.3.4 will not be able to make requests targeting IP 192.168.0.1 or IP 127.0.0.1. You can control this behavior using the InsecurePrivateNetworkRequestsAllowed and InsecurePrivateNetworkRequestsAllowedForUrls enterprise policies, which became available for testing in Chrome 92.

Ability for PWAs to be registered as (platform level) URL handlers

Chrome 94 will run an Origin Trial to allow Progressive Web Apps (PWAs) to register as URL handlers. This means that PWAs can be launched in response to URL link activations, including activations from native apps. PWAs will be allowed to register to handle any https URL, not just URLs from their own app scope. If you're interested in learning more about PWAs as URL handlers, please refer to this article.

Launching a sharing hub

In Chrome 94, users will be able to more easily share their current page, including the ability to send the current page to their devices, get a QR code for the current URL, and share to third-party apps. You will be able to control this feature using an enterprise policy called DesktopSharingHubEnabled.

Chrome 94 will use updated language in managed profile sign-in notice

Chrome 94 will update the notice when users sign into a managed profile. The new notice will have language clarifying that a separate profile is required and the available buttons will be simplified. Some users will see a link to open Chrome in guest mode when they sign in to a new profile that's different from the profile signed in to Chrome.

Chrome 94 will add a new enterprise policy for the Web Serial API

The Web Serial API allows sites to request access to serial devices (USB, Bluetooth, etc.) through a device selection prompt. In previous Chrome versions, policy controls could only control how the feature was blocked. In Chrome 94, admins will be able to grant a site access to specific (or all) connected serial devices, streamlining workflows by removing the need for users to select the correct device.

Chrome settings restructure

To aid in navigability, Chrome will replace the single long page in Chrome settings with individual sections. The updated experience will be available starting with Chrome 94.

Chrome 94 will launch HTTPS-First mode (Android and Desktop)

HTTPS-First mode will attempt to upgrade all page loads to HTTPS and display a full-page warning before loading sites that don’t support it. Users who enable this mode gain confidence that Chrome is connecting them to sites over HTTPS whenever possible, and that they will see a warning before connecting to sites over HTTP. An enterprise policy will exist to disable the use of this mode.

Chrome 94 will update certificate transparency log list via component updater

Chrome 94 will start using Component Updater to dynamically update the certificate transparency log list, separating these updates from full browser updates, and allowing out-of-date clients to keep enforcing Certificate Transparency.

Chrome 94 will introduce tab grid bulk actions

Chrome for iOS will add an edit mode to the tab grid to allow easier management of open tabs. Multiple tabs can be selected and then added to the reading list, bookmarked, shared, or closed.

As early as Chrome 94, Chrome will delete inactive browsers from Chrome Browser Cloud Management

Many enterprise customers have to adhere to regulation around data retention. To aid in this effort, we will launch a new policy that will automatically delete inactive browser information from Google servers.

By default, browsers that do not connect to the Google servers for 365 days will be considered inactive and automatically deleted. Admins will be able to modify the default value.

Chrome 94 will test Chrome Accuracy Check

Chrome plans to remind users to evaluate the accuracy of information. Chrome Accuracy Check will show users tips for evaluating information quality for news sites when they might be helpful.

Chrome 94 will remove UserAgentClientHintsEnabled policy

The use of Structured Headers in the User Agent Client Hints, and in particular, the Sec-CH-UA and Sec-CH-UA-Mobile headers, caused some unintended consequences where not all servers were able to accept all characters. An enterprise policy UserAgentClientHintsEnabled was created to disable this feature. This policy will be removed in Chrome 94.

Chrome 94 will add new Security Events to BeyondCorp Enterprise Threat and Data Protection (Password Leak and Login)

Chrome 94 will add two new Security Events to BeyondCorp Enterprise Threat and Data Protection: Password leak and login. This functionality will allow administrators to understand enterprise credential usage and Shadow IT within their organization, and to stay ahead of potential security incidents regarding passwords exposed in data breaches.

Chrome 94 will launch an API that allows sites to know when the user is active

Chrome 94 will launch the Idle Detection API, allowing websites to request the ability to query if users are idle, allowing messaging apps to direct notifications to the best device. This was previously in Origin Trial and is now rolled out to Stable.

Chrome 94 will launch display-capture

The display-capture permissions-policy allows sites to more safely embed documents in an iframe. The display-capture permissions-policy can be used to remove the capability of a document in an iframe initiating a screen-capture. An enterprise policy will be created to control this feature - **DisplayCapturePermissionsPolicyEnabled**. This policy will be removed in Chrome 100.

Migrate to Open Screen Library Cast channel

Chrome 95 will use a new implementation to connect to devices that support Cast like Chromecast, Nest Hub and Android TV. Chrome users will not observe any differences in how Cast works.

Chrome 95 will introduce stricter parsing rules for Legacy Browser Support

Organizations that rely on Legacy Browser Support (LBS) to redirect their users to Microsoft® Edge® or Internet Explorer® can use the **BrowserSwitcherParsingMode** policy to choose how their site list is interpreted by Chrome. If set to strict mode, Chrome will interpret those rules in the same way as Edge® and Internet Explorer®.

In Chrome 95, Chrome apps will be deprecated on Mac, Windows, and Linux

As part of the previously-communicated plan to replace Chrome apps with the open web, Chrome apps will no longer function on Mac, Windows, and Linux in Chrome 94. For enterprises that need extra time to adjust to the removal of Chrome apps, a policy will be available to extend support for them until June 2022.

As early as Chrome 95, Chrome will no longer allow TLS 1.0 or TLS 1.1

The SSLVersionMin policy no longer allows setting a minimum version of TLS 1.0 or 1.1. This means the policy can no longer be used to suppress Chrome's interstitial warnings for TLS 1.0 and 1.1. Administrators must upgrade any remaining TLS 1.0 and 1.1 servers to TLS 1.2. In Chrome 91 we announced that the policy no longer works, but users could still bypass the interstitial. As early as Chrome 95, it will no longer be possible to bypass the interstitial.

As early as Chrome 95, the network Service on Windows will be sandboxed

To improve the security and reliability of the service, the network service, already running in its own process, will be sandboxed on Windows to improve the security and reliability of the service. As part of this, third-party code that is currently able to tamper with the network service will 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. You'll be able to disable the change with an enterprise policy when it becomes available.

Chrome 95 will conduct an Origin Trial for User-Agent Reduction

Chrome 95 will be conducting an Origin Trial for the fully reduced User-Agent string. We would like sites to begin participating in the trial so we may collect feedback and allow sites to have ample time to address breakage. The reduced User-Agent string will appear in both the User-Agent HTTP request header as well as the JavaScript APIs that access the User-Agent string (`navigator.userAgent`, `navigator.appVersion`, `navigator.platform`). The Origin Trial will last six milestones until the reduced User-Agent string becomes the default in Chrome, with a deprecation Origin Trial to continue receiving the full User-Agent string for those sites that still need more time to migrate. Enterprises can opt in to the Origin Trial here when it is available.

Chrome 95 will deprecate WebAssembly cross-origin module sharing

Chrome 95 will prevent WebAssembly module sharing between cross-origin but same-site environments.This will allow agent clusters to be tied to origins in the long-term. This change conforms to recent changes in the WebAssembly spec.

If your enterprise needs any additional time to adjust to this change, a temporary enterprise policy will be made available to allow module sharing for cross-origin same-site environments.

As early as Chrome 95, Apps shortcut in the Bookmarks Bar will default to off

Chrome will make the Apps shortcut in the bookmark bar default to off and update the current state for all users to the new default (off).

As early as Chrome 97, Chrome may leverage MiraclePtr to improve security

Chrome will leverage MiraclePtr to reduce the risk of security vulnerabilities relating to memory safety. The Chrome team gathered data on the performance cost of MiraclePtr in Chrome 91, but domain-joined enterprises on the stable channel were excluded from MiraclePtr builds during that phase. A full release of MiraclePtr in Chrome is planned as early as Chrome 97.

As early as Chrome 97, Chrome will maintain its own default root store

To improve user security, and provide a consistent experience across different platforms, Chrome intends to maintain its own default root store. If you are an enterprise admin managing your own Certificate Authority (CA), you should not have to manage multiple root stores. We do not anticipate any changes will be required for how enterprises currently manage their fleet and trusted enterprise CAs, such as through group policy, macOS Keychain Access, or system management tools like Puppet.

Chrome 97 will remove legacy policies with non-inclusive names

Chrome 86 through Chrome 90 introduced new policies to replace policies with less inclusive names. To minimize disruption for existing managed users, both the old and the new policies currently work. This transition time is to ensure it's easy for you to move to and test the new policies in Chrome.

Note: 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.

This transition period will end in Chrome 97, and the following policies in the left column will no longer function. This change was originally announced for Chrome 95, but has been extended to Chrome 97.

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

As early as Chrome 98, different-origin iframes will no longer trigger JavaScript dialogs

Chrome will prevent iframes from triggering prompts (`window.alert`, `window.confirm`, `window.prompt`) if the iframe is a different origin from the top-level page. This change will prevent embedded content from spoofing the user into believing a message is coming from the website they're visiting, or from Chrome itself. Please note that this change was originally planned for Chrome 92, but has been postponed until at least Chrome 98 due to the feedback we received on this change. You can test if this future change will affect applications now by setting the *enable_features=SuppressDifferentOriginSubframeJSDialogs* flag.