Chrome 95 Enterprise release notes

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

These Chrome 95 release notes contain Chrome Browser updates only. To bridge the gap between Chrome 94 and Chrome 96, Chrome OS will skip Chrome 95 and will include all relevant security fixes on the Chrome 94 milestone.

We are in the process of improving the release notes and we would love to hear your feedback. Please fill out this survey to let us know what you think.

These release notes were last updated on October 19, 2021.

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

Chrome 95

Release summary
- Chrome browser updates
- Admin console updates

Coming soon
- Upcoming Chrome browser changes
- Upcoming Admin console changes

Previous release notes

Additional resources

Still need help?

Chrome 95

Release summary

Chrome browser updates	**Security**	**User productivity /Apps**	**Management**
Stricter parsing rules for Legacy Browser Support			✓
Origin Trial for reduced User-Agent strings	✓		
Chrome deprecates WebAssembly cross-origin module sharing			✓
Explicit user prompts for Autofill addresses		✓	✓
New Side Panel feature		✓	
New and updated policies in Chrome browser			✓
Admin console updates	**Security**	**User productivity /Apps**	**Management**
New and updated policies in the Admin consoleNew RelaunchWindow policy			✓
Upcoming Chrome browser changes	**Security**	**User productivity /Apps**	**Management**
Chrome on Android no longer supports Android Lollipop			✓
Apps shortcut in the bookmarks bar will default to off		✓	
Network data will be migrated to a new folder on Windows	✓		
Network service on Windows will be sandboxed	✓		
New security events for BeyondCorp Enterprise Threat and Data Protection	✓		✓

NewTabPageLocation enterprise policy on Incognito			✓
Feature flag to force the Chrome major version number to 100			✓
DNS-based HTTP to HTTPS redirect	✓		
Chrome will begin deprecating the U2F Security Key API	✓	✓	
CORS Authorization mishandling	✓		
Chrome will maintain its own default root store	✓		✓
Chrome will remove legacy policies with non-inclusive names			✓
Chrome will no longer allow TLS 1.0 or TLS 1.1	✓		✓
Different-origin iframes will no longer trigger JavaScript dialogs	✓		✓
Upcoming Admin console changes	**Security**	**User productivity /Apps**	**Management**
Browser list data downloadable in CSV format			✓

Chrome browser updates

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 *IESiteListMode*, Chrome interprets those rules in the same way as Edge and Internet Explorer.

Origin Trial for reduced User-Agent strings

Chrome 95 begins 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 appears in both the User-Agent HTTP request header and the JavaScript APIs that access the User-Agent string (`navigator.userAgent`, `navigator.appVersion`, `navigator.platform`). This Origin Trial will run over the next six releases, until the reduced User-Agent starts a phased rollout. Subsequently, for sites that may need more time for migration, a deprecation Origin Trial will be available. Enterprises can opt in to the Origin Trial here when it is available.

Chrome deprecates WebAssembly cross-origin module sharing

Chrome 95 prevents WebAssembly module sharing between cross-origin but same-site environments. This allows agent clusters to be tied to origins in the long-term. This change conforms to recent changes in the WebAssembly spec (Chrome Status).

If your enterprise needs any additional time to adjust to this change, a temporary enterprise policy CrossOriginWebAssemblyModuleSharingEnabled is available to allow module sharing for cross-origin same-site environments. This policy will be removed in Chrome 97.

Explicit user prompts for Autofill addresses

In previous releases, when Autofill was enabled, Chrome saved detected addresses as users submitted forms. This update provides more transparency and control to the user by adding a save prompt, and giving the user the control to edit, save, update, or discard the detected address before it is stored. When the AutofillAddressEnabled policy is set to false, this feature is not enabled.

New Side Panel feature

Chrome on Windows, Mac, ChromeOS, and Linux, introduces a new side panel feature. This panel, opened by a toolbar icon, provides easier access to the Reading list and Bookmarks in a vertical list. The side panel can be left open while the user browses.

New and updated policies in Chrome browser

Policy	Description
BrowserLegacyExtensionPointsBlocked	Setting the policy to Enabled or leaving it unset will enable ProcessExtensionPointDisablePolicy to block legacy extension points in the Browser process.
BrowserSwitcherParsingMode	This policy controls how Google Chrome interprets sitelist/greylist policies for the Legacy Browser Support feature. It affects the following policies: BrowserSwitcherUrlList, BrowserSwitcherUrlGreylist, BrowserSwitcherUseIeSitelist, BrowserSwitcherExternalSitelistUrl, and BrowserSwitcherExternalGreylistUrl.
ContextAwareAccessSignalsAllowlist	Enables Chrome Enterprise Platform Identity Connector for a list of URLs. Setting this policy specifies which URLs should be allowed to be part of the attestation flow to get the set of signals from the machine.
PrintPdfAsImageDefault	Controls if Google Chrome makes the Print as image option default to set when printing PDFs.
PrintPostScriptMode	Controls how Google Chrome prints on Microsoft Windows.

Admin console updates

New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
SuggestLogoutAfterClosingLastWindow	Managed Guest Session Settings	Chrome OS	Session settings / Display the logout confirmation dialog
DeviceMinimumVersion	Device Settings	Chrome OS	Device update settings / Auto-update settings / Enforce updates
DeviceMinimumVersionAueMessage	Device Settings	Chrome OS	Device update settings / Auto-update settings / Enforce updates Auto Update Expiration (AUE) message
JavaScriptJitAllowedForSites	User & Browser Settings; Managed Guest Session Settings	Chrome Chrome OS Android	Content / JavaScript JIT / Allow JavaScript to use JIT on these sites
DefaultJavaScriptJitSetting	User & Browser Settings; Managed Guest Session Settings	Chrome Chrome OS Android	Content / JavaScript JIT
JavaScriptJitBlockedForSites	User & Browser Settings; Managed Guest Session Settings	Chrome Chrome OS Android	Content / JavaScript JIT / Block JavaScript from using JIT on these sites
RemoteDebuggingAllowed	User & Browser Settings; Managed Guest Session Settings	Chrome Chrome OS	Security / Allow remote debugging

DesktopSharingHub Enabled	User & Browser Settings	Chrome	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 on Android will no longer supports Android Lollipop

The last version of Chrome that will support Android Lollipop will be Chrome 95, and it includes a message to affected users informing them to upgrade their operating system. Chrome 96 will not support nor ship to users running Android Lollipop.

Apps shortcut in the bookmarks bar will default to off

As early as Chrome 96, Chrome will make the Apps shortcut in the bookmark bar default to off. Chrome will also update the current state for all users who have never changed their setting to the new default (off).

Network data will be migrated to a new folder on Windows

In Chrome 96, data that is needed by the network service, including cookies and other data files, will be migrated to a subdirectory underneath the current location called *Network*. This is to support the upcoming Network Sandbox (see below). This migration will happen automatically and transparently. No action is required, however, you might need to update any scripts that rely on the location of these files.

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 early as Chrome 97). As part of this, third-party code that is currently able to tamper with the network service may 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. An enterprise policy has been added to allow early testing of the new sandbox, and to disable the sandbox if incompatibilities are discovered. You can test the sandbox in your environment using these instructions and report any issues encountered.

New security events to BeyondCorp Enterprise Threat and Data Protection

Chrome 96 will add two new security events to BeyondCorp Enterprise Threat and Data Protection: Password leak and login. This functionality will allow admins to understand enterprise credential usage, to shadow IT within their organization, and to stay ahead of potential security incidents regarding passwords exposed in data breaches.

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).

Feature flag to force the Chrome Major Version number to 100

Starting in Chrome 96, users and site owners can experiment with the upcoming three-digit (Chrome 100) major release version number in the User-Agent string by turning on the *ForceMajorVersion100InUserAgent* flag. This forces the browser to send 100 as the major version number. When Chrome went from version 9 to 10, the increase in the number of digits in the major version number uncovered many issues in User-Agent string parsing libraries. With this feature flag, we can uncover and address these issues before Chrome 100 rolls out. We encourage admins to submit any issues encountered here.

DNS-based HTTP to HTTPS redirect

As early as Chrome 96, Chrome will query DNS for HTTPS records (alongside traditional A and AAAA queries). When a website has deployed an HTTPS DNS record and Chrome receives it, Chrome will always connect to the website via HTTPS (Chrome Status).

Chrome will begin deprecating of the U2F security key API

The U2F API is Chrome's legacy API for interacting with USB security keys. It has been superseded by the W3C Web Authentication API (WebAuthn). Beginning with Chrome 96, when sites make U2F API requests, users may see a prompt that includes a notice about the U2F API's deprecation. In Chrome 98, Chrome will disable the U2F API by default. With Chrome 104, the U2F API will be removed from Chrome.

Sites can continue to use the U2F API beyond Chrome 98 if they enroll in an Origin Trial. Using the Origin Trial also suppresses the deprecation prompt on the enrolled pages. The Origin Trial will end on July 26, 2022, shortly before the release of Chrome 104.

Enterprises can suppress deprecation related changes, and keep the U2F enabled, by using the **U2fSecurityKeyApiEnabled** enterprise policy. This enterprise policy will be removed from Chrome, together with the U2F API, in Chrome 104.

If you run a website that still uses this API, please refer to the deprecation announcement for more details.

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 (Chrome Status). 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.

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

Chrome will maintain its own default root store

To improve user security, and provide a consistent experience across different platforms, Chrome, as early as Chrome 97, 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 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. Deprecated policies will be available in the **Deprecated policies** folder and deleted policies will be in the **Removed policies** folder in the GPO editor.

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.

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 98, it will no longer be possible to bypass the interstitial.

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 downloadable in CSV format

As early as Chrome 97, a CSV format will be introduced as an option to download the browser list data from the Admin console.

Previous release notes

Chrome version & targeted Stable channel release date	PDF
Chrome 94 OS: October 14, 2021	PDF
Chrome 94: September, 2021	PDF
Chrome 93: August, 2021	PDF
Chrome 92: July 20, 2021	PDF
Chrome 91: May 25, 2021	PDF
Archived release notes	

Additional resources

- For emails about future releases, sign up here.
- To try out new features before they're released, sign up for the trusted tester program.
- Connect with other Chrome Enterprise IT admins through the Chrome Enterprise Customer Forum.
- How Chrome releases work—Chrome Release Cycle
- Chrome Browser downloads and Chrome Enterprise product overviews—Chrome Browser for enterprise
- Chrome version status and timelines—Chrome Platform Status | Google Update Server Viewer
- Announcements: Chrome Releases Blog | Chromium Blog
- Developers: Learn about changes to the web platform and features planned for upcoming releases.

Still need help?

- Google Workspace, Cloud Identity customers (authorized access only)—Contact support
- Chrome Browser Enterprise Support—Sign up to contact a specialist
- Chrome Administrators Forum
- Chrome Enterprise Help Center