chrome enterprise

M76 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 30, 2019

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 76

Chrome Browser updates

Flash is blocked by default

As communicated in the Chromium Flash Roadmap, Adobe® Flash® will be blocked by default in Chrome 76. Users can manually switch back to ASK ("Dialog to Ask first before running Flash") before running Flash. This change won't impact existing policy settings for Flash. You can still control Flash behavior using DefaultPluginsSetting, PluginsAllowedForUrls, and PluginsBlockedForUrls. For more details, see the Flash Roadmap.

All privately hosted extensions must be packaged with CRX3 format in Chrome 76

This change was originally planned for Chrome 75, but we delayed it to Chrome 76 to allow more time for customer transition. It was originally announced in the Chrome 68 release notes.

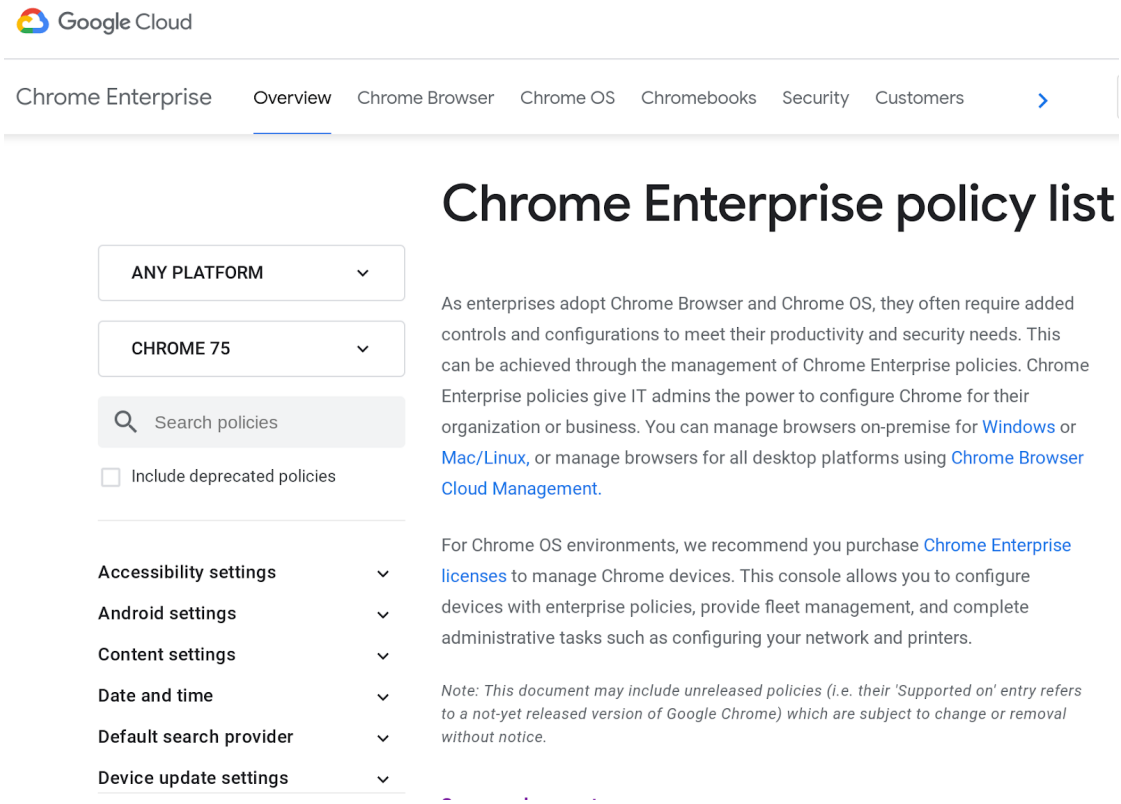
CRX2 uses SHA1 to secure updates to a Chrome extension. Breaking SHA1 is technically possible, which allows attackers to intercept an extension update and inject arbitrary code into it. CRX3 uses a stronger algorithm, avoiding this risk.

Starting with Chrome 76, all force-installed extensions will need to be packaged in the CRX3 format. For details on temporarily enabling CRX2, see ExtensionAllowInsecureUpdates. This policy is only meant to provide extra time to repackage extensions, and will stop working in Chrome 78. For the CRX2 deprecation timeline, see Chromium.

Privately hosted extensions that were packaged using a custom script or a version of Chrome prior to Chrome 64.0.3242.0 must be repackaged. If your organization is force-installing privately hosted extensions or third-party extensions hosted outside of the Chrome Web Store that are packaged in CRX2 format, the extensions will stop updating in Chrome 76 and new installations of the extension will fail.

A new page for documenting enterprise policies is available

Chrome's policies are now listed on a new Chrome Enterprise policy list. This documentation allows you to filter by platform and Chrome version to see which policies are available for your fleet.



A new layout engine is being used

LayoutNG is a new layout engine with several improvements such as:

- Improved performance isolation
- Better support for scripts other than Latin
- Many issues around floats and margins fixed
- Numerous web-compatibility issues fixed

Although the impact to the user should be minimal, LayoutNG changes some behavior in very subtle ways, fixes hundreds of tests, and improves compatibility with other browsers. Despite our best efforts, it is likely that this will cause some sites and applications to render or behave slightly differently.

If you suspect that WNG caused a website to break, please file a bug report, and we'll investigate.

Site isolation is enforced

In Chrome 67, we introduced enterprise policies to opt in to site isolation early or opt out if users encountered an issue. We've resolved the reported issues. Starting with Chrome 76, we will remove the ability to opt out of site isolation on desktop using the SitePerProcess or IsolateOrigins policies. This change only applies to desktop platforms (including Chrome OS). On Android, the SitePerProcessAndroid and IsolateOriginsAndroid policies will continue to have the ability to disable

site isolation. If you run into issues with the policies, file a bug in Chromium.

--disable-infobars is no longer supported

Chrome will no longer support the --disable-infobars flag, which was used to hide pop-up warnings from Chrome Browser. To support automated testing, kiosks, and automation, the CommandLineFlagSecurityWarningsEnabled policy was added to allow you to disable some security warnings.

Policies with a dictionary value type can be merged

In Chrome 76, you can merge policies that take a dictionary of values set from multiple sources, including the cloud and by platform and Active Directory. Without this policy, if different sources conflict, only the dictionary from the highest priority source will have an effect. For details, see PolicyDictionaryMultipleSourceMergeList.

Legacy Browser Support has been improved

A new page at chrome://browser-switch/internals makes it easier to debug and troubleshoot Legacy Browser Support. We also fixed a bug where LBS wouldn't switch during the first minute of a browser session (when using XML site lists).

New version of the On-Prem Chrome Reporting Extension

Version 2.0 of the Chrome Reporting Extension will soon ship in the Chrome Web Store. Download the corresponding native component MSI.

If you have user browsing data reporting turned on, you will start seeing a new piece of data for each visited site: "legacy_technologies." It's an array of strings that will initially contain one value, "Flash." This means this site requires Adobe Flash and might soon stop working correctly (see paragraph above). Future releases will list other obsolete web technologies such as Java Applets, Silverlight, and more.

The output file has changed from a single file called chrome_reporting_log.json to a daily rotated file with file name in the format chrome_reporting_log_YYYY_MM_DD.json. This will make it simpler to manage the disk usage of the application and clear obsolete data.

"https" scheme and "www" subdomain will be hidden

To make URLs easier to read and understand, and to remove distractions from the registrable domain, we will hide URL components that are irrelevant to most Chrome users. We will hide the "https" scheme and the special-case subdomain "www" in Chrome omnibox on Chrome desktop and

Chrome-on-Android. After the site loads, the full URL can still be revealed by clicking twice in the URL bar (desktop) or tapping once (mobile).

The Chrome team has also worked to build a Chrome extension to help power users recognize suspicious sites and report them to Safe Browsing. Power users can use this extension to display the full URL with no scheme or subdomain hiding, and report suspicious sites to Safe Browsing.

Chrome OS updates

Enhancements to automatic clicks accessibility feature

Chromebooks have had a feature called Automatic clicks in accessibility settings for years, which has given users with motor and dexterity challenges the ability to hover over an item and have Chrome OS click it (without pressing the touchpad or mouse). In Chrome OS version 76, we have expanded this feature to not only be able to left click, but also right-click, double-click, and click and drag by simply hovering.

Built-in FIDO security key is now supported

In this release, all latest-generation Chromebooks will gain support for built-in FIDO security keys backed by the Titan M chip. This feature is disabled by default, but an admin can enable the built-in security key by changing the Chrome OS policy called DeviceSecondFactorAuthentication to U2F.

Account consistency between the Chrome content area and the ARC++ container

We are rolling out a single sign-on experience for Chrome and Android applications on Chrome OS over several weeks, beginning August 21, 2019, to simplify user management of Google Accounts on Chrome OS. We added a new section to Settings: "Google Accounts."

From here, a user can manage all signed in Google Accounts. This includes reauthenticating or removing some secondary accounts and adding others. Attempts to add secondary accounts from Chrome or ARC++ will be redirected to this unified flow. Users that previously had a secondary account signed in to Chrome or ARC++ will need to reauthenticate following the update, which will add their account to Account Manager.

Admin console updates

Updates to the Chrome device list and device details

- Search and filter devices and organizational units directly from the device list.
- Customize your preferred view with auto-update expiration date, Chrome OS version, and device model.
- Long-running tasks such as screenshot, log capture, and reboot will now complete in the background, so you don’t need to wait for them.

New and updated policies (Chrome Browser and Chrome OS)

Policy	Description
BrowserSwitcherExternalGreylistUrl *Browser only* Chrome 77+	URL of an XML file that contains URLs that should never trigger a browser switch
CommandLineFlagSecurityWarningsEnabled *Browser only*	Enable security warnings for command-line flags
PolicyDictionaryMultipleSourceMergeList	Allows the selected policies to be merged when they come from different sources, with the same scopes and level

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

Flags will be cleaned up from chrome://flags, starting in Chrome 77
Many flags in chrome://flags will be removed in upcoming Chrome versions, starting with Chrome 77. You shouldn't use flags to configure Chrome Browser because they're not supported. Instead, configure Chrome Browser for your enterprise or organization using policies.

- **Atomic policy groups will be introduced in Chrome 77**
  To ensure predictable behavior from policies that are tightly coupled together, some policies will be regrouped based on atomic policy groups. These groups ensure that all applied policies from a single group come from the same source—the one with the highest priority—to prevent unpredictable behavior when mixing policies from multiple sources. The order of precedence for Chrome Policies is documented here.

  This may be a breaking change if you set GPOs from multiple sources (e.g. the Admin Console and via Windows Group Policy). You can check if any GPOs are in conflict by visiting chrome://policy in

Chrome browser. If you have multiple policies in the same policy group from different sources, update your policies to ensure that all policies in a given policy group come from the same source.

The First Run Experience will be updated in Chrome 77

Chrome 77 will no longer show the single page welcome. It will instead have a new flow to welcome users, get them set up with popular Google services, and set a default web browser. The same policy that was used to disable the previous First Run Experience can be used to disable the new flow: PromotionalTabsEnabled.

It will be possible to make guest browsing the default in Chrome 77

You will be able to set Chrome to launch immediately into guest mode by using a `--guest` command line flag or a new policy called BrowserGuestModeEnforced. In this mode, your users won't see or change any other Chrome profile. When they exit guest browsing, their browsing activity is deleted from the computer.

Experiment for DNS-over-HTTPS (DoH) in Chrome 78

Starting in Chrome 78, the DNS requests of some users will autoupgrade to DNS-over-HTTPS if they are using a DNS provider that supports it. This is part of ongoing work to bring secure DNS options to Chrome. Individual users can opt out by disabling this experiment at chrome://flags. Admins can opt-out their enterprise from this experiment by policy. Instructions will be provided in a future Chromium blog post and release notes.

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

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

Ambient authentication will be disabled by default in Incognito sessions in Chrome 79

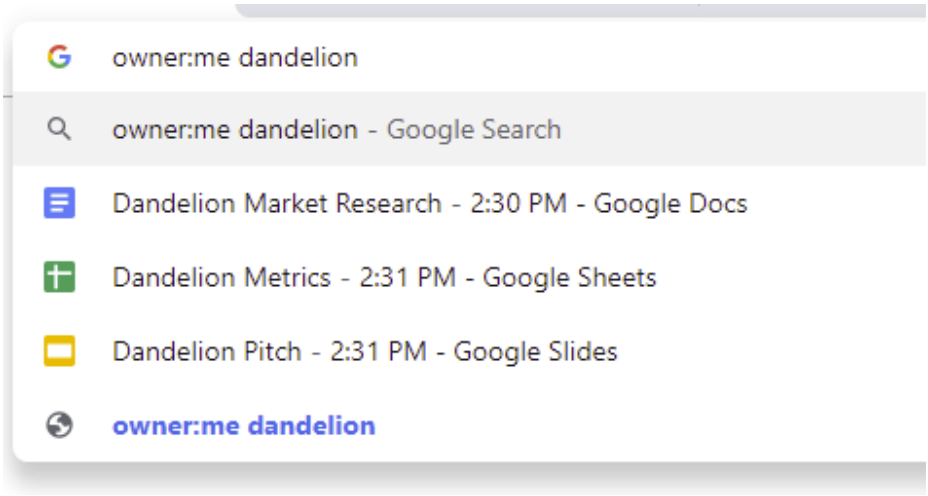
Starting in Chrome 79, ambient authentication (NTLM/Kerberos) will be disabled by default in Incognito sessions. Admins will be able to revert to the old behavior, allowing ambient authentication using an enterprise policy.

Cookies with SameSite by default, and Secure SameSite=None cookies 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. They must also be marked Secure and delivered over HTTPS. Policies will be made available for enterprises that need to configure Chrome to temporarily revert to legacy SameSite behavior.

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.



Extension User Data Policy Updated

As part of Project Strobe, Google is updating its User Data Policy, and these changes go into effect starting October 15, 2019. For more information, see the blog post.

- We're requiring extensions to only request access to the least amount of data. While this has previously been encouraged for developers, now we're making this a requirement for all extensions.
- We're requiring more extensions to post privacy policies, including extensions that handle personal communications and user-provided content. Our policies have previously required any extension that handles personal and sensitive user data to post a privacy policy and handle that data securely. Now, we're expanding this category to include extensions that handle user-provided content and personal communications. Of course, extensions must continue to be transparent in how they handle user data, disclosing the collection, use and sharing of that data.

Upcoming Chrome OS changes

New certificate verification engine and fallback enterprise policy

Chrome 76 will start rolling out a new certificate verifier. For a few versions, we will provide an enterprise policy that will allow deployments to fall back on the legacy certificate verifier in case of certificate verification regressions or incompatibilities. We will provide more information about this feature in the Chrome 76 release notes.

Adding print server support for CUPS

We're working on a feature to add support for CUPS printing from print servers on Chrome OS. Chrome OS will be able to discover printers on print servers using CUPS. You and your users will be able to configure connections to external print servers and print from the printers on these servers.

User account and file name in IPP Header in Chrome 77

If enabled by policy, all print jobs will include the requesting user account and file name of the document in the IPP header. 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.

Linux apps USB devices

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

Upcoming Google Admin console changes

Remove 20-printer limit for CUPS print management (device settings)

The 20-printer maximum cap will be raised to allow for thousands of printers for each organizational unit in the Google Admin console. If you're interested in testing this new feature, sign up for our Trusted Tester program.

New default policies for printing (CUPS)

There will be new controls for you to manage 2-sided and color printing.

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}, ${MACHINE_NAME}.