chrome enterprise

M91 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 May 25, 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 91

Chrome browser updates

Chrome pauses collapsed tab groups

Chrome allows users to organize tabs into collapsible groups, helping them stay productive. For some users, Chrome 91 pausesthose tabs when the user collapses them, to reduce CPU and power consumption. Chrome does not pause tabs if they are playing audio, holding a web lock, holding an IndexedDB lock, connected to a USB device, capturing video or audio, being mirrored, or capturing a window or display.

Chrome blocks port 10080 and adds a policy for allowing specific ports

Chrome 91 adds port 10080 to the restricted ports list and blocks traffic through it. This does not affect customers using standard ports, but custom configurations using non-standard ports may be affected.

If you're affected by this change, or if you were affected by the previous change that blocked port 554, Chrome introduces the ExplicitlyAllowedNetworkPorts enterprise policy, where you can allow these specific ports in your environment.

Chrome enables quantum computer resistant security

Chrome 91 supports a post-quantum key-agreement mechanism in TLS when communicating with some domains. This increases the size of TLS handshake messages which, in rare cases, may cause issues with network middleboxes that incorrectly assume that TLS messages fit in a single network frame.

You can set the CECPQ2Enabled policy to disable this mechanism. You can also disable it by setting the ChromeVariations policy to a non-default value. For more details, see https://www.chromium.org/cecpq2.

Chrome no longer allows 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.

We previously communicated that this would happen as early as January 2021, but we extended the deadline until Chrome 91.

PWAs can launch when the user logs into the OS

Users expect some apps, like chat apps, to launch as soon as they log into a Windows or Mac device. Chrome 91 allows users to set Progressive Web Apps (PWAs) to launch as soon as the user logs into the OS.

As an admin, you can configure a PWA at install time with the option to launch automatically when a user logs in to its OS session.

You control this behavior using the WebAppSettings enterprise policy.

Chrome on iOS warns users if they reuse their saved passwords on known phishing sites

To better protect users from phishing schemes, Chrome warns users if it appears that they've entered a saved password on a known phishing site. This feature is now being expanded to Chrome on iOS.

You control your organization's use of this feature using the PasswordManagerEnabled enterprise policy.

Chrome introduces initial_preferences

As part of Chrome's move to using more inclusive naming, admins can control the browser's initial preferences using a file named *initial_preferences*. This file behaves the same way as, and will eventually replace, the master_preferences file that exists today. To minimize any disruption, Chrome continues to support the *master_preferences* file and more notice will be given before we remove support for *master_preferences*.

Chrome uses DNS-over-HTTPS on Linux

DNS-over HTTPS protects user privacy by encrypting DNS queries, and was already enabled for Windows, Mac, ChromeOS, and Android in prior releases. Chrome 91 supports this feature on Linux. The DNS requests of all users will be auto-upgraded to their DNS provider's DNS-over-HTTPS (DoH) service if available (based on a list of known DoH-capable servers). You can disable DNS-over-HTTPS for your users with the DnsOverHttpsMode policy with

Group Policy or in the Google Admin Console. Setting it to off ensures that your users are not affected by Secure DNS.

Chrome adds Referrer Chain to Client Side Detection pings

To better protect users, Chrome conducts client-side checks of suspicious websites. In Chrome 91, if Enhanced Protection is enabled, the referrers of the website are also sent to Chrome.

You control this behavior using the SafeBrowsingProtectionLevel enterprise policy.

Download deep scanning available for Enhanced Safe Browsing users

Users who consented to Enhanced Safe Browsing can send downloads to Google for deep scanning when the existing safety checks are inconclusive. You can disable this by controlling the user's Safe Browsing setting via the policy SafeBrowsingProtectionLevel.

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

For users who consented to Enhanced Safe Browsing, who have signed in to their Google accounts, Google Account-tied tokens are added to various phishing detection pings. This provides better protection and reduces false positives.

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

Chrome rollout status is available with the Chrome VersionHistory API

The Chrome VersionHistory API is a web service API for retrieving information about Chrome versions and releases. It may be useful for administrators who want to see which versions of Chrome are currently rolled out, including to which fraction of users, to also see the history of Chrome rollouts.

For more details, see https://developer.chrome.com/docs/versionhistory/.

Chrome can survey users about their experience managing Privacy Sandbox settings

Users who visit the Privacy Sandbox settings page may be asked for their opinion about their experience.

You control if such surveys appear for your users with the MetricsReportingEnabled policy.

Chrome on Android tablets requests the desktop site

Chrome 90 on Android tablets requested the desktop version of websites for some users. This is rolling out to all users in Chrome 91.

BrowserSignIn enterprise policy is available on iOS

Admins can use the BrowserSignIn policy to allow, disable, or force users to sign into Chrome. Chrome 91 extends this policy to iOS. On iOS, you can use this policy to allow or disable user sign-in, but not force users to sign in.

Chrome uses updated table rendering

Chrome 91 updates the way it renders tables on web pages. This change fixes known issues and brings Chrome closer to the behavior of other browsers, so we expect the impact to be minimal. However, you should test important workflows in your environment for unexpected issues. A full explainer is available here.

Chrome no longer accepts server certificates issued by the Camerfirma

Websites that use server certificates issued by the Camerfirma Certification Authority are distrusted in Chrome 91. Affected sites should have already been contacted by Camerfirma and have migration plans in place. Note that this does not affect client certificates, only those used for authentication of TLS servers.

Network state partitioned in Chrome 91

Today, some network objects are shared globally for performance reasons, but this makes it possible to fingerprint users and track them across sites. To protect user privacy, Chrome 91 partitions many network objects by topmost frame domain and iframe domain. A comprehensive description is available here.

No impact is expected other than minor performance changes, but you can test the change in advance by using the command line flag:

```
--enable-features=PartitionConnectionsByNetworkIsolationKey,PartitionExpectCTStateByNetworkIsolationKey,PartitionHttpServerPropertiesByNetworkIsolationKey,PartitionNelAndReportingByNetworkIsolationKey,PartitionSSLSessionsByNetworkIsolationKey,SplitHostCacheByNetworkIsolationKey
```

Legacy Browser Support (LBS) parsing fix reverted in Chrome 91

A fix in LBS was made in M90 that resulted in our rules parsing engine to be more strict and similar to the IE-sitelist rules parsing engine. We have learned, however, that many customers relied on less-strict parsing behavior. Due to the unintended impact, we are reverting the fix for Chromium bug 1176742. Please verify that your LBS rules work in M91 before deployment. In a future release, we will offer a new policy to enable stricter rules parsing.

Chrome OS updates

Nearby Share on Chrome OS

Nearby Share is a platform that provides easy, reliable, and secure file, text, and URL sharing across Chrome OS and Android devices.

VPN before login

Admins can configure built-in VPNs on Chrome OS so that users can connect to a VPN from the login screen. This allows users to authenticate securely via a VPN connection, which is especially helpful for enterprise-hosted single sign-on situations. Built-in VPN support includes L2TP/IPsec and OpenVPN.

Admin Console updates

Pin extensions to the browser toolbar

Admins can now pin Chrome extensions to the browser toolbar from the Apps & Extension Page. We recommend admins test out the feature on a small set of devices and browsers before deploying to their fleet. For more details, see here.

Chrome Insights Report: AUE Report

The Auto Update Expiration (AUE) Chrome Insights Report allows admins to easily see how many Chrome OS devices in their fleet have reached their AUE dates or are expiring soon. Admins can navigate directly to the Device List from the report to view all devices expiring in the time frame selected.

Sending Remote Commands for Chrome Desktop

As an admin, you can use your Google Admin console to remotely send actions to managed Chrome Desktop Browsers (Win/Mac). For example, you can delete browser cache or cookies remotely. For more details on sending commands, see here.

Additional policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
KerberosRememberPasswordEnabled	User & Browser Settings	Chrome OS	Kerberos / Remember Kerberos passwords
KerberosAddAccountsAllowed	User & Browser Settings	Chrome OS	Kerberos / Kerberos accounts
SecurityTokenSessionBehavior	User & Browser Settings; Managed Guest Session Settings	Chrome OS	Security / Security token removal / Action on security token removal (for example, smart card)
SecurityTokenSessionNotificationSeconds	User & Browser Settings; Managed Guest Session Settings	Chrome OS	Security / Security token removal / Removal notification duration (seconds)
WebXRImmersiveArEnabled	User & Browser Settings	Android	Other settings / WebXR "immersive-ar" sessions
SSLErrorOverrideAllowedForOrigins	User & Browser Settings; Managed Guest Session Settings	Chrome Chrome OS Android	Network / SSL error override allowed domains / Domains that allow clicking through SSL warnings
SystemProxySettings	Device Settings	Chrome OS	Other settings / Authenticated Proxy Traffic
DeviceAllowMGSToStoreDisplayProperties	Managed Guest Session Settings	Chrome OS	User experience / Persist display settings

DeviceAllowedBluetoothServices	Device Settings	Chrome OS	Other settings / Bluetooth services allowed / Only allow connection to Bluetooth services in the list
DevicePciPeripheralDataAccessEnabled	Device Settings	Chrome OS	Other settings / Data access protection for peripherals
AccessibilityShortcutsEnabled AutoclickEnabled CaretHighlightEnabled CursorHighlightEnabled DictationEnabled FloatingAccessibilityMenuEnabled HighContrastEnabled KeyboardFocusHighlightEnabled LargeCursorEnabled MonoAudioEnabled PrimaryMouseButtonSwitch ScreenMagnifierType SelectToSpeakEnabled SpokenFeedbackEnabled StickyKeysEnabled VirtualKeyboardEnabled	Device Settings	Chrome OS	Kiosk accessibility

New and updated policies (Chrome and Chrome OS)

Policy	Description
BrowserThemeColor *Browser Only*	Configure the color of the browser's theme
CECPQ2Enabled	CECPQ2 post-quantum key-agreement enabled for TLS
DefaultFileHandlingGuardSetting	Lets web apps ask for access to file types via the File Handling API.
DeviceAllowedBluetoothServices *Chrome OS Only*	Only allow connection to the Bluetooth services in the list
ExplicitlyAllowedNetworkPorts	Permits bypassing the list of restricted ports
FileHandlingAllowedForUrls	Specifies web apps allowed to access file types via the File Handling API.
FileHandlingBlockedForUrls	Specifies web apps blocked from accessing file types via the File Handling API.
ForcedLanguages *Browser Only*	Configure the content and order of preferred languages
HeadlessMode	Control use of the Headless Mode
SharedArrayBufferUnrestrictedAccessAllowed	Specifies whether SharedArrayBuffers can be used in a non cross-origin-isolated context.
SuppressDifferentOriginSubframeDialogs	Specifies if JavaScript dialogs triggered from a different origin subframe will be blocked
URLBlocklist *New on iOS*	Specifies disallowed URLs
URLAllowlist *New on iOS*	Specificies allowed URLs
WebAppSettings *Browser only*	Specifies settings for web apps installed through WebAppInstallForceList **Note:** This is an experimental policy that may be replaced in a future version of Chrome.
WebRtcIPHandling	WebRTC will use TCP on the public-facing interface, and will only use UDP if supported by a configured proxy

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

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.

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. More details can be found on our blog post at blog.chromium.org.

Chrome OS is working on the changes to the release cadence and will send a separate announcement. As always, Chrome OS will prioritize the latest security updates, and maintain a high quality and stable experience for users, customers, partners, and developers.

Upcoming Chrome browser changes

Managed profile sign-in popup will be more clear in Chrome 92

Chrome will update the notice when users sign into a managed profile. The new notice will use clear language and the available actions 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.

SharedArrayBuffers will need Cross-Origin-Opener-Policy and Cross-Origin-Embedder-Policy in Chrome 92

If your organization uses apps that leverage SharedArrayBuffers, those apps will need to set Cross-Origin-Opener-Policy and Cross-Origin-Embedder-Policy in the HTTP header. Web apps not setting the appropriate policies will no longer be able to access SharedArrayBuffers.

If your organization needs additional time to make the transition, the SharedArrayBufferUnrestrictedAccessAllowed policy will be available in Chrome 91. This is a temporary policy that will eventually be removed. The removal timeline will be communicated in future release notes.

Insecure public pages no longer allowed to make requests to private or local URLs in Chrome 92

Insecure pages will no longer be able to make subresource requests to IPs belonging to a more private address space (as defined in Private Network Access). For example, **http**://public.page.example.com will not be able to make requests targeting IP 192.168.0.1 or IP 127.0.0.1. You will be able to control this behavior using the **InsecurePrivateNetworkRequestsAllowed** and **InsecurePrivateNetworkRequestsAllowedForUrls** enterprise policies.

Different-origin iframes will not be able to trigger javascript dialogs in Chrome 92

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 is intended to prevent embedded content from spoofing the user into believing a message is coming from the website they're visiting, or from Chrome itself.

If you have any web apps affected by this change, you'll be able to use the temporary enterprise policy SuppressDifferentOriginSubframeDialogs to revert to the previous behavior. This policy will be removed in Chrome 95.

Chrome will launch a sharing hub in Chrome 92

Users will be able to more easily share their current page in Chrome 92, including the ability to send the current page to their devices, get a QR code for the current URL, screenshot and markup the current page, and share to third party apps.

You'll be able to control this feature using an enterprise policy.

Chrome 92 on iOS will prefer https to http when not specified in the address bar

When a user types an address into the address bar without specifying the protocol, Chrome will attempt to navigate using https first, then fallback to http if https is not available. For example, if the user navigates to example.com, Chrome will first attempt to navigate to **https**://example.com, then fallback to **http**://example.com if required. For more information, see Chrome's blog post, A safer default for navigation: HTTPS.

Desktop and Android users already had this change, and iOS will be rolled out in Chrome 92.

Chrome 92 on Android will introduce the Magic Toolbar

The Chrome toolbar on Android will add a new adaptable button, which will show different shortcuts depending on what the user is most likely to need and will also be customizable.

Chrome 92 will expand DNS HTTPS records queries for users using classic DNS

Chrome is currently querying and parsing DNS HTTPS records alongside the traditional A and AAAA records for users using Secure DNS. From Chrome 92, we will expand this behavior to users using classic DNS. The information from these records will be used to improve privacy and performance of HTTPS web connections. You can temporarily disable these extra queries for users using classic DNS, via the AdditionalDnsQueryTypesEnabled policy with Group Policy or in the Google Admin Console. Please share details about issues that led you to use the policy as a workaround. Note that this policy has no effect for users using Secure DNS.

Lock in address bar will be replaced in Chrome 93

The lock in the address bar will be replaced with a new icon. Chrome is moving to security messaging that highlights known security issues, and shows neutral messaging otherwise. Showing an icon that implies safety based solely on the connection's encryption may lead to a false sense of security.

Network Service on Windows will be sandboxed as early as Chrome 93

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 may leverage MiraclePtr to improve security, as early as Chrome 93

Chrome will leverage MiraclePtr to reduce the risk of security vulnerabilities relating to memory safety. The Chrome team is gathering data on the performance cost of MiraclePtr in Chrome 91, but domain-joined enterprises on the stable channel are excluded from MiraclePtr builds during this phase. A full release of MiraclePtr in Chrome may be as early as Chrome 93.

UserAgentClientHintsEnabled will be removed in Chrome 93

When Chrome introduced User-Agent Client Hints, some servers were not able to accept all characters in the User-Agent Client Hints headers as part of the broader Structured Headers emerging standard.

To give enterprises extra time updating these servers, the UserAgentClientHintsEnabled policy was introduced. This transition period will end with Chrome 93, and the policy will be removed.

SyncXHR policy will no longer be supported on Chrome 93

The AllowSyncXHRInPageDismissal enterprise policy will be removed in Chrome 93. For any apps that rely on the legacy web platform behavior, be sure to update them before Chrome 93. This change was previously planned for Chrome 88, but delayed to provide more time for enterprises to update legacy applications.

LegacySameSiteCookieBehaviorEnabled will be removed in Chrome 93

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 will end in Chrome 93, and LegacySameSiteCookieBehaviorEnabled will no longer take effect. You will still be able to opt specific sites into the legacy cookie behavior using LegacySameSiteCookieBehaviorEnabledForDomainList until Chrome 109.

Chrome 93 will not support Ubuntu 16.04

Ubuntu 16.04 is past the end of standard support, and will not be supported as of Chrome 93. The updated system requirements for Chrome are available here.

Chrome 93 will remove 3DES TLS cipher suites

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

Chrome apps will be deprecated in Chrome 94 on Mac, Windows, and Linux

Chrome apps will no longer function on Mac, Windows, and Linux in Chrome 94, as part of the previously-communicated plan to replace Chrome apps with the open web. 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.

Chrome will maintain its own default root store as early as Chrome 95

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, you should not have to manage multiple root stores. We do not anticipate any changes to 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.

Legacy policies with non-inclusive names will be removed in Chrome 95

Chrome 86 through Chrome 90 introduced new policies to replace policies with less inclusive names (for example, whitelist blacklist). 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 95, and the following policies in the left column 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 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.

Upcoming Admin Console changes

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. You can sign up to get early access to this feature by filling out our Trusted Tester form.