chrome enterprise

M80 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 February 4, 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 80

Chrome Browser updates

Updates to cookies with SameSite

Starting in Chrome 80, 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 can 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 88. You can specify trusted domains using LegacySameSiteCookieBehaviorEnabledForDomainList or control the

global default with LegacySameSiteCookieBehaviorEnabled. For more details, visit Cookie Legacy SameSite Policies.

Pop-ups and synchronous XHR requests not allowed on page unload

Pop-ups and synchronous XHR requests won't be allowed on page unload. This change will improve page load time and make code paths simpler and more reliable. If you encounter incompatibilities with legacy software, you will be able to revert to behavior matching Chrome 79 and earlier using the following policies, which will be available until Chrome 88:

- To allow pop-ups on page unload, see AllowPopupsDuringPageUnload.
- To allow synchronous XHRs on page unload, see AllowSyncXHRInPageDismissal.

Control data types in Chrome sync

Chrome users have the ability to granularly enable or disable each type of data that's synchronized in the advanced Data from Chrome sync settings. In Chrome 80, you can also control the data types synced using the SyncTypesListDisabled policy.

Changes to how HTTPS pages load secure subresources in Chrome 80 and 81

In Chrome 80, http:// audio and video resources on https:// pages will be autoupgraded to https://, and Chrome will block them by default if they fail 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**. In Chrome 80, http:// images on https:// pages will still be allowed to load, but users will see "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, 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.

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.

Control if websites can check for user payment methods

The PaymentMethodQueryEnabled policy allows you to control if websites can check for user payment methods. For details, see PaymentMethodQueryEnabled.

Web Components v0 removed

The Web Components v0 APIs (Shadow DOM v0, Custom Elements v0, and HTML Imports) were supported only by Chrome Browser. To ensure interoperability with other browsers, late last year, we announced that these v0 APIs were deprecated and will be removed in Chrome 80. For more information, see the Web Components update.

Until Chrome 85, you can use the WebComponentsV0Enabled policy to re-enable web components v0.

Introduction of tab groups for some users

Starting in Chrome 80, some users will be 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. A wider rollout is planned for Chrome 81.

Block external extensions

In Chrome 80, you can use the BlockExternalExtensions policy to stop the installation of external extensions on your devices. The policy will not block kiosk apps or extensions installed by policy.

Chrome Browser Cloud Management Reporting Companion no longer required

The functionality previously provided by the Chrome Browser Cloud Management - Reporting Companion extension has been integrated directly into Chrome Browser. If you're using Chrome Browser Cloud Management, users will no longer see the extension on their devices when reporting is turned on. No action is required from admins or users.

Chrome OS updates

Enable autorotate for tablet devices with connected external inputs

Autorotation will stay enabled when you connect a mouse to a device in tablet mode. You can pair a mouse with a tablet in portrait mode or a convertible device in tent mode without having to manually rotate your screen.

Switch default Linux (Beta) container to Debian 10 (Buster)

Developers who set up Linux (Beta) for the first time will now receive a container with Debian 10 (Buster). Previously, containers used Debian 9 (Stretch). Existing Debian 9 containers will be upgraded in the future.

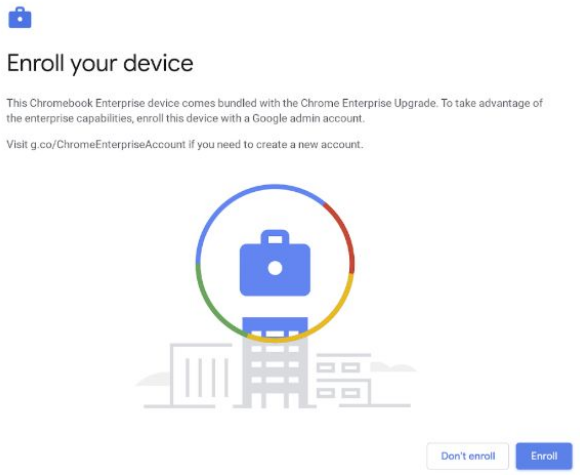
Policy to show PIN pad on sign-in and lock screen for tablets

In certain environments, such as K–6 education, you might assign numeric-only passwords when more complex passwords are too cumbersome or hard to remember. To make signing in easier on Chrome OS touchscreen devices, you can now show the PIN pad on the sign-in and lock screens by

default. Users can still get to the virtual keyboard to enter a full alphanumeric password if needed. For details, see the DeviceShowNumericKeyboardForPassword policy.

New notification for Chromebook Enterprise enrollment

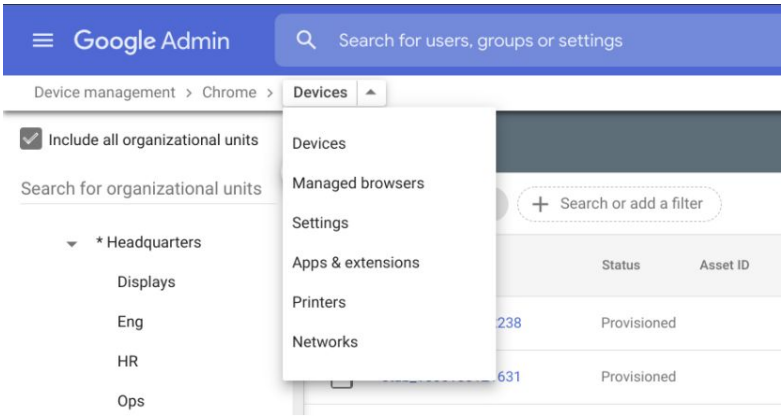
In Chrome 80, you no longer need to press **Ctrl+Alt+E** to begin the device enrollment process. At the end of the onboarding process, you'll see a welcome page where you can start enrollment.



Admin Console updates

Quick switch between pages

Admins can now quickly switch between Chrome pages in the Google Admin console. At the top, click the current page name to go to other pages.



New and updated policies (Chrome Browser and Chrome OS)

Policy	Description

AmbientAuthenticationInPrivateModesEnabled	Enables ambient authentication for profile types
DNSInterceptionChecksEnabled	Enables DNS interception checks
NTPCustomBackgroundEnabled	Allows users to customize the background on the New Tab page
PaymentMethodQueryEnabled	Allows you to control if websites can check for user payment methods
PrinterTypeDenyList	Disables printer types on the deny list
StricterMixedContentTreatmentEnabled	Controls treatment for mixed content
SyncTypesListDisabled	Controls data types that should be excluded from synchronization

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

Known incompatibility with older versions of Carbon Black Protection (Bit9) in Chrome 81

Carbon Black Protection (previously known as Bit9) has a known incompatibility with Chrome 81, which causes multisecond delays to some page loads. An upcoming version of Carbon Black Protection (8.1.8) will fix the incompatibility.

Improved resource consumption when window not visible in Chrome 81

To save on CPU and power consumption, Chrome 81 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.

Ambient authentication disabled by default in Incognito mode and guest sessions in Chrome 81

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 in Chrome 81

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.

DNS-over-HTTPS in Chrome 81

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 81, DoH is expected to 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.

FTP support removed in Chrome 81

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

New Chrome UI for legacy TLS versions in Chrome 81

The Chrome team recently announced updated plans for the deprecation of legacy TLS versions (TLS 1.0 and 1.1). In Chrome 81, 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.

Shared clipboard between computers and Android devices in Chrome 82

Users will have the option to share their clipboard content between their computers and Android devices. To share, they need to have Chrome Browser installed, be signed in on both devices with the same account, and have Chrome sync turned on.

The text is end-to-end encrypted, and Google can't see the contents. You can control this feature using the SharedClipboardEnabled policy.

Changes to the ManagedBookmarks policy in Chrome 82

The ManagedBookmarks policy will be subject to stricter verification in Chrome 82. On Android and Apple® macOS®, this policy might become invalid if any of "name", "toplevel_name", or "url" fields are not of type "string" as described by the policy.

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 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.

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.

Updates for USB devices with Linux

From the Chrome shell (crosh), you'll be able to attach a USB device to Linux apps running on a Chromebook so that Linux apps can access the Linux instance.

Upcoming Google Admin console changes

Chrome OS kiosk mode support for web apps

In a future Chrome OS release, devices in kiosk mode will support Progressive Web Apps and websites. Support will include Auto-Launch App mode.

Android on Chrome OS kiosk mode

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.