chrome enterprise

M81 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 April 7, 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 81

Chrome Browser updates

Chrome's consumer Terms of Service will be updated on March 31, 2020

We are updating the Google Terms of Service effective March 31, 2020, and the improved Terms will now cover Chrome and Chrome OS. See a summary of the key changes and a preview of the new Terms and Additional Terms. Google users have been notified in-product of this change.

NTLM / Kerberos authentication disabled by default in Incognito mode and guest sessions

Ambient authentication (NTLM/Kerberos) will be disabled by default in Incognito mode and guest sessions in Chrome 81. To revert to the old behavior and allow ambient authentication, use the AmbientAuthenticationInPrivateModesEnabled policy.

TLS 1.3 hardening measure

TLS 1.3 includes a hardening measure to strengthen the protocol's protections against a downgrade to TLS 1.2 and earlier. This measure is backward compatible and doesn't require that proxies support TLS 1.3. It only requires that proxies correctly implement TLS 1.2. However, last year, we had to partially disable this measure due to noncompliant, TLS-terminating proxies.

The following list contains the minimum firmware versions for affected products that we're aware of:

Palo Alto Networks:

- PAN-OS 8.1 must be upgraded to 8.1.4 or later.
- PAN-OS 8.0 must be upgraded to 8.0.14 or later.
- PAN-OS 7.1 must be upgraded to 7.1.21 or later.

Cisco Firepower Threat Defense and ASA with FirePOWER Services when operating in "Decrypt - Resign mode/SSL Decryption Enabled" (advisory PDF):

- Firmware 6.2.3 must be upgraded to 6.2.3.4 or later.
- Firmware 6.2.2 must be upgraded to 6.2.2.5 or later.
- Firmware 6.1.0 must be upgraded to 6.1.0.7 or later.

You can opt in to the new measure to test it and confirm if your proxy is affected using the TLS13HardeningForLocalAnchorsEnabled policy. If you encounter problems, you should upgrade affected proxies to fixed versions.

Starting in Chrome 81, the new measure will become the default. However, you will be able to use the same policy to opt out if you need to upgrade affected proxies. This policy will be available until Chrome 86.

Changes to how HTTPS pages load subresources

In Chrome 81, http:// audio and video resources on https:// pages started getting autoupgraded to https://, and Chrome blocked them by default if they failed to load over https://. Users can unblock affected audio and video resources by clicking on the lock icon in the address bar and selecting **Site**

Settings. Also in Chrome 80, http:// images on https:// pages were still allowed to load, but users started seeing “Not Secure” in the address bar.

In Chrome 81, http:// images on https:// pages will be autoupgraded to https://, and Chrome will block them by default if they fail to load over https://.

You can control these changes using the StricterMixedContentTreatmentEnabled policy (**Strict treatment for mixed content** in the admin console), which disables autoupgrades for audio and video and the warning for images. This policy is a temporary policy and will be removed in Chrome 84.

The InsecureContentAllowedForUrls and InsecureContentBlockedForUrls policies will control the site setting described above. These policies will eventually be removed, but there is no timeframe for their removal yet.
You should begin ensuring that resources in pages are fetched over HTTPS and manage exceptions using a policy. For more information, see the Chromium blog.

FTP support removed

FTP will no longer be directly supported in Chrome 81. Your users should use a native FTP client instead.

Known incompatibility with older versions of Carbon Black Protection (Bit9)

Carbon Black Protection (previously known as Bit9) has a known incompatibility with Chrome 81, which causes multi-second delays to some page loads. Update to Carbon Black Protection 8.1.8 when it becomes available to fix the incompatibility. Carbon Black has more information about the issue here.

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 Mac, Windows, and Linux users throughout Chrome 81.

Updated form control elements

A small number of users will see a preview of new form control elements in Chrome 81. These will be launched more broadly with enterprise controls in Chrome 83. If any of your users are having trouble displaying form controls (text boxes, radio buttons, checkboxes, etc), please open a new issue at crbug.com.

Developer changes to Chrome Web Store

The Chrome Web Store charges a $5.00 fee to register as a Chrome Web Store developer. This fee was previously required only before publishing an item to the public, but is now required for all Chrome Web Store developers. For more information, see this blog post.

Chrome OS updates

Use websites and Progressive Web Apps (PWAs) on Chrome OS Kiosk

IT admins can now use the Google Admin console to install websites and Progressive Web Apps (PWAs) on managed Chrome devices in locked-down kiosk mode.

Linux (Beta) support for Android emulators

Developers often need to run virtual machines, such as an Android developer who uses the Android emulator to test their app. While previously Linux for Chromebooks (aka Crostini) did not support virtual machines, this change allows Crostini to run virtual machines on specific boards.

Deploy Android apps to Android runtime from Linux (Beta)

Android developers using Linux for Chromebooks (aka Crostini) can now build apps with Android Studio and test them natively on their Chromebook using Chrome OS's built-in Android runtime (ARC++). This feature can be turned on from Linux settings.

IP reporting for all managed devices

Extend support for IP address reporting (LAN and WAN) under "System reporting and troubleshooting" under "Device Details" to include all managed devices with a signed-in, managed user, instead of just single app kiosk devices. This is enabled if "Device state reporting" is enabled under device policy.

Gestures in tablet mode

Try new gesture navigation to quickly switch between apps and interact with your Chromebook in tablet mode.

- To get to the Home Screen at any time, swipe up from the bottom.
- To see all pinned apps, small-swipe up from the bottom.
- To return to the previous screen, swipe from the left.
- To see all open windows, swipe up from the bottom and hold.

End to end support for printers via print servers
Users are now able to connect to and save printers defined by print servers. IT admins can use this functionality to test print server setups for their organization.

Extended caching of Android apps
So far, APK caching was only applied to force installed apps. From Q1 2020, APK caching is extended to Android apps in allow install mode.

APK caching significantly reduces the installation time of Android apps if the same app was already installed on the device before. This especially applies to ephemeral sessions which require the re-installation of apps after every login.

With the extension of APK caching to apps that are marked as "Allow install" in the admin console, students and users of Chrome OS devices experience a significantly reduced installation time of their Android apps, helping them to spend more time on relevant tasks.

Android on Chrome OS kiosk mode deprecation
In Chrome 81, you will no longer have access to set new policies for Android apps in kiosk mode. Existing policies for Android apps in kiosk mode will not be impacted and will be supported until June 2021. Websites and PWAs are the replacement technology for Kiosk, now supported in Chrome 81.

Admin Console updates

Managed guest session settings redesign and idle settings
The new redesigned settings page for managed guest sessions includes performance improvements, new search filters, and new settings. Admins can now set idle settings and lid close behavior for managed guest sessions.

Networks settings redesign

The new redesigned Networks page for Chrome & mobile device management includes performance improvements and a fresh look.

Device list CSV export

Admins can now export a CSV of the Chrome device list, including serial number, last policy sync time, OS version, latest user, and more. To export, go to the device list and click the download icon at the top right of the table.

Simultaneously manage Active Directory and Cloud devices

Admins can now manage Chrome OS devices with Active Directory and Chrome OS devices with Cloud policy in the same admin console. A new set of enrollment policies support a mixed device environment along with a new Management Mode flag specifying whether the device is managed by cloud or Microsoft® Active Directory® on the device details page.

Remotely clear user profiles from device

Admins can now clear all user profiles from a device remotely for use cases such as getting a device ready for a new user for the coming school year, supporting a rotating internship program and clearing data for troubleshooting without losing device settings.

New and updated policies (Chrome Browser and Chrome OS)

Policy	Description
LocalDiscoveryEnabled	Enable chrome://devices
ScreenCaptureAllowed	Allow or deny screen capture

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

DNS-over-HTTPS in Chrome 83

The DNS requests of some users are being autoupgraded to their DNS provider's DNS-over-HTTPS (DoH) service if available, but DoH is disabled by default for managed devices running Chrome OS and for desktop Chrome Browser instances that are domain joined or have at least one active policy.

In Chrome 83, DoH will launch by default for all remaining users. You can disable DNS-over-HTTPS for your users with the DnsOverHttpsMode policy. Setting it to **off** will ensure your users are not affected by DoH.

Updated form control elements in Chrome 83

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 will introduce 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.

Deprecation of TLS 1.0 and TLS 1.1 in Chrome 83

The Chrome team announced plans for the deprecation of legacy TLS versions (TLS 1.0 and 1.1) last October. In Chrome 83, 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 disable 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.

Third-party cookies will be blocked by default for Incognito sessions in Chrome 83

Chrome 83 will block 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:

- **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

Changes to the ManagedBookmarks policy in Chrome 83

The ManagedBookmarks policy will be subject to stricter verification in 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. If you see an error, make sure the ManagedBookmarks policy uses string types for the above fields.

CORS enterprise policies will no longer work in Chrome 83

The CorsMitigationList and CorsLegacyModeEnabled policies will be removed in Chrome 83, as previously communicated.

Users will be able to check all their saved passwords for leaks in Chrome 83

Chrome 79 started warning users if their credentials had been compromised in a data leak when they logged into a website. Chrome 83 will build 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.

Control over the variations framework in Chrome 83

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

- **Variations enabled**—This is the default, and allows all variations in Chrome.
- **Critical fixes only**—This will disable all experiments and progressive rollouts.

- **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.

Flash Dialog Changes in Chrome 83

Chrome will add warning text to the activation prompt for Flash Player, highlighting the industry wide end of support date (Dec 2020) with a link to learn more. It is not shown to users who have Flash enabled by policy.

Updated UI for extensions in Chrome 83

Chrome 83 will have an improved extensions area in both the main browser and PWA windows, with an enhanced extensions menu.

Updated Tabstrip UI in Chrome 83

Chrome 82 will feature a way to group related tabs, and will display preview images when hovering over tabs.

Improved resource consumption when a window is not visible in Chrome 83

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.

Chrome apps deprecation in Chrome 83

As announced in January, Chrome apps will be phased out and ultimately disabled by June 2022. Beginning in Chrome 81, new public Chrome apps will no longer be accepted by the Chrome Web Store. Beginning in Chrome 83, Chrome will no longer support Chrome apps on Microsoft® Windows®, Apple® Mac®, and Linux®. If your organization needs extra time to adjust, a policy will be available to extend support until Chrome 87.

Insecure downloads will be blocked from secure pages, with changes in Chrome 83 through Chrome 86

By Chrome 86, 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</th><th>Chrome 82</th><th>Chrome 83</th><th>Chrome 84</th><th>Chrome 85</th><th>Chrome 86 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 82, and files will be blocked in Chrome 83
- Archives—Users will be warned in Chrome 83, and files will be blocked in Chrome 84
- Other non-safe types (e.g. pdfs)—Users will be warned in Chrome 84, and files will be blocked in Chrome 85
- Other files—Users will be warned in Chrome 85, and files will be blocked in Chrome 86

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.

Cross-origin fetches will be disallowed from content scripts in Chrome Extensions in Chrome 84
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 M84. 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. For more details please see: www.chromium.org

Factor in scheme when determining if a request is cross-site in Chrome 84
Chrome 84 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. E.g., **`http`**`://site.example` and **`https`**`://site.example` will be considered cross-site to each other.

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.

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 from print servers on 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.