chrome enterprise

M84 Chrome 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 14, 2020

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 84

Important: Adobe will no longer update and distribute Flash Player after December 31, 2020, therefore Chrome will no longer support Flash content. You can read more about Adobe's plans to discontinue Flash player and your options in Adobe's blog post. Adobe is working with HARMAN, their exclusive licensing/distribution partner, to provide support for Flash Player in legacy browsers.

Chrome is designed to meet the needs of Chrome Enterprise customers, including integration with legacy web content. Companies that need to use a legacy browser to run Flash content after December 31, 2020 can get set up with HARMAN and Legacy Browser Support.

Chrome Browser updates

Updates to cookies with SameSite

Starting on July 14, cookies that don't specify a SameSite attribute will be treated as if they were SameSite=Lax. Cookies that still need to be delivered in a cross-site context must explicitly request SameSite=None. Cookies with SameSite=None must also be marked Secure and delivered over HTTPS. To reduce disruption, the updates will be enabled gradually, so different users will see it at different times. We recommend that you test critical sites using the instructions for testing.

You will be able to revert to the legacy cookie behavior using policies until Chrome 91. You can specify domains accessing cookies that require legacy semantics using LegacySameSiteCookieBehaviorEnabledForDomainList or control the global default with LegacySameSiteCookieBehaviorEnabled. For more details, visit Cookie Legacy SameSite Policies.

This change started with Chrome 80, but was temporarily on hold in light of the COVID-19 pandemic. It's being set in motion again, and will take effect in Chrome 80 and more recent versions of Chrome.

Insecure downloads will be blocked from secure pages in Chrome 84 through Chrome 88

By Chrome 88, downloads from insecure sources will no longer be allowed when started from secure pages. This change will be rolled out gradually, with different file types affected in different releases:

<table>
<tr><th></th><th>Chrome 81 and 83</th><th>Chrome 84</th><th>Chrome 85</th><th>Chrome 86</th><th>Chrome 87</th><th>Chrome 88 and later</th></tr>
<tr><td>Executables
(e.g. .exe, .apk, etc.)</td><td rowspan="4">Console warning</td><td>Warn</td><td colspan="4">Block</td></tr>
<tr><td>Archives
(e.g. .zip, .iso, etc.)</td><td rowspan="3">Console warning</td><td>Warn</td><td colspan="3">Block</td></tr>
<tr><td>All other non-safe types
(e.g. .pdf, .docx, etc.)</td><td rowspan="2">Console warning</td><td>Warn</td><td colspan="2">Block</td></tr>
<tr><td>Images, audio, video, text
(e.g. .png, .mp3, etc.)</td><td>Console warning</td><td>Warn</td><td>Block</td></tr>
</table>

- Executables—Users will be warned in Chrome 84, and files will be blocked in Chrome 85.
- Archives—Users will be warned in the Chrome developer console in Chrome 85, and files will be blocked in Chrome 86.
- Other non-safe types (e.g. pdfs)—Users will be warned in the Chrome developer console in Chrome 86, and files will be blocked in Chrome 87.
- Other files—Users will be warned in the Chrome developer console in Chrome 87, and files will be blocked in Chrome 88.

Warnings on Android will lag behind Desktop warnings by one release. For example, executables will show a warning starting in Chrome 85.

The existing InsecureContentAllowedForUrls policy can be used to allow specific page URLs to download insecure files. You can read more details in our blog post.

Improved resource consumption when window is not visible

To save on CPU and power consumption, Chrome will detect when a window is covered by other windows and will suspend work painting pixels. A previous version of this feature had an incompatibility with some virtualization software. Known bugs have been fixed, but if you experience any issues, you will be able to disable this feature using the NativeWindowOcclusionEnabled policy.

Some users will see this feature in Chrome 84, with a full release planned in Chrome 85.

Chrome remembers user preferences when launching external protocols

As requested by IT admins, users are able to select "always allow for this site" when opening an external protocol in Chrome 84. The approval is scoped to the current origin, and is only available for secure origins.

The URLWhitelist policy only allows external protocols for domain joined devices

A recent release of Chrome changed the behavior of the URLWhitelist policy which lets you allow external protocols such as “callto:” or “ms-calendar”. To improve security on Windows®, this policy only allows external protocols for devices joined to an Active Directory domain.

Deprecation of TLS 1.0 and TLS 1.1

The Chrome team announced in October 2019, plans for the deprecation of legacy TLS versions (TLS 1.0 and 1.1). In Chrome 84, we will mark sites that do not support TLS 1.2 and above with a full-page warning telling users that the connection is not fully secure.

If users have sites affected by these changes and need to opt out, you can use the SSLVersionMin policy to turn off the security indicator and warning. To allow TLS 1.0 and later without additional warnings, set the policy to **tls1**. The SSLVersionMin policy will work until January 2021. More details are available in our blog post.

Improvements to Chrome downgrades

When a managed Chrome browser updates to the next version, it will retain a snapshot of User Data. This is useful for admins when Sync is turned off and they need to rollback to a previous version of Chrome. The number of snapshots can be controlled using the UserDataSnapshotRetentionLimit policy and Chrome can function as it did before by setting UserDataSnapshotRetentionLimit to 0. For more details, visit Downgrade your Chrome version.

Stronger consent for the search and new tab page

Chrome will protect against extensions that attempt to change the user's preferences without their consent. After an extension changes the default search engine or the new tab page, Chrome will confirm the change with the user, and allow them to keep the change or revert back to the old settings.

As an admin, you can control your employees' default search provider directly using the Default Search Provider and NewTabPageLocation policies. They will not trigger a confirmation dialog.

User-Agent Client Hints

As part of an ongoing effort to reduce bad actors' ability to track users, Chrome plans to reduce the granularity of information that is part of the user agent string and expose that information through User-Agent Client Hints. In Chrome 84, we are introducing User-Agent Client Hints for some users. This is an additive change only, and should not have any negative effect when interacting with any standards-compliant server.

However, some servers may not be able to accept all characters in the User-Agent Client Hints headers, part of the broader Structured Headers emerging standard. If the addition of this header causes problems with servers that cannot be fixed quickly, you will be able to use the UserAgentClientHintsEnabled policy to disable the added headers. Although, this is a temporary policy that will be removed in Chrome 88.

You can test your environment by enabling the "experimental web platform features" flag in Chrome. A wider rollout of this change is planned in Chrome 85.

Cross-Origin Resource Setting (CORS) enterprise policies will no longer take effect

The CorsMitigationList and CorsLegacyModeEnabled policies have been removed in Chrome 84, as previously communicated.

The ForceNetworkInProcess policy is now deprecated

Chrome 73 introduced a change to move network activity into a separate process. We were aware of known incompatibilities with some third-party software that were injected into Chrome's process, so the ForceNetworkInProcess policy was provided as a temporary stop-gap to revert to the old behavior. The transition period for this change ends in Chrome 84, and the policy is no longer available.

Chrome OS updates

Camera app supports MP4 (H.264)

Videos captured in the Chrome OS Camera app will now save as MP4 (H.264) videos. This makes it easier to use your recorded videos in other apps.

Window management improvements for multiple monitors and split screen

When in Overview mode you can now drag a window to the left or right edge to quickly set up a split screen. If you use multiple monitors, you can drag windows to other displays while in Overview mode.

Adding search functionality to the ChromeVox menu

For screen reader users, the ChromeVox menu is a one-stop-shop for learning about ChromeVox and accessing key information and commands. When ChromeVox is turned on, press Search + Period at any time to open the menu and explore options such as jump commands, speech options, and much more. As of Chrome 84, it's now possible to search within the ChromeVox menu to find what you are looking for even faster! Simply open the menu and your mouse cursor will automatically be placed in the Search field. You can either search for a given item, or use the arrow keys to navigate the menu options.

Sheet Limit Policy for Native Printing

Many organizations would like to limit the amount of paper used when printing. With the PrintingMaxSheetsAllowed policy, admins can limit the number of sheets used in a single print job for their managed devices users. For example, placing a limit on printing excessively large documents such as an entire digital textbook, ebook, or accidental print requests, prevents ink and paper waste.

Chrome OS login/lock screen enterprise disclosure

On the login screen, Chrome OS now shows an enterprise badge on managed profiles. This allows users to see at first glance whether their profile is managed or not.

Crostini mic permission

You can now give Crostini access to your microphone through Settings. If you're developing an Android app, you can test the microphone feature using the Android emulator.

Admin Console updates

Update controls are available for managed browsers

In the Admin console, admins can now configure additional update policies for Chrome browsers that are managed by Chrome Browser Cloud Management. For example, you might want to allow or disable updates, pin to a specific version of Chrome, roll back to previous version of Chrome, set relaunch notifications, or control when Chrome checks for updates. The configuration details are further described in this help center article.

Network file shares policy

Admins can now configure network file shares for users under **Chrome management** > **User settings** > **Network file shares**. These policies include configuration of SMB settings for NetBIOS discovery, NTLM authentication, and preconfiguring file shares so users can see them within the Files app on Chrome OS.

Readable data in the devices export

Timestamps in the device list's CSV export file are now in a "human-readable" format. This format helps to make the timestamps easy for users to read. Previously, these columns contained the same value as reported through the Directory API.

Domain-restricted apps & extensions from the Chrome Web Store

In the Google Admin console, admins can now add domain-restricted apps & extensions from the Chrome Web Store. These apps are available under **Chrome management** > **Apps** > **Add from Chrome Web Store** > **View private apps**.

Device screen resolution

Admins can now configure the screen resolution and UI scaling for displays. These settings are available under **Chrome management** > **Device settings** > **Screen settings**.

Dinosaur game policy

When Chrome cannot connect to the internet it displays a "Dinosaur game" for users to play. This game is disabled by default for domain-enrolled Chrome OS devices, but admins can enable it under **Chrome management** > **User settings** > **Dinosaur game**.

Ignore proxy on captive portals policy

Chrome OS can open captive portal authentication pages in a separate window that ignores all policies for the current user, including proxy settings. This policy only takes effect if a proxy is configured. For example, through policy by the user in chrome://settings or by extensions. This policy is available under **Chrome management** > **User settings** > **Ignore proxy on captive portals**.

Display system info on the sign-in screen

Your users can view system information such as serial numbers and OS versions on the sign-in screen by pressing Alt+V. Admins can force or block this feature under **Chrome management** > **Device settings** > **System info on sign-in screen**.

Accessibility device policy settings

In addition to the launch of advanced accessibility controls for users, a similar set of controls for the login screen allows admins to enable accessibility features remotely or restrict them when necessary. For example, restricting dictation features in hospitals or blocking certain features in classrooms to prevent disruption. See the full list of features below:

- Spoken feedback
- Select to speak
- High contrast
- Screen magnifier
- Sticky keys
- Virtual keyboard
- Dictation
- Keyboard focus highlighting
- Caret highlight
- Auto-click enabled
- Large cursor
- Cursor highlight

- Primary mouse button
- Mono audio
- Accessibility shortcuts

New and updated policies (Chrome Browser and Chrome OS)

Policy	Description
AccessibilityImageLabelsEnabled	Enable Get Image Descriptions from Google
AppCacheForceEnabled	Allows the AppCache feature to be re-enabled even if it is turned off by default
AutoOpenAllowedForURLs	List of URLs specifying which urls AutoOpenFileTypes will apply to
AutoOpenFileTypes	List of file types that should be automatically opened on download
PrintRasterizationMode *Windows only*	Controls how Google Chrome prints on Windows

Coming soon

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

Upcoming Chrome Browser changes

Wildcards no longer supported in PluginsAllowedForUrls in Chrome 85

In preparation for the Flash deprecation later this year, Chrome will be removing the ability for enterprises to define entries with wildcards in hostnames (e.g., “https://*” or “https://[*.]mysite.foo”) for the PluginsAllowedForUrls policy. If you're using hostname wildcards, you will need to explicitly specify which hostnames still require Flash. For example, “https://[*.]mysite.foo” would need to be updated to match explicit entries like “https://flash.mysite.foo”. This change is intended to help determine which sites still require updating, with time to make an adjustment before support for Flash is removed completely in December, 2020.

Compiler optimization performance improvements in Chrome 85

Chrome will use an improved compiler optimization technique on Mac and Windows in Chrome 85. Enterprises aren't expected to notice any changes, but software interacting with Chrome in

unexpected or unsupported ways such as, code injection, may not function as expected with Chrome 85.

To ensure compatibility, you can test your environment with the Chrome 85 beta channel, starting July 23, 2020.

The Legacy Browser Support extension will be removed from the Chrome Web Store in Chrome 85

Legacy Browser Support (LBS) is now built into Chrome, and the old extension is no longer needed. The Chrome team is planning to unpublish LBS from the Chrome Web Store in Chrome 85, and it will be removed from browsers in Chrome 86. To continue using Legacy Browser Support, ensure you're using Chrome's built-in policies, documented here. The old policies set through the extension will no longer take effect when the extension is removed. If you run into issues using the built-in LBS policies please file a new issue report at http://crbug.com/new.

Cross-origin fetches will be disallowed from content scripts in Chrome Extensions in Chrome 85

As part of an effort to improve Chrome Extension security, cross-origin fetches are being disallowed from content scripts in Chrome Extensions. Cross-Origin Read Blocking (CORB) has already applied to content scripts since M73. We plan to also enable CORS for content script requests starting in M85. We expect most extensions to be unaffected by the CORS change, but there is a chance that some requests initiated from content scripts may start to fail.

Please test Chrome Extensions that your business depends on, to make sure they work with the new behavior when Chrome is launched with the following cmdline flags (in 81.0.4035.0 or later):

```
--enable-features=OutOfBlinkCors,CorbAllowlistAlsoAppliesToOorCors
```

During the test, watch for fetches or XHRs that are initiated by content scripts and blocked by CORS. If extensions you depend on are affected, then please open bugs to add the affected extensions to a temporary allowlist to exempt them from the change. The changes only affect fetches or XHRs for content types not blocked by CORB (such as images, JavaScript, and CSS), and only if the server does not approve the CORS request with an Access-Control-Allow-Origin response header.

Improved resource consumption for background tabs in Chrome 85

To save on CPU and power consumption, Chrome will throttle the amount of CPU that background tabs can use. With this change, Chrome will only allow background tabs to wake up once per minute and to only use 1% CPU time.

You will be able to control this behavior using the IntensiveWakeUpThrottlingEnabled policy.

Introduction of AutoLaunchProtocolsFromOrigins policy in Chrome 85
The new AutoLaunchProtocolsFromOrigins policy will allow you to specify combinations of external protocols and origins that should be launched automatically, without requiring user confirmation.

The SafeBrowsingExtendedReportingOptInAllowed policy will no longer take effect in Chrome 85
The support of SafeBrowsingExtendedReportingOptInAllowed policy will be removed in Chrome 85. Please use SafeBrowsingExtendedReportingEnabled policy instead. You can find the migration instructions on the deprecated policy page.

Chrome on MacOS will have additional protections for sensitive enterprise policies in Chrome 85
Macs that are not managed by a UEM/EMM/MDM (or legacy MCX) will ignore sensitive enterprise policies that may be set by malware. This check already happens for sensitive policies on Windows, and will apply to the same set of policies on MacOS.

Single words will not be treated as intranet locations by default in Chrome 86
By default, Chrome 85 will improve user privacy by avoiding DNS lookups for single keywords entered into the address bar, which could theoretically be read by a malicious actor. However, this change to default behavior will likely interfere with enterprises that use single-word domains in their intranet. That is, a user typing "helpdesk" will no longer be directed to "https://helpdesk/".

You will be able to control the behavior of Chrome via policy. In addition to preserving the existing behavior (which will perform a search immediately and then ask the user if they're trying to reach the intranet site), you can also set the intranet site as Chrome's first action.

Chrome will warn about mixed content forms in Chrome 86
Web forms that load via HTTPS but submit their content via HTTP (unsecured) pose a potential risk to users' privacy. Chrome 85 will show a warning on such forms, telling the user that the form is insecure. Chrome will show an interstitial warning when the form is submitted, which will stop any data transmission, and the user will be able to choose to proceed or cancel the submission.

You will be able to control this behavior using the DisableMixedFormsWarning enterprise policy.

The address bar will show the registrable domain rather than the full URL for some users in Chrome 86
To protect your users from some common phishing strategies, Chrome will begin showing only the registrable domain in the address bar in Chrome 86. This change makes it more difficult for

malicious actors to trick users with misleading URLs. For example, **https://google-secure.example.com/secure-google-sign-in/** will appear only as **example.com** to the user.

Although this change is designed to keep your users' credentials safe, you will be able to revert to the old behavior through the ShowFullUrls policy. This change will initially only roll out to some users, with a full rollout planned for a later release.

DTLS 1.0 will be removed in Chrome 86

DTLS 1.0, a protocol used in WebRTC for interactive audio and video, will be removed by default. Any applications that depend on DTLS 1.0 (most likely gateways to other teleconferencing systems) should update to a more recent protocol. You can test if any of your applications will be impacted using the following command line flag when launching Chrome:

```
--force-fieldtrials=WebRTC-LegacyTlsProtocols/Disabled/
```

If your enterprise needs additional time to adjust, a policy will be made available to temporarily extend the removal.

Insecure public pages no longer allowed to make requests to private or local URLs in Chrome 86

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. A policy will be provided to turn off this mechanism, and another one to allow specific pages to make requests to more private IP Address Spaces.

Chrome extensions will not be able to inject Flash content settings in Chrome 86

Extensions will not be able to inject content settings for Flash. Admins should instead use policies to control Flash behavior on Chrome. See PluginsAllowedForUrls.

More inclusive policy names will be introduced in Chrome 86

Chrome will be moving to more inclusive policy names in Chrome 86. The terms "whitelist" and "blacklist" will be replaced with "allowlist" and "blocklist". The following policies will be deprecated, and equivalent policies will be introduced for each:

Deprecated policy name	New policy name
ExtensionInstallWhitelist	ExtensionInstallAllowlist

ExtensionInstallBlacklist	ExtensionInstallBlocklist
NativeMessagingBlacklist	NativeMessagingBlocklist
URLBlacklist	URLBlocklist
URLWhitelist	URLAllowlist
AuthNegotiateDelegateWhitelist	AuthNegotiateDelegateAllowlist
AuthServerWhitelist	AuthServerAllowlist
SpellcheckLanguageBlacklist	SpellcheckLanguageBlocklist
AutoplayWhitelist	AutoplayAllowlist
SafeBrowsingWhitelistDomains	SafeBrowsingAllowlistDomains
DeviceNativePrintersWhitelist	DeviceNativePrintersAllowlist
ExternalPrintServersWhitelist	ExternalPrintServersAllowlist
NativePrintersBulkWhitelist	NativePrintersBulkAllowlist

If you're already using the existing policies, they will continue to work, though you will see warnings in chrome://policy stating that they're deprecated.

Factor in scheme when determining if a request is cross-site (Schemeful Same-Site) in Chrome 88

Chrome 88 will modify the definition of same-site for cookies such that requests on the same registrable domain but across schemes are considered cross-site instead of same-site. For example, http://site.example and https://site.example will be considered cross-site to each other.

For enterprises that need extra time to adjust to these changes, policies will be made available.

The Chrome Browser Cloud Management reporting extension will cease functionality in Chrome 86

The Chrome Browser Cloud Management reporting extension is no longer necessary, as its functionality has been integrated into Chrome browser. If you are manually force-installing this extension, you can safely stop doing so. Please ensure that you've set "Enable managed browser cloud reporting" in the admin console instead.

The extension will no longer function in Chrome 86.

Upcoming Admin console changes

New Version Report and Update Controls

There will be a new Version Report and Update Controls available in the Admin console. These features give increased visibility into the Chrome versions deployed in your enterprise and allows you to more granularly control how managed Chrome browsers update. If you would like to sign up

to be a Trusted Tester for these features please enter your test domain and a contact email into this form.