chrome enterprise

M77 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 September 10, 2019

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

Chrome 76
- Chrome Browser updates
- Chrome OS updates
- Admin console updates
- New and updated policies (Chrome Browser and Chrome OS)
- Coming soon
- Upcoming Chrome Browser changes
- Upcoming Chrome OS changes
- Upcoming Google Admin console changes

Sign up **here** for our email distribution for future releases.

Chrome 77

Admin console updates

Faster and simpler Admin console for Chrome Enterprise

Starting in September, we're rolling out a major redesign of the Google Admin console for Chrome Enterprise administrators. Expect to see improvements in page load times, a new unified app-management page for managing Android, Chrome, and web apps together, and many new policies. For details, see the Admin Insider blog.

Prevent password reuse

In the Admin console, you can now specify the URL where users are redirected to change their password if they reuse it on a non-whitelisted website or are a victim of phishing. If this policy is unset, users are directed to their Google Account sign-in page to change their password. For details, see Prevent password reuse and read more in our white paper.

New default policies for printing (CUPS)

New native print policies help you manage your users' printing options more closely—set defaults and restrictions on duplex and color.

Unified native printer management (CUPS)

Use a new interface for managing thousands of native (CUPS-based) printers for users, devices, and managed guests. The 20-printer maximum cap has been raised to allow for thousands of printers for each organizational unit in the Google Admin console. Support has also been extended beyond user policy to include device and managed guest policy.

Chrome Browser updates

Site isolation improvements

Chrome Browser now protects cross-site data, such as cookies and HTTP resources, in attacker-controlled websites. Site isolation works even if an attacker finds a bug in an untrusted renderer process and tries to execute arbitrary code in it.

Site isolation will also now be enabled on some Android devices to protect websites and data where mobile users enter passwords.

Legacy Browser Support updates

You can now define the URL of an XML file that will never trigger a browser switch using the BrowserSwitcherExternalGreylistUrl policy with Legacy Browser Support. You can also use the new **chrome://browser-switch/internals** page to verify that Legacy Browser Support rules are being followed. Please try it out and send feedback.

The First Run Experience has been updated

Chrome Browser now has a new flow to welcome users, get them set up with popular Google services, and set a default web browser. You can disable the new flow with the PromotionalTabsEnabled policy.

Launch guest browsing by default

You can now immediately launch Chrome Browser in guest browsing mode using the `--guest` command line flag or the new BrowserGuestModeEnforced policy. With guest browsing, browsing activity is not written to the disk and does not persist between browser sessions.

Chrome OS updates

More secure built-in certificate verifier

Updates to the certificate verifier now provide better isolation of trust settings between different contexts. Users with valid certificates should not have any issues. In rare instances, the legacy Network Security Services (NSS) implementation tolerated some classes of invalid certificates which are now no longer tolerated. You can issue new, valid certificates or contact Chrome Enterprise support for help.

User account and file name in IPP Header

If enabled by policy, all print jobs will include the requesting user account and file name of the document in the IPP header over a secure IPPS connection. This added functionality will provide additional information about a print job that enables third-party printing features, such as secure printing and print-usage tracking.

Automatic shutdown after extended standby

With Linux kernel 4.4 and later, devices will automatically go from standby to shutdown after 3 days to increase battery life. To find the kernel version, go to **chrome://system** and search for **uname**. The kernel version is the first set of digits.

HD copy-protected content support for ARC++ apps

In Android apps, you can now play high-definition (HD) copy protected HDMI 1.4 content. This update is useful for externally connected displays, such as televisions.

Volume control based on orientation for convertibles

On devices running Chrome OS, the volume button on the top or right will always increase the volume, whether the device is in laptop mode or tablet mode.

Chromebook accessibility enhancements

Chromebook accessibility features remove the need to physically click the touchpad or mouse. Instead, you can point to an item and the Chromebook will click, right-click, left-click, or drag for you after a certain amount of time. With Chrome 77, you can now point to an item and the device will automatically scroll up, down, left, or right. For details, see Turn on Chromebook accessibility features.

Enhanced formatting support of external drives

When formatting a FAT32, exFAT, or NTFS external drive, users will now be able to pick a file system and label for their drive.

Chrome OS file selector now the default for Android apps

For a consistent user experience, Android apps now open the Chrome OS file selector. This change provides a consistent file-selection experience across apps.

New and updated policies (Chrome Browser and Chrome OS)

Policy	Description
BrowserGuestModeEnforced	Enforces guest browsing mode when a user launches Chrome Browser
SafeBrowsingRealTimeLookupEnabled	Checks Safe Browsing reputation of visited URLs in real time
UserFeedbackAllowed	Allows users to send feedback to Google

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

G Suite add-ons and extensions moving to G Suite Marketplace

In the coming weeks, all G Suite apps and extensions will be moved from the Chrome Web Store to the G Suite Marketplace. Developers need to migrate their unmigrated add-ons so that new users can install them. Existing users can continue to use unmigrated add-ons. However, if they uninstall Google Docs Editor add-ons or Google Drive apps, they will not be able to reinstall them. And, if an existing user creates a template with one of the add-ons, users who do not already have the add-on installed will not be able to use the add-on in the template. Have your developers review the background and what they need to do. To check whether an add-on has been migrated, search for it in the G Suite Marketplace. For details on the move to the G Suite Marketplace, see the Google Cloud blog.

ExtensionAllowInsecureUpdates policy will stop working in Chrome 78

The policy to allow extensions to update using the previous CRX2 packaging will stop working in Chrome 78, as previously communicated. In Chrome 78, all extensions must be repackaged into the new CRX3 format to ensure secure delivery of updates to your browsers and devices.

Trial of auto-upgrade for DoH in Chrome 78

Starting in Chrome 78, the DNS requests of some users will auto-upgrade to their DNS provider's DNS-over-HTTPS (DoH) service if available. DoH will be 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. A new group policy, DnsOverHttpsMode, will also be available. Setting it to "off" will ensure users are not affected by DoH.

Pop-ups and synchronous XHR requests not allowed in Chrome 78

Starting in Chrome 78, pop-ups and synchronous XHR requests will not be allowed to improve page load time and make code paths simpler and more reliable. You will be able to revert to the old behavior using policies, which will be available until Chrome 82.

Flags will be cleaned up starting in Chrome 78

Many flags in **chrome://flags** will be removed in upcoming Chrome versions, starting with Chrome 78. As a reminder, flags should not be used to configure Chrome Browser because they're not supported. Instead, configure Chrome Browser for your enterprise or organization using policies.

Atomic policy groups introduced in Chrome 78

To ensure predictable behavior from policies that are tightly coupled together, some policies will be regrouped based on atomic policy groups. If you enable atomic policy groups, policies in a single group will all be forced to set their behavior from the same source—the one with the highest priority.

If you set policies from multiple sources, such as the Admin console and the Group Policy Management Editor, you will be able to enable atomic policy groups in Chrome 78. You can also see if there are any conflicting policies at chrome://policy. If you have multiple policies in the same policy group from different sources, they will be affected by this change. For more details, see Atomic Policy Groups and Understand Chrome policy management.

Users warned if credentials are leaked in Chrome 78

Beginning in Chrome 78, users will be notified if their credentials are part of a known data breach. This detection occurs without plain-text passwords being sent to Google. You will be able to enable or disable this feature using the PasswordLeakDetectionEnabled policy.

Chrome Renderer Integrity to protect users in Chrome 78

In Chrome 78, Chrome Renderer Integrity will be enabled by default for users on Microsoft® Windows® 10 version 1511 and later. It prevents loading of unsigned modules in Chrome Browser's renderer processes that deal with user content to prevent certain types of malicious attacks.

Note: There is a known incompatibility between Chrome Renderer Integrity and old versions of Symantec® Endpoint Protection® (14.0.3929.1200 and below). We recommend updating to the latest version of Symantec Endpoint Protection (14.2 or above). For a download of the latest version or more details, refer to the Symantec documentation. To help with any incompatibilities, you can temporarily disable Chrome Renderer Integrity.

Send a call from Chrome Browser to your Android device in Chrome 78

In Chrome 78, users will be able to highlight and right-click a phone number link in Chrome Browser and send the call to their Android device.

Windows-8 specific welcome page removed in Chrome 78

The Windows 8-specific welcome page will be removed in Chrome 78. Support for the distribution.suppress_first_run_default_browser_prompt master_preferences setting will be removed accordingly. For more about master preferences, see Use master preferences for Chrome Browser.

Ambient authentication disabled by default in Incognito mode in Chrome 79

Starting in Chrome 79, ambient authentication (NTLM/Kerberos) will be disabled by default in Incognito mode. You will be able to use a policy to revert to the old behavior and allow ambient authentication.

FTP support removed in Chrome 80

Beginning in Chrome 80, FTP will not be directly supported in Chrome Browser. Your users should use a native FTP client instead. To help with the transition, you will be able to use the FTPProtocolSupport policy to temporarily re-enable FTP until Chrome 82.

TLS 1.3 hardening measure implemented in Chrome 80

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 does not 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 bugs in some non-compliant, TLS-terminating proxies.

Starting in Chrome 78, you will be able to opt in to the new measure to test it and confirm if your proxy is affected. 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 should upgrade affected proxies to fixed versions.

Starting in Chrome 80, the new measure will become the default. However, you can use a policy to opt out if you need extra time to upgrade affected proxies.

Updates to cookies with SameSite in Chrome 80

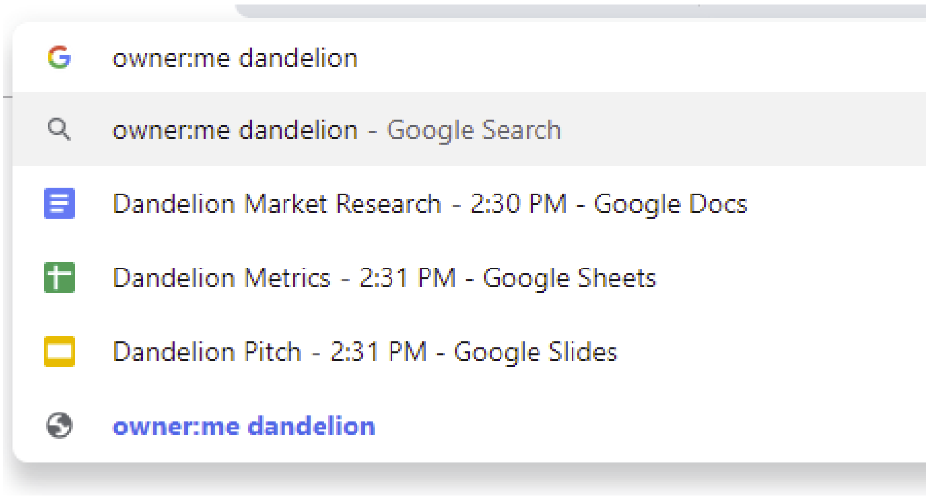
Starting in Chrome 80, cookies that do not specify a SameSite attribute will be treated as if they were SameSite=Lax. Cookies that still need to be delivered in a cross-site context can explicitly request SameSite=None. The attributes must also be marked Secure and delivered over HTTPS. We will provide policies if you need to configure Chrome Browser to temporarily revert to legacy SameSite behavior.

Web Components v0 removed in Chrome 80

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. You can find more information in the Web Components update.

Drive integration in the address bar

In the future, users will be able to search for Google Drive files that they have access to from the address bar. If you have G Suite Business, Enterprise, or Enterprise for Education, you can apply for the beta program. For more details and to apply, see Search Google Drive files in Chrome URL bar BETA.



owner:me dandelion

owner:me dandelion - Google Search

Dandelion Market Research - 2:30 PM - Google Docs

Dandelion Metrics - 2:31 PM - Google Sheets

Dandelion Pitch - 2:31 PM - Google Slides

owner:me dandelion

Upcoming Chrome OS changes

Chrome OS and Chrome Browser settings split in Chrome 78

Starting in Chrome 78, Chrome OS settings will be in a new window and use a new URL that's separate from Chrome Browser settings. If you block Chrome Browser settings by URL (chrome://settings), you might also want to block the new URL for Chrome OS settings, which is chrome://os-settings.

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

Managed guest session support for managed Google Play

A setting in the Admin console will allow Android apps to run in managed guest sessions (previously known as public sessions). Currently, Android apps can only run in a signed-in session.

Device host name in DHCP requests

You will be able to configure the device host name used during DHCP requests, including variable substitutions for ${ASSET_ID}, ${SERIAL_NUM}, ${MAC_ADDR}, and ${MACHINE_NAME}.