chrome enterprise

M90 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 April 15, 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 90

Chrome Browser updates

Single words are not treated as intranet locations by default

By default, Chrome improves user privacy and reduces load on DNS servers by avoiding DNS lookups for single keywords entered into the address bar. This change may interfere with enterprises that use single-word domains in their intranet. That is, a user typing "helpdesk" is no longer directed to "https://helpdesk/".

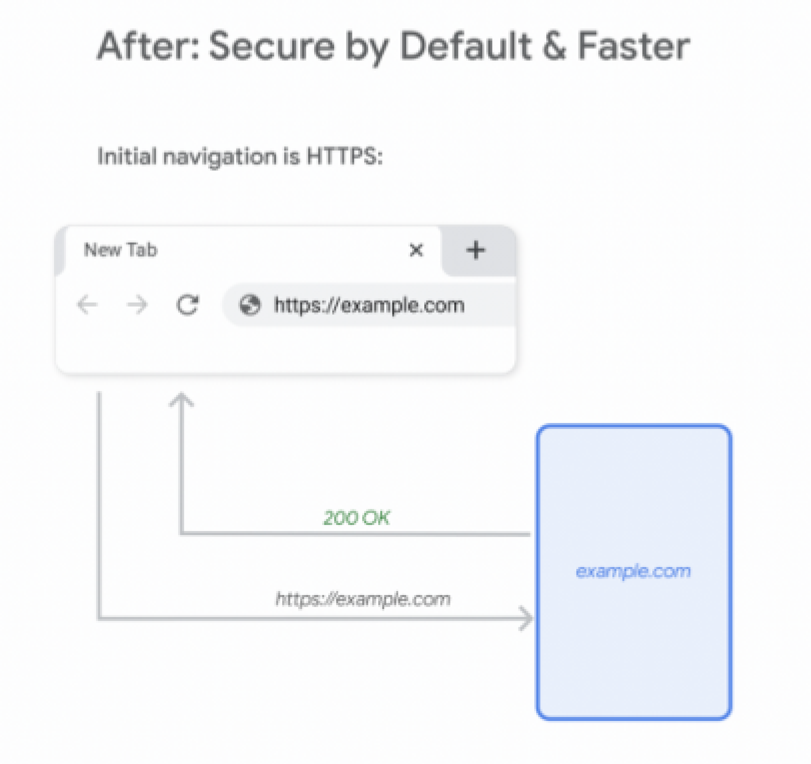
You can control the behavior of Chrome using the IntranetRedirectBehavior enterprise policy, including preserving the existing behavior (**value 3**: Allow DNS interception checks and did-you-mean "http://intranetsite/" infobars.).

Some users saw this change in Chrome 88 and 89; a full rollout is happening in Chrome 90.

Chrome prefers 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 attempts to navigate using **https** first, then falls back to **http** if **https** is not available. For example, if the user navigates to *example.com*, Chrome first attempts to navigate to **https**:*//example.com*, then falls back to **http**:*//example.com* if required. See Chrome's blog post, A safer default for navigation: HTTPS, for more information.

Desktop and Android users see this in Chrome 90, with a release on iOS following soon after.



Chrome blocks port 554 in Chrome 90

Port 554 is added to the restricted ports list, so Chrome blocks traffic through port 554. This should have no effect on customers using standard ports, but custom configurations (for example, delivering PAC scripts) using non-standard ports may be affected. You should instead use standard ports for your use case (for example, delivering PAC scripts via HTTPS through port 443).

The TargetChannel policy allows you to set Chrome's channel

Chrome 90 allows you to choose between stable, beta, and dev channels via the enterprise policy TargetChannel. You can read more about setting the policies for Mac and Windows.

Chrome compresses public HTTPS images

When Chrome Lite mode is enabled, Chrome compresses public HTTPS images to reduce users' data costs, by routing the requests through a Google service. You can control this using the DataCompressionProxyEnabled enterprise policy.

Chrome saves data with Lite videos

To reduce the data-cost and improve the experience of videos on metered and limited data connections, Chrome on Android reduces the effective bitrate of videos for Lite mode users on cellular connection. You can control this feature using the **DataCompressionProxyEnabled** policy.

AllowNativeNotifications updated to AllowSystemNotifications

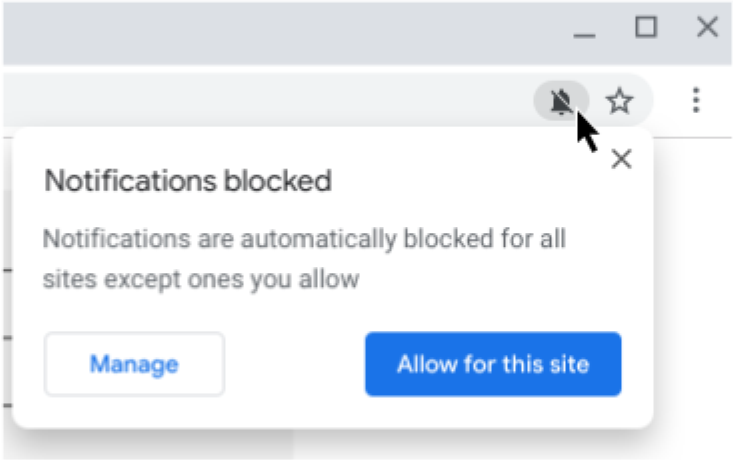
As part of Chrome's move to using more inclusive policy names, **AllowNativeNotifications** is renamed to AllowSystemNotifications. The existing **AllowNativeNotifications** policy will be available until Chrome 95.

Chrome supports Intel CET

Chrome supports Intel's Control Flow Enforcement Technology (CET), known as Hardware-enforced Shadow Stacks on Windows. This only affects Chrome running on hardware that supports CET (Intel 11th Gen or AMD Zen 3). While no issues are expected, you can manage CET by manipulating Image File Execution Options (IFEO) through group policy.

Some permission requests are less intrusive

Permission requests that the user is unlikely to allow are automatically blocked, when Safe Browsing is set to Enhanced. A less intrusive UI allows the user to manage permissions for each site.



Notifications blocked

Notifications are automatically blocked for all sites except ones you allow

You can control this feature on your environment using the SafeBrowsingProtectionLevel enterprise policy. Set it to 1 (standard), 2 (enhanced), or leave the policy unset to enable the quieter requests. Set it to 0 (disabled) to always use the standard requests instead of the quieter requests.

You can also explicitly allow or disable notifications for certain sites using the NotificationsAllowedForUrls and NotificationsBlockedForUrls. This may be better suited for your use case and doesn't require the user to be prompted at all.

Extension settings load from the same place for all channels on Mac

All Chrome channels read the extension policies from the same .plist file. For example, the extension Password Alert always loads its policies from com.google.Chrome.extensions.noondiphcddnnabmjcihcjfbhfklnnep.plist instead of com.google.Chrome.canary.extensions.noondiphcddnnabmjcihcjfbhfklnnep.plist in Chrome Canary.

Security key enterprise attestation

Chrome supports device-unique attestation of security keys without needing a policy configured. This is useful in situations where security keys are distributed by an enterprise to personnel who may use them on non-policy-managed computers. This requires specially-manufactured security keys—talk to your security key vendor if this sounds useful.

WebXR depth sensing API will be supported

The WebXR Depth Sensing API allows Chrome to measure distance from the user's device to real world geometry in the user's environment. With this, Chrome will be able to power immersive experiences in WebXR-powered apps (for example, for physics, and lifelike occlusion for augmented reality).

You will be able to control access to WebXR and other augmented reality APIs using the WebXRImmersiveArEnabled enterprise policy.

Admin controls on shutdown delay for fetch keepalive

When Chrome is closed, any outstanding fetch keepalive requests are cancelled by default. In Chrome 90, you can use the FetchKeepaliveDurationSecondsOnShutdown enterprise policy to block browser shutdown for a specified period of time to serve any outstanding fetch keepalive requests.

This may be suitable for enterprise web applications that require the fetch keepalive requests to signal the end of a user session.

Legacy browser support works between Chrome and Microsoft Edge

You can configure Legacy Browser Support to automatically switch between multiple browsers, assigning certain sites to always open in Chrome, while other sites always open in another browser, for example, Internet Explorer. With Chrome 90, we now support configuring your environment to switch between Chrome and Microsoft Edge in IE mode. See this help center article for more details.

Chrome on Android tablets requests the desktop site

Chrome 90 on Android tablets requests the desktop version of websites for some users. This is expected to be rolled out to all users in Chrome 91.

Chrome OS updates

Deprecation of AMR and GSM audio codecs

AMR-NB, AMR-WB, and GSM audio codecs are deprecated as part of this release. Affected users should file bugs here and may temporarily rollback this change via the use of chrome://flags/#deprecate-low-usage-codecs. Users with long-term need for these codecs may use stand-alone applications found in the Google Play Store.

New Diagnostics app

The new Diagnostics app helps users understand how their Chrome OS device [battery, CPU, and memory] is performing. Within the app, users can also run troubleshooting tests – results are saved in a session log file for easy sharing with customer support.

Device Dock Update

Device updates provide users the ability to have reliable and safe peripherals, by providing an avenue to update their software if needed. In Chrome OS 90, we are releasing a path for updates to docks with minimal user experience disruption, making it simple and safe for all our users that use Works With Chromebook certified accessories.

Updated UI for recent screenshots and downloads

Quickly access your recent screenshots and downloads. Pin your important Files to launch, copy, or drag with one click. Visit here for more information.

Better account manager and add account flow

Chrome OS's account manager is getting a brand new design to help users better understand the Chrome OS identity model, such as the difference between device account and secondary Google Accounts, and the implications of adding multiple Google Accounts to a user session. Instead of being nested under the "People" section, the redesigned account manager is part of a new "Accounts" section for clarity and ease of access. Finally, the add account flow is also redesigned to help nudge users away from adding their Google Accounts to user sessions that are not their own.

Add Live captions settings to Chrome OS settings

Chrome Live Caption now supports Chrome OS. Live Captions enables you to caption any audio or video in your browser.

YouTube and Maps open in standalone windows for new users

New users can now experience YouTube and Maps in standalone app windows by default, rather than opening as browser tabs. Existing users can right-click on the YouTube or Maps app icon, then select **Open link in new tab** or **Open link in new window.**

Files app: Enable offline for Docs, Sheets, and Slides files on Drive

Users now have the ability to make Google Docs, Sheets, and Slides available for offline access directly from their Drive folder in the Chrome OS file manager.

Admin console updates

Chrome Policy API

The Chrome Policy API is a brand new API for configuring Admin console Chrome policies. Admins can use the API to script changes across multiple OUs, compare policies or copy policies across multiple OUs, and more. The Chrome Policy API is now available with support for user & browser settings, as well as printer settings. Future versions of the API will also support managing apps & extensions, device settings, kiosk, and managed guest session settings.

Update Controls for macOS

Admin Console now supports configuring update controls for macOS. Please see the Help Center article on how to configure these settings.

Version History API

The Chrome Update team released a web service API for retrieving information about Chrome versions and releases.

Additional policies in the Admin console

Many new policies are available in the Admin console, including:

Policy Name	Pages	Supported on	Category/Field
BasicAuthOverHttpEnabled	User & Browser Settings	Chrome OS, Windows, Mac, Linux	Network / Allow Basic authentication for HTTP
BrowserLabsEnabled	User & Browser Settings	Windows, Mac, Linux	User experience / Browser experiments icon in toolbar
DefaultSensorsSetting	User & Browser Settings; Managed Guest Session Settings	Chrome OS, Windows, Mac, Linux, Android	Hardware / Sensors / Default access
EnableDeprecatedPrivetPrinting	User & Browser Settings; Managed Guest Session Settings	Chrome OS, Windows, Mac, Linux	Printing / Deprecated privet printing
FullscreenAlertEnabled	User & Browser Settings	Chrome OS	User experience / Fullscreen alert
IntegratedWebAuthenticationAllowed	User & Browser Settings	Chrome OS	Network / Login credentials for network authentication
NTPCardsVisible	User & Browser Settings	Chrome OS, Windows, Mac, Linux	User experience / Show cards on the New Tab Page
PhoneHubAllowed	User & Browser Settings	Chrome OS	Connected devices / Phone Hub

PhoneHubNotificationsAllowed	User & Browser Settings	Chrome OS	Connected devices / Phone Hub
PhoneHubTaskContinuationAllowed	User & Browser Settings	Chrome OS	Connected devices / Phone Hub
ProfilePickerOnStartupAvailability	User & Browser Settings	Windows, Mac, Linux	Startup / Profile picker availability on browser startup
RemoteAccessHostDomainList	User & Browser Settings; Managed Guest Session Settings	Chrome OS, Windows, Mac, Linux	Remote access / Remote access hosts / Remote access host domain
SensorsAllowedForUrls	User & Browser Settings; Managed Guest Session Settings	Chrome OS, Windows, Mac, Linux, Android	Hardware / Sensors / Allow access to sensors on these sites
SensorsBlockedForUrls	User & Browser Settings; Managed Guest Session Settings	Chrome OS, Windows, Mac, Linux, Android	Hardware / Sensors / Block access to sensors on these sites
SigninInterceptionEnabled	User & Browser Settings	Windows, Mac, Linux	Sign-in settings / Signin interception
TargetBlankImpliesNoOpener	User & Browser Settings; Managed Guest Session Settings	Chrome OS, Windows, Mac, Linux, Android	Security / Popup interactions
WifiSyncAndroidAllowed	User & Browser Settings	Chrome OS	Other settings / Wi-Fi network configurations sync

New and updated policies (Chrome Browser and Chrome OS)

Policy	Description
AllowSystemNotifications Linux Only	Allow system notifications
AudioProcessHighPriorityEnabled Windows Only	Allow the audio process to run with priority above normal on Windows
FetchKeepaliveDurationSecondsOnShutdown	Fetch keepalive duration on Shutdown
SSLErrorOverrideAllowedForOrigins	Allow proceeding from the SSL warning page on specific origins
WebXRImmersiveArEnabled Android	Allow creating WebXR's "immersive-ar" sessions
WindowOcclusionEnabled Browser only	Enable Window Occlusion

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 switch Chrome 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 also planning changes to the release cycle during the same release. 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

Chrome 91 will block port 10080 and add a policy for allowing specific ports

Port 10080 will be added to the restricted ports list and traffic will be blocked through it. This should have no effect on customers using standard ports, but custom configurations using non-standard ports may be affected.

If you're affected by this change, or other changes blocking ports for security reasons, Chrome will introduce an enterprise policy where you can allow specific ports in your environment.

Collapsed tab groups will be frozen in Chrome 91

Chrome allows users to group tabs into collapsible groups, helping them stay organized and productive. In Chrome 91, those tabs will be frozen when the user collapses them, freeing up resources on the system. Chrome will not freeze 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.

Web apps will be able to run when the user logs into the OS in Chrome 91

Users will be able to configure Progressive Web Apps to start automatically when they log into the OS. This allows some apps that the user expects to be always-on to behave as expected.

You will be able to control which apps can start on OS login using the WebAppSettings enterprise policy.

Chrome will introduce initial_preferences in Chrome 91

As part of Chrome's move to using more inclusive naming, Chrome will support an admin using a file to control the browser's initial preferences, 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, master_preferences will continue to be supported in Chrome 90 and more notice will be given before support for master_preferences is removed.

Different-origin iframes will not be able to trigger javascript dialogs in Chrome 91

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 94.

You can test apps in your environment for compatibility using Chrome 91 Canary, and Chrome 91 Beta on April 22.

Network state will be partitioned in Chrome 91

At present, 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 will partition 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
```

The BrowserSignIn enterprise policy will be available for Chrome 91 on iOS

The BrowserSignIn policy allows you to either disable or force users to sign into Chrome browser. The IncognitoModeAvailability policy allows you to disable Incognito mode. Both of these policies will be available for Chrome 90 on iOS.

Quantum computer resistant security will be enabled in Chrome 91

Chrome will start supporting 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 will fit in a single network frame.

The **CECPQ2Enabled** policy can be set to disable this. It will also be disabled if the ChromeVariations policy is set to a non-default value.

For more details on this rollout, see https://www.chromium.org/cecpq2

The SSLVersionMin policy will not allow TLS 1.0 or TLS 1.1 in Chrome 91

The SSLVersionMin enterprise policy allows you to bypass Chrome's interstitial warnings for legacy versions of TLS. This will be possible until Chrome 91 (May 2021), then the policy will no longer allow TLS 1.0 or TLS 1.1 to be set as the minimum.

We previously communicated that this would happen as early as January 2021, but the deadline has since been extended.

Server certificates issued by the Camerfirma will no longer be accepted, no later than Chrome 91.

Websites that use server certificates issued by the Camerfirma Certification Authority will be distrusted in a future release of Chrome. Affected sites should have already been contacted by Camerfirma and have migration underway. Note that this does not affect client certificates, only those used for authentication of TLS servers.

Chrome 91 on iOS will warn 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. In Chrome 91, this feature will be expanded to Chrome on iOS.

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

Chrome 91 will use updated table rendering

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

You can enable the new rendering behavior using *chrome://flags/#enable-table-ng* in Chrome 90 and above. If you experience any unexpected issues when testing with the flag enabled, please file a chromium bug.

Managed profile sign-in popup will be more clear, with changes as early as Chrome 91

Chrome will update the notice when users sign into a managed profile. The new notice has more clear language and the available actions have been simplified. Some users will see a link to open Chrome in guest mode when they sign into a new profile that's different from the profile signed into Chrome.

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 requests to IPs belonging to a more private address space (as defined in CORS-RFC1918). 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.

Lock in address bar will be replaced in Chrome 92

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.

The Network Service on Windows will be sandboxed as early as Chrome 92.

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

Chrome will leverage MiraclePtr to reduce the risk of security vulnerabilities related to memory safety. The Chrome team is gathering data on the performance cost of MiraclePtr in Chrome 91, but 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.

Chrome will maintain its own default root store as early as Chrome 92

In order 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.

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.

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 be ending 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 97.

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). In order 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 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.

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/Linux). For example, you will be able to delete browser cache or cookies remotely.