chrome enterprise

M83 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 May 19, 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 83

Chrome Browser updates

Secure DNS

The DNS requests for all users will be auto upgraded to their DNS provider's DNS-over-HTTPS (DoH) service if available (based on a list of known DoH-capable servers). This change will be rolling out gradually throughout Chrome 83. You can turn off DNS-over-HTTPS for your users with the DnsOverHttpsMode policy with Group Policy or in the Google Admin console. Setting it to **off** will ensure that your users are not affected by Secure DNS.

Flash Dialog Changes

Chrome will add the following warning text to the activation prompt for Flash Player, highlighting the industry wide end of support: "Flash Player will no longer be supported after December 2020." Users will see this prompt, even if Flash is enabled by policy. Learn more.

Legacy Browser Support improvements

Legacy Browser Support (LBS) will have incorporated multiple improvements such as: 1) better Kerberos support, 2) better interoperability between the LBS extension and LBS Cloud Policies, as well as 3) mitigating switching time.

Introduction of tab groups for all users

Starting in Chrome 80, some users were able to organize their tabs by grouping them on the tab strip. Each group can have a color and a name to help your users keep track of their different tasks and workflows. This will be rolled out widely to ChromeOS, Mac, Windows, and Linux users throughout Chrome 83.

Changes to the Managed Bookmarks policy

The ManagedBookmarks policy will be subject to stricter verification. From chrome 83, this policy might become invalid if any of "name", "toplevel_name", or "url" fields are not of type "string" as described by the policy.

If your users have any issues seeing managed bookmarks, check to see if the policy has an error in chrome://policy, or if you're using Chrome Browser Cloud Management, you can check for errors in the Google Admin console. If you see an error, make sure the ManagedBookmarks policy uses string types for the above fields.

Third-party cookies blocked by default for Incognito sessions

Chrome now blocks third-party cookies by default in Incognito sessions, with the ability to enable third-party cookies on a site-by-site basis.

You will be able to control Chrome's behavior with the existing BlockThirdPartyCookies policy via Group Policy or the Google Admin console:

- **Not set**—The user will be able to control third-party cookies, and they'll be blocked by default in Incognito sessions
- **True** —Third-party cookies blocked in both Incognito and standard sessions
- **False**—Third-party cookies will not be blocked, and the setting cannot be changed

Users can check all their saved passwords for leaks

In Chrome 79 we started warning users if their credentials had been compromised in a data leak when they logged into a website. Chrome 83 builds on this feature, allowing users to check on all their saved passwords at once. This feature uses the same privacy-preserving system introduced in Chrome 79; it does not send plain-text passwords to Google.

If you wish, you can prevent your users from accessing this feature by preventing Chrome from saving passwords, using the PasswordManagerEnabled policy via Group Policy or in the Google Admin console.

Control over the variations framework

You will have more granular control over update behavior in Chrome 83. In addition to the version controls that exist today, Chrome 83 allows you to configure Chrome variations with the ChromeVariations (Mac, Windows, and Linux) and DeviceChromeVariations (Chrome OS) policies. You can pick between:

- **Variations enabled**—This is the default, and allows all variations in Chrome.
- **Critical fixes only**—This will turn off all experiments and progressive rollouts, but will still apply variations with immediate and important security or compatibility improvements.
- **Variations disabled**—No changes will be deployed using the variations framework. Choosing this setting significantly increases the risk of security and compatibility issues, and is not recommended.

Updated form control elements

HTML form controls provide the backbone for much of the web's interactivity. One issue, however, is inconsistency in their styling. Older controls were styled to match the user's operating system, while more recent controls were designed to match whatever style was popular at the time. This has led to controls that look mismatched and sometimes outdated. They've also suffered from inconsistent accessibility, touch, and keyboard support.

To address these gaps, Chrome 83 introduces a new set of defaults for form controls. Developers will have less work to do to keep their controls looking great, consistent, and broadly usable.

If you encounter any incompatibility issues with this change, the UseLegacyFormControls enterprise policy will revert to the old defaults.

Updated UI for extensions

Chrome has an improved extensions area that keeps the top of the browser tidy and makes it easier for users to control their installed extensions. By default, extensions will show up inside the extension icon, but they can be pinned beside the address bar using the pin icon.

SameSite cookie changes were rolled back

With the stable release of Chrome 80 in February, Chrome began enforcing secure-by-default handling of third-party cookies as part of our ongoing effort to improve privacy and security across the web.

However, in light of the extraordinary global circumstances due to COVID-19, we temporarily rolled back the enforcement of SameSite cookie labeling. While most of the web ecosystem was prepared for this change, we want to ensure stability for websites providing essential services including banking, online groceries, government services and healthcare that facilitate our daily life during this time.

We plan to resume enforcement as early as Chrome 84. The SameSite Updates page will be updated regularly with the latest schedule.

New Trusted Tester sign up page available for Chrome Enterprise

If you're interested in trying new Chrome Enterprise features ahead of release and provide feedback, we have an updated sign up form for our Trusted Tester program, available here.

More intuitive privacy and security controls for end users in Chrome

Chrome is launching new tools and a redesign of Chrome's privacy and security settings on desktop, to make them easier for end-users to understand and control. See the Chrome blog post for all the details.

Chrome OS updates

Relaunch Notification for Chrome OS Updates

From Chrome 83, relaunch notifications allow Chrome OS admins to recommend or enforce Chrome OS relaunches within a certain time period after an update was downloaded..

Gesture Navigation & Education

From chrome 83 there will be new gestures available for Chromebook tablet mode, which make it easier for users to navigate using touch. Users will now be shown tips on how to use gestures to go Home, go Back, and see your open apps. For those who need navigation buttons, they can be turned on from Accessibility.

Virtual Desks Renaming and Restore

In Chrome 78 we released Virtual Desks, which allowed users to create up to four separate work spaces. This feature helps create boundaries between projects or activities, making it easier to multitask and stay organized.

Now users will now be able to name their virtual desks, enabling users to know what each desk is for. Plus, desks (and their names) will persist after the device reboots or crashes to make it simple to stay organized.

To enable Virtual Desks, users can tap the overview key on the top of the keyboard or swipe down on the keypad using three fingers; "+ New desk" will appear in the top right hand corner

Idle Settings Changes

Users can now set different functionality for what their Chromebook does when it becomes idle depending on whether the device is charging or on battery. Users can find these settings in the Settings app (available through App Launcher or the cog icon in the Quick Settings menu) under Device > Power.

Files media views available on all devices

Media views (Recents, Audio, Images, Videos) located at the top of the Files app side navigation are now available on all devices. These views allow users to more quickly access their recent files by category.

Get device hostname from enterprise.deviceAttributes Extension API

The enterprise.deviceAttributes extension API has been updated with a new method (getDeviceHostname) to return the hostname that Chrome OS announces for itself in DHCP queries.

Improved APK caching (non-library direct installs, split APKS, postpone Play self-update, multiple versions)

With Chrome 83, users should see a significant increase in the install reliability of Android apps on Chrome OS. Especially, we released three major changes: (1) We significantly improved the reliability of force install & allow install policies on Chrome OS by the fast policy propagation feature (2) Due to delayed Play self-updates, Android apps get installed before eventual updates of the Play store. (3) By extending caching to allow-installed apps and split-APKs, apps will be installed much quicker for a user if they were already installed by another user before.

Admin Console updates

Update blackout windows

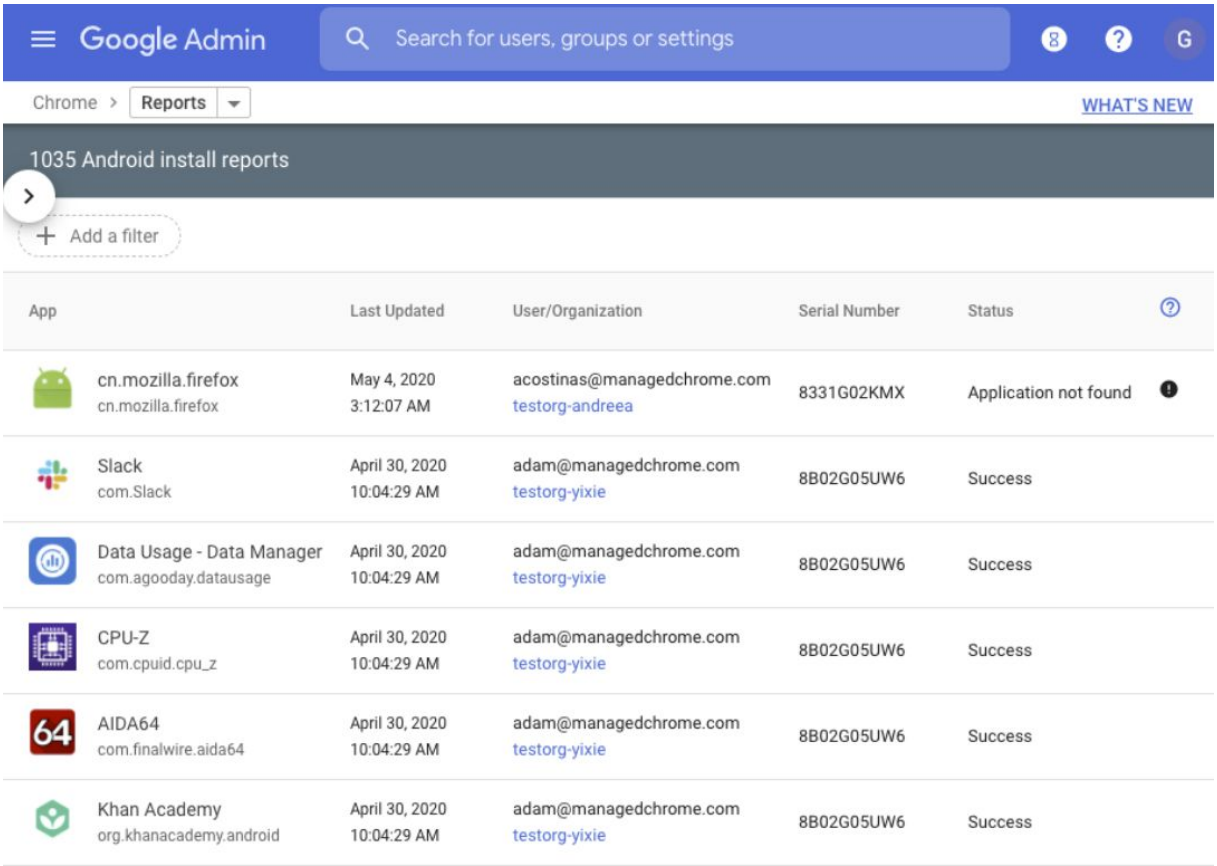
The DeviceAutoUpdateTimeRestrictions policy is now available in the Admin console. This policy allows you to set time blocks when automatic update checks are not to be performed. This policy only affects devices configured to auto-launch a kiosk app.

Manage accessibility settings for user sessions & managed guest sessions

Advanced accessibility controls allow administrators to enable accessibility features remotely or restrict them when necessary (e.g. restricting dictation features in hospitals, or blocking certain features in classrooms to prevent disruption.)

Android app installations report

The new Android app (ARC++) installation report page allows you to view the status of Android app installations across their fleet, providing greater visibility into app ecosystem health. The redesigned UI features stronger filtering capabilities, streamlined status descriptions, and layout updates such as app icons.



Bulk reboot for devices

You can now select multiple kiosk devices from the device list and reboot them in bulk. Previously reboot was available on a device-by-device basis only.

Deprecation of remote commands for Chrome OS devices running version Chrome 77 and lower

Due to a service upgrade, remote commands will no longer be served for Chrome devices running Chrome 77 and lower versions from May 15, 2020. Remote commands are mainly used to monitor and control kiosk health, for example by remotely taking screenshots or rebooting devices. To keep remote commands working for your device fleet, you should make sure that their devices are running the Chrome OS version Chrome 78 or higher. (See Remote commands no longer supported on version 77 or earlier).

New and updated policies (Chrome Browser and Chrome OS)

Policy	Description
ChromeVariations	Configuring this policy allows to specify which variations are allowed to be applied in Google Chrome
UserDataSnapshotRetentionLimit *(Chrome browser)*	Limits the number of user data snapshots retained for use in case of emergency rollback
NativeWindowOcclusionEnabled *(Windows only)*	Enables native window occlusion in Google Chrome
AllowNativeNotifications *(Linux only)*	Configures whether Google Chrome on Linux will use native notifications
UseLegacyFormControls	Use Legacy Form Controls until M84
AdvancedProtectionAllowed	Enable additional protections for users enrolled in the Advanced Protection program
ScrollToTextFragmentEnabled	Enable scrolling to text specified in URL fragments

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

Deprecation of TLS 1.0 and TLS 1.1 in Chrome 84

The Chrome team announced plans for the deprecation of legacy TLS versions (TLS 1.0 and 1.1) last October. 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.

DTLS 1.0 will be removed in Chrome 84

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

CORS enterprise policies will no longer work in Chrome 84

The CorsMitigationList and CorsLegacyModeEnabled policies will be removed in Chrome 84, as previously communicated.

The URLWhitelist policy will not allow you to whitelist external protocols in Chrome 84

A recent release of Chrome changed the behavior of the URLWhitelist policy to let you whitelist an external protocol. To improve security, this policy will be changed back to its original behavior. As a result, external protocols will not be whitelisted through the policy.

Chrome will be able to remember approval for launching external protocols in Chrome 84

Users will be able to check "always allow for this site" when opening an external protocol in Chrome 84. The approval will be scoped to the current origin, and will only be available for secure origins.

Compiler optimization performance improvements in Chrome 84

Chrome will use an improved compiler optimization technique on Mac and Windows in Chrome 84. Enterprises aren't expected to notice any changes, but you should test Chrome 84 Beta in their environment to confirm this change doesn't interfere with any software running in their environment. Software interacting with Chrome in unexpected or unsupported ways (e.g. code injection) may not function as expected with Chrome 84..

The ForceNetworkInProcess policy will no longer take effect in Chrome 84

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 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 will end in Chrome 84, and the policy will no longer have any effect.

Chrome on Mac will have additional protections for sensitive enterprise policies in Chrome 84

Macs that are not managed by a UEM/EMM/MDM (or legacy MCX) will ignore certain sensitive enterprise policies that may be set by malware, on Chrome 84.

Insecure downloads will be blocked from secure pages, with changes 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 Chrome 85, and files will be blocked in Chrome 86
- **Other non-safe types** (e.g. pdfs)—Users will be warned in Chrome 86, and files will be blocked in Chrome 87
- **Other files**—Users will be warned in Chrome 87, and files will be blocked in Chrome 88

Warnings on Android will lag behind Desktop warnings by one release (e.g. 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.

Wildcards no longer supported in PluginsAllowedForUrls in Chrome 85

Also in preparation for the Flash deprecation later this year, Chrome will be removing the ability for enterprises to define wildcards for PluginsAllowedForUrls policy in Chrome 85. If you're using wildcards in that policy, you will need to switch to specific whitelists for any sites that are still using Flash. This change is intended to help determine which sites still require updating, with time to adjust before support for Flash is removed completely in Dec 2020.

Insecure public pages no longer allowed to make requests to private or local URLs in Chrome 85
Insecure pages will no longer be able to make requests to IPs belonging to a more private address space (as defined in CORS-RFC1918). E.g., 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.

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

This feature will roll out to some users in Chrome 83.

DTLS 1.0 will be removed in Chrome 83
DTLS 1.0, a protocol used in WebRTC for interactive audio and video, will be removed by default in Chrome 83. Any applications that depend on DTLS 1.0 (most likely gateways to other teleconferencing systems) should update to a more recent protocol. 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 83
Insecure pages will no longer be able to make requests to IPs belonging to a more private address space (as defined in CORS-RFC1918). E.g., **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 disable this mechanism, and another one to allow specific pages to make requests to more private IP Address Spaces.

Wildcards no longer supported in PluginsAllowedForUrls in Chrome 83
Also in preparation for the Flash deprecation later this year, Chrome will be removing the ability for enterprises to define wildcards for **PluginsAllowedForUrls** policy in Chrome 83. If you're using wildcards in that policy, you will need to switch to specific whitelists for any sites that are still using Flash. This change is intended to help determine which sites still require updating, with time to adjust before support for Flash is removed completely in Dec 2020.

Upcoming Chrome OS changes

Adding print server support for CUPS
We're working on a feature to add support for Common UNIX Printing System (CUPS) printing to print servers from Chrome OS. You and your users will be able to configure connections to external print servers and print from the printers on servers using CUPS.

Upcoming Admin console changes

New Version Report and Update Controls
There will be a new Version Report and Update Controls available in Admin console. These features give increased visibility into the Chrome versions deployed in your enterprise and allows you to more granularly control how Chrome Browser updates. 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.