chrome enterprise

M92 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 July 20, 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 92

Chrome browser updates

Chrome blocks ports 989 and 990

Chrome 92 adds ports 989 (ftps-data) and 990 (ftps) to the restricted ports list and blocks traffic through them. 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, you can use the ExplicitlyAllowedNetworkPorts enterprise policy to allow these specific ports in your environment. You can specifically allow ports 989 and 990 until February 2022.

Chrome adds FLoC controls to Privacy Sandbox settings

Last year, we announced a new initiative (known as Privacy Sandbox) to develop a set of open standards to fundamentally enhance privacy on the web. Chrome 92 adds controls to the Privacy Sandbox settings page to provide improved transparency and control for FLoC. You can disable the complete Privacy Sandbox (including FLoC) by policy in general by blocking 3P cookies, or all cookies. Alternatively for specific sites, you can disable the sandbox by blocking cookies for a URL.

Chrome on Android includes a new on-device model for phishing detection

Chrome on Android uses an on-device Machine Language (ML) model to better detect phishing attempts, and better protect users. As in earlier versions, Chrome displays a full-page interstitial warning if Chrome detects a possible phishing attempt.

With this change, Chrome sends the following to the Safe Browsing service:

- the version of the model that was executed
- the scores the model gave for each category
- a boolean describing whether the new model was used to generate the scores

You can control Safe Browsing using the SafeBrowsingProtectionLevel policy. This feature applies to users with the **SafeBrowsingProtectionLevel** policy set at protection level of 1 or greater.

Back/forward cache desktop full launch for all websites

As a follow-up to a previous launch on Chrome for Android, Chrome 92 launches back/forward cache on desktop platforms. Back/forward cache is a browser optimization that enables instant back and forward navigations. You can temporarily disable this feature via the BackForwardCacheEnabled policy with Group Policy or in the Google Admin console. If you do so, please share details about the issue that led you to disable back/forward cache.

Magic Toolbar is now available on Chrome on Android

The Chrome toolbar on Android now includes a new customizable button that shows different shortcuts depending on what the user is most likely to need.

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 *prior* to 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.

Chrome expands DNS HTTPS record queries for users using classic DNS

In previous versions, Chrome only queried and parsed DNS HTTPS records alongside the traditional A and AAAA records for users using Secure DNS. Chrome 92 expands this behavior to users using classic DNS. Chrome uses these records to improve privacy and performance of HTTPS web connections. You can temporarily disable these extra queries for users using classic DNS with the AdditionalDnsQueryTypesEnabled policy with Group Policy or in the Google Admin console. If you do so, 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.

Different-origin iframes cannot trigger JavaScript dialogs

Chrome 92 prevents 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 can use the temporary enterprise policy SuppressDifferentOriginSubframeDialogs to revert to the previous behavior. This policy will be removed in Chrome 95.

SharedArrayBuffers need Cross-Origin-Opener-Policy and Cross-Origin-Embedder-Policy

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

Android removes setting for “Show suggestions for similar pages”

Chrome 92 on Android removes the end user setting for "Show suggestions for similar pages when a page can't be found" from the Sync and Google services settings. This setting was previously removed on Desktop.

You can control the DNS probes associated with this feature with the AlternateErrorPagesEnabled enterprise policy.

Drive priority launchpad on New Tab page

To help users get work done faster, Chrome 92 shows the Drive docs 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 drive.google.com. Some users see this change in Chrome 92 and a full launch is expected in Chrome 93.

Developers can change the name and icons of PWAs

Developers can now update the name and icon for default Progressive Web Apps (PWAs) and PWAs installed using the ExtensionInstallForcelist enterprise policy.

Chrome trials the suppression of autofill suggestions

In Chrome 92, we are conducting a short trial on a small randomly selected number of forms where the browser doesn't show autofill suggestions. The trial is limited to address and credit card forms. Passwords are not affected. You can opt out by using the ChromeVariations policy. Setting the policy to **CriticalFixesOnly** (value 1) allows only variations considered critical security or stability fixed to be applied to Google Chrome.

Google Lens replaces Search by Image on Chrome Desktop

In Chrome 92, for Chrome users whose default search engine is set to Google, the **Search with Google Lens** context menu item replaces the Search Google for Image desktop context menu item. The new menu item sends users to a standalone Lens Web app. If desired, however, users can navigate to Google Image Search from Lens.

Chrome separates sign-in and sync on iOS

On iOS, Chrome 92 separates the Sync and Google services settings into two items: Sync and Google services. There is a new control in Google services, Allow Chrome sign-in, to disable Chrome sign-in (and therefore also sync).

Chrome displays a new warning text if a download might lead to account compromise

If a user initiates a download that Safe Browsing determined is associated with stealing cookies, some users on desktop platforms see a new warning, **filename.exe could let attackers steal your personal information**.

Incognito removes UI links to history

Chrome does not save history in Incognito mode, but some platforms still show a link to history on the Incognito UI. On Android, to make it clear that Chrome is not saving history, the **History** menu item in Incognito windows temporarily links to an explainer page instead of linking to a user's history.

Chrome disables extensions removed from the Chrome Web Store

Chrome disables extensions that were removed from the Chrome Web Store due to non-compliance with our Chrome Web Store policies. However, if an admin has force-installed an extension, Chrome does not disable it.

Remember, if you need help with an extension that you manage, you can visit Chrome Web Store One Stop Support.

Chrome OS updates

Chrome improves Android and Linux app support for Desks

http://crbug/1203496

You can now assign Android and Linux apps to desks. Right-click on the app window to assign it to a specific desk or to all desks.

Chrome supports continuous dictation

http://crbug/1200667

Dictation now allows you to continuously dictate your text and only times out if you stop talking.

Point Scanning for Switch Access

http://crbug/1167368

Point Scanning is a new navigation mode for Switch Access. It allows users to select any spot on the screen and trigger an action. The user first presses their switch when the correct horizontal position is selected, and presses their switch again when the correct vertical position is selected.

Chrome adds further integrations to Tote

http://crbug/1201265

You can now quickly find downloads from your Android Apps and from your Chrome print to pdf functionality in Tote.

MultiPaste now available for Virtual Keyboard

http://crbug/1175122

Chrome OS makes its clipboard history, which launched in Chrome OS 89, accessible from the Virtual Keyboard in Chrome OS 91 and later.

Chrome 92 improves shortcuts for international keyboards

http://crbug/1159454

Chrome OS improves keyboard shortcuts for both international and US users; you can see these updates in the Shortcuts app.

Chrome OS Camera now supports PTZ Controls

http://crbug/1186787

You can now pan, tilt, or zoom your camera from the Chrome Camera app. This feature requires a camera with PTZ support.

Emoji picker for physical keyboards

http://crbug/1152237

Chrome OS includes a new emoji picker, with search functionality and multi-skintone support.

Chrome OS device help in launcher search

http://crbug/1126816

Quickly find help for your Chrome OS device by searching for it in launcher search.

Some protected content may no longer play on M89 and earlier

https://support.google.com/chrome/a/answer/9813310

From August 3rd, some protected video and audio content may no longer play on M89 and earlier.

Admin console updates

Additional policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
SystemFeaturesDisableMode	Managed Guest Session Settings	Chrome OS	User experience / Disabled system features visibility
SuppressDifferentOriginSubframeDialogs	User & Browser Settings; Managed Guest Session Settings	Chrome Chrome OS Android	Content / Cross-origin JavaScript dialogs
EnterpriseHardwarePlatformAPIEnabled	User & Browser Settings; Managed Guest Session Settings	Chrome Chrome OS Android	Hardware / Enterprise Hardware Platform API
LensCameraAssistedSearchEnabled	User & Browser Settings	Android	User experience / Google Lens camera assisted search
NearbyShareAllowed	User & Browser Settings	Chrome OS	Connected devices / Nearby share
SharedArrayBufferUnrestrictedAccessAllowed	User & Browser Settings; Managed Guest Session Settings	Chrome Chrome OS	Network / SharedArrayBuffer

WebRtcIPHandling	User & Browser Settings; Managed Guest Session Settings	Chrome Chrome OS	Network / WebRTC IP handling
FetchKeepaliveDurationSecondsOnShutdown	User & Browser Settings	Chrome	Power and shutdown / Keepalive duration / Fetch keepalive duration on Shutdown (in seconds)
CECPQ2Enabled	User & Browser Settings; Managed Guest Session Settings	Chrome Chrome OS Android	Network / CECPQ2 post-quantum key-agreement for TLS
AudioProcessHighPriorityEnabled	User & Browser Settings	Chrome	Hardware / Audio process priority / Adjust the priority for the Chrome audio process
ExplicitlyAllowedNetworkPorts	User & Browser Settings; Managed Guest Session Settings	Chrome Chrome OS Android	Network / Allowed network ports
AllowSystemNotifications	User & Browser Settings	Chrome	Security / System notifications
DefaultFileHandlingGuardSetting	User & Browser Settings; Managed Guest Session Settings	Chrome Chrome OS	Content / File Handling API
FileHandlingBlockedForUrls	User & Browser Settings; Managed Guest Session Settings	Chrome Chrome OS	Content / File Handling API / Block the File Handling API for these URLs

FileHandlingAllowedForUrls	User & Browser Settings; Managed Guest Session Settings	Chrome Chrome OS	Content / File Handling API / Allow the File Handling API for these URLs
BrowserThemeColor	User & Browser Settings	Chrome	General / Custom theme color / Hex color
PdfAnnotationsEnabled	User & Browser Settings	Chrome OS	Content / PDF Annotations
DeviceSystemWideTracingEnabled	Device Settings	Chrome OS	User and device reporting / System-wide performance trace collection
GaiaOfflineSigninTimeLimitDays	User Settings	Chrome OS	Security/Google online login frequency

New and updated policies (Chrome and Chrome OS)

Policy	Description
InsecurePrivateNetworkRequestsAllowed	Controls whether insecure websites are allowed to make requests to any network endpoint, subject to other cross-origin checks.
CloudUserPolicyMerge	Allows policies associated with a Google Workspace account to be merged into machine-level policies.
GaiaLockScreenOfflineSigninTimeLimitDays	Limit the time for which a user authenticated via GAIA without SAML can log in offline at the lock screen.
SamlLockScreenOfflineSigninTimeLimitDays	Limit the time for which a user authenticated via SAML can log in offline at the lock screen.
AdditionalDnsQueryTypesEnabled	Allow DNS queries for additional DNS record types.

PromptForDownloadLocation	Ask where to save each file before downloading.
DataLeakPreventionReportingEnabled	Enable data leak prevention reporting.
DataLeakPreventionRulesList	Sets a list of data leak prevention rules.
DeviceDebugPacketCaptureAllowed	Allow debug network packet captures.
SuggestLogoutAfterClosingLastWindow	Display the logout confirmation dialog.
TripleDESEnabled	Enable 3DES cipher suites in TLS.

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. 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. You can find more details on 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

Chrome 93 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. Similarly, **http**://intranet.example served on IP 192.168.0.1 will not be able to make requests targeting localhost. You can control this behavior using the InsecurePrivateNetworkRequestsAllowed and InsecurePrivateNetworkRequestsAllowedForUrls enterprise policies, which are available for testing in Chrome 92.

Chrome 93 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 93, 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.

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

Chrome 93 will add 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. Before 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)) will now be useful.

Chrome 93 will support using 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 have 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 93 will use updated language in managed profile sign-in notice

Chrome 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 93 will test replacing the lock icon with a new icon

Some users will see a new icon replacing the lock in the address bar, improving the discoverability of the Page Info surface, which includes site-level security and privacy information and controls. An enterprise policy, **LockIconInAddressBarEnabled,** will become available to revert to the original lock icon.

Chrome 93 will launch a sharing hub

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 93 will make Chrome Browser Cloud Management available on iOS

The enterprise team is working to support Chrome-on-iOS for Chrome Browser Cloud Management. If you are interested in testing this functionality out earlier in Chrome 92, please sign up for our Trusted Tester program.

Chrome 93 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.

As early as Chrome 94, 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. 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 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 93 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 have this change, and iOS will be rolled out in Chrome 93.

Chrome 93 on iOS will add 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 93 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 93 will introduce JavaScript JIT setting policies

Chrome 93 will introduce three new policies;

- **DefaultJavaScriptJitSetting**
- **JavaScriptJitAllowedForSites**
- **JavaScriptJitBlockedForSites**

These policies will allow you to switch Chrome's JavaScript engine to use the Ignition interpreter in a JIT-less mode, by default.

Disabling 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 disables some parts of JavaScript, including WebAssembly.

Chrome 93 will no longer support SyncXHR policy

Chrome 93 will remove the AllowSyncXHRInPageDismissal enterprise policy. Admins must update any apps that rely on the legacy web platform behavior before Chrome 93. This change was previously planned for Chrome 88, but delayed to provide more time for enterprises to update legacy applications.

Chrome 93 will remove LegacySameSiteCookieBehaviorEnabled

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 December 31st, 2022.

Chrome 93 will no longer 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 94 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®.

As early as Chrome 94, 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 94.

In Chrome 94, 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.

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.

As early as Chrome 95, 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 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.

Chrome 95 will remove legacy policies with non-inclusive names

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.