chrome enterprise

Chrome 94 Enterprise release notes

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

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 September 21, 2021.

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

Chrome 94

Chrome browser updates

Chrome moves to a 4-week stable channel and introduces an 8-week extended stable channel

Chrome on mobile, Windows, Mac, and Linux moves from its 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 can use the existing TargetChannel policy to switch Chrome on Mac and Windows to an extended stable channel, with a new major release every 8 weeks instead. You can find more details in our help center article. **Note:** If you decide to move to the extended stable channel, we recommend testing it out on a small set of machines or organizational units before deploying it on your entire fleet. Extended Stable is identical to Stable for the first 4 weeks of each cycle, so this sort of testing is most valuable in the last 4 weeks of the Extended Stable cycle.

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).

Chrome on iOS can 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 on iOS now allows users to download these files. Users then have to manually install the profile from the *Settings* app.

Chrome deprecates WebSQL in third-party contexts

Chrome 94 no longer uses WebSQL in third-party contexts, such as cross-origin iframes. A console message is printed each time a WebSQL database opens in a third-party context to alert developers of the upcoming removal. This change does not affect WebSQL in first-party contexts, but the eventual goal is to deprecate and remove all WebSQL.

WebSQL in third-party contexts will be disabled in Chrome 97, but an enterprise policy will be made available to re-enable it. As of Chrome 101, WebSQL in third-party contexts will be removed entirely.

Chrome launches HTTPS-First mode (Android and desktop)

HTTPS-First mode attempts to upgrade all page loads to HTTPS and displays 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. Users see a warning before connecting to sites over HTTP.

An enterprise policy, **HttpsOnlyMode**, is available to control the use of this mode.

Chrome blocks the MK external protocol

Chrome now blocks the legacy external MK protocol for use with Internet Explorer. This protocol enables legacy web apps to extract information from compressed files. This is a legacy asynchronous pluggable protocol that is disabled by default in Internet Explorer. Chrome now blocks this protocol to mitigate potential malicious use.

Chrome / Citrix Workspace (self-service plugin) stability

Recent versions of Citrix Workspace install a DLL on Windows that can interfere with the Chrome browser process. Only Windows 10 or 11 systems with Control-flow Enforcement Technology (CET) or Hardware-enforced Stack Protection (Intel 11th Gen and AMD Zen 3 CPUs) with Citrix Workspace installed and Client Protection enabled are affected. While we are working with Citrix to resolve this, please consider using Citrix Workspace with Client Protection Disabled as a temporary workaround.

Chrome no longer allows insecure public pages to make requests to private or local URLs

Non-secure contexts served from public IP addresses can no longer make subresource requests to IP addresses belonging to private and local IP addresses (as defined in Private Network Access). For example, **http**://public.example served on IP 1.2.3.4 cannot make requests targeting IP 192.168.0.1 or IP 127.0.0.1. You can control this behavior using the InsecurePrivateNetworkRequestsAllowed or

InsecurePrivateNetworkRequestsAllowedForUrls enterprise policies, which became available for testing in Chrome 92. See this blog post for more details.

PWAs can register as (platform level) URL handlers

Chrome 94 runs 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 can 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.

Chrome sync ends support for Chrome 48 and earlier

Chrome sync no longer supports Chrome 48 and earlier. You need to upgrade to a more recent version of Chrome if you want to continue using Chrome sync.

Chrome launches a sharing hub

In Chrome 94, users can more easily share their current page, including **Send to your devices**, get a QR code for the current URL, and share to third-party websites. The option to **Send to your devices** is only available to signed-in users. If the user is not signed in, the option does not appear. You can control this feature using an enterprise policy called DesktopSharingHubEnabled.

Admins can enforce profile separation through enterprise policy

Chrome 94 updates the dialog when users sign into a managed profile if the ManagedAccountsSigninRestriction policy is set. The new notice clarifies that a separate profile is required by the admin, and the choices for the user are simplified. Some users 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.

New enterprise policies for the Web Serial API

The Web Serial API allows websites to request access to serial devices (USB, Bluetooth, etc.) through a device selection prompt. In previous Chrome versions, policies could only control how the feature was blocked. In Chrome 94, SerialAllowAllPortsForUrls and SerialAllowUsbDevicesForUrls allow admins to grant a website 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 is available starting with Chrome 94.

Chrome updates Certificate Transparency log list via Component Updater

Chrome 94 uses Component Updater to dynamically update the Certificate Transparency log list, separating these updates from full browser updates. This allows out-of-date clients to keep enforcing Certificate Transparency. Note that full browser updates still contain the transparency log list.

Chrome introduces tab grid bulk actions

Chrome for iOS adds an edit mode to the tab grid to allow easier management of open tabs. Users can select multiple tabs and then add them to the reading list, bookmarked, shared, or closed.

New onboarding experience for Chrome on iOS

Chrome 94 revamps the existing onboarding screens, separating the sign-up and sync features.

Chrome removes the 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. Chrome 94 removes this policy.

Chrome launches an API that allows sites to know when the user is active

Chrome 94 launches the Idle Detection API, allowing websites to request to know 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 launches display-capture

The display-capture permissions-policy allows sites to more safely embed documents in an iframe. It does so by controlling such documents' access to screen-capture APIs. This permissions-policy's default setting prevents screen-capture by cross-origin iframes. For websites that are non-compliant with the spec and need more time to implement the display-capture feature, an enterprise policy, named **DisplayCapturePermissionsPolicyEnabled**, allows selective bypassing of the display-capture permissions-policy. This enterprise policy will be removed after Chrome 100.

BeyondCorp Enterprise: custom warnings and bypass justifications

Today BeyondCorp Enterprise shows generic, predefined warn and block messages when files are flagged due to DLP Rule violations or other Chrome Security events. Chrome 94 introduces the ability to provide more meaningful, customized warning messages to end users. Administrators can now customize these warning messages to make it meaningful, and also add a *learn more* link to such warnings.

Chrome launches *What's New in Chrome*

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

New and updated policies in Chrome browser

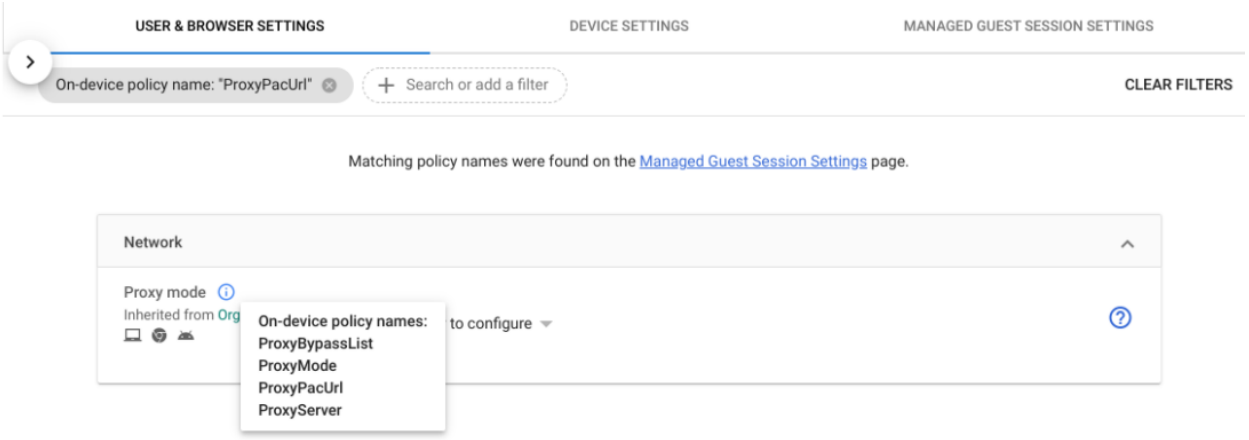
Policy	Description
CrossOriginWebAssemblyModuleSharingEnabled	Specifies whether WebAssembly modules can be sent to another window or worker cross-origin. Cross-origin WebAssembly module sharing will be deprecated as part of the efforts to deprecate document.domain, see https://github.com/mikewest/deprecating-document-domain. This policy allows admins to re-enable cross-origin WebAssembly module sharing to offer a longer transition period in the deprecation process.
DisplayCapturePermissionsPolicyEnabled	The display-capture permissions-policy gates access to getDisplayMedia(), as per this spec: https://www.w3.org/TR/screen-capture/#feature-policy-integration. However, if this policy is Disabled, this requirement is not enforced, and getDisplayMedia() is allowed from contexts that would otherwise be forbidden. This Enterprise policy is temporary; it's intended to be removed after Google Chrome version 100. It is intended to unblock Enterprise users whose application is non-spec compliant, but needs time to be fixed.
HttpsOnlyMode	Controls whether users can enable HTTPS-Only Mode in Settings. HTTPS-Only Mode upgrades all navigations to HTTPS.
LensRegionSearchEnabled	Leaving this policy unset or setting it to Enabled allows users to view and use the Google Lens region search menu item in the context menu.
ManagedAccountsSigninRestriction	Controls whether a managed account must be a primary account.
PrintPdfAsImageAvailability	Controls how Google Chrome makes the Print as image option available on Microsoft Windows and macOS when printing PDFs.
PrintRasterizePdfDpi	Controls print image resolution when Google Chrome prints PDFs with rasterization.

SameOriginTabCaptureAllowedByOrigins	Lets you set a list of URL patterns that can capture tabs with their same Origin.
ScreenCaptureAllowedByOrigins	Lets you set a list of URL patterns that can use Desktop, Window, and Tab Capture.
SerialAllowAllPortsForUrls	Allows you to list sites which are automatically granted permission to access all available serial ports.
SerialAllowUsbDevicesForUrls	Allows you to list sites which are automatically granted permission to access USB serial devices with vendor and product IDs matching the vendor_id and product_id fields. Omitting the product_id field allows the given sites permission to access devices with a vendor ID matching the vendor_id field and any product ID.
TabCaptureAllowedByOrigins	Lets you set a list of URL patterns that can use Tab Capture.
WindowCaptureAllowedByOrigins	Lets you set a list of URL patterns that can use Window and Tab Capture.

Admin console updates

Search by on-device policy name in the Admin console

Chrome 94 adds the ability to search by on-device policy name to the Admin console. Now when admins enter an on-device policy name, for example, ProxyPacUrl, into the search bar, they'll see the corresponding setting, for example, Proxy mode, in the Admin console. Admins can also use new info bubbles that appear next to a setting name to see the corresponding on-device policy name.



New channel option Extended Stable for Chrome Browser Cloud Management

Chrome adds Extended Stable as a drop-down option for channel selection in the **Chrome update** section.

New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
DesktopSharingHub Enabled	User & Browser Settings	Chrome Win/Mac/Linux	Content/Desktop sharing in the omnibox and 3-dot menu

Coming soon

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

Upcoming Chrome browser changes

Chrome 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.

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 who have never changed their setting to the new default (off).

Chrome 96 will add new security events to BeyondCorp Enterprise Threat and Data Protection (Password leak and login)

Chrome 96 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.

Migrate to Open Screen Library Cast channel

Chrome 96 will use a new implementation, Open Screen Library, 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.

NewTabPageLocation enterprise policy on Incognito

Chrome 96 will fix a bug that prevents users from starting new Incognito sessions when the enterprise policy NewTabPageLocation is set to a *chrome://…* URL. In future, this policy will be ignored in Incognito mode. Users on Incognito will see the default new tab page. There's no change in how the policy is applied on regular mode (non-Incognito windows).

As early as Chrome 97, 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 97, it will no longer be possible to bypass the interstitial.

CORS Authorization mishandling

When scripts make a cross-origin network request via fetch() and XMLHttpRequest with an Authorization header, the header should be explicitly allowed by the Access-Control-Allow-Headers header in the CORS preflight response. The wildcard symbol (*) in the Access-Control-Allow-Headers should not work. This has not been implemented correctly, and the wildcard symbol has taken effect. This will be fixed in Chrome 97.

Please note that Authorization headers attached by Chrome during the authentication process are out of scope for this change.

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.

In Chrome 98, 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 98. For enterprises that need extra time to adjust to the removal of Chrome apps, a policy called **ChromeAppEnabled** will be available to extend support for them until June 2022.

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. Once this deprecation launches, you can control the behavior with the enterprise policy **SuppressDifferentOriginSubframeDialogs**.

You can test if this future change will affect applications now by setting the *enable_features=SuppressDifferentOriginSubframeJSDialogs* flag.

Upcoming Admin console changes

Browser list data will be available for download in CSV format in the Admin console

As early as Chrome 95, a CSV format will be introduced as an option to download the browser list data from the Admin console.

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, as early as chrome 95, 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 (Allowable range: 28 - 730 days).