chrome enterprise

M73 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.

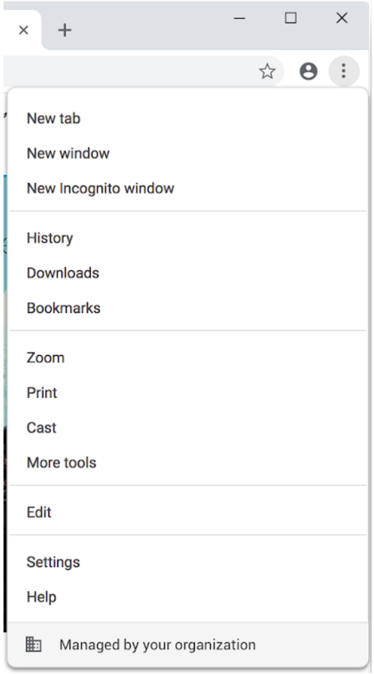
These release notes were last updated on March 12, 2019

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

Chrome Browser updates

Managed by your organization menu item

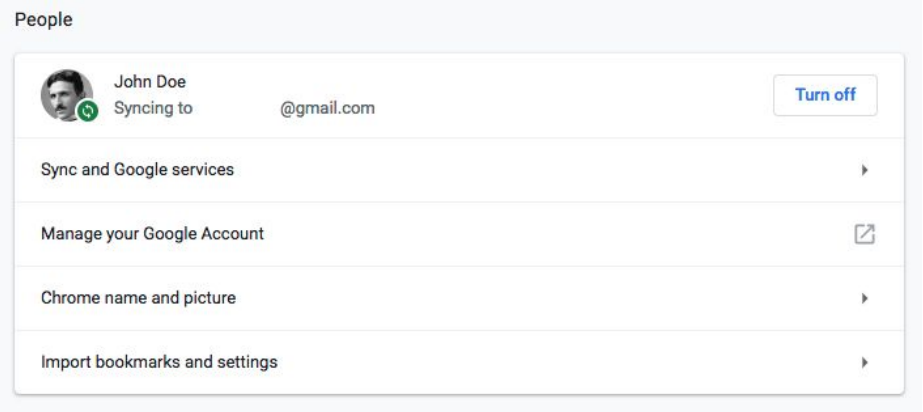
Starting in Chrome 73, when one or more policies are set in Chrome Browser, some users will see a new item on the More menu that indicates that Chrome is being managed. If a user clicks **Managed by your organization**, they are directed to details about Chrome Browser management.



Changes to the Chrome sign-in flow

In Chrome 73, we're rolling out the following changes to Chrome Browser settings:

- When a user turns Chrome sync on, they now get additional features, including an enhanced spellchecker and extended reporting for safe browsing.
- Sync and Google services—A new section that lists all of the settings related to data collected by Google in Chrome Browser. Many of these settings were previously in the Privacy section.
- Make searches and browsing better—A new setting in theSync and Google services section that allows users to control whether features in Chrome Browser can collect anonymous URLs.



People

John Doe
Syncing to @gmail.com

Chrome Browser binaries signed with new digital certificate

Chrome Browser binaries and installer are now signed with a digital certificate issued to Google LLC (rather than Google Inc). There are no changes to the Certificate Authority (CA).

Password Manager enterprise policy for Android now aligned to desktop

The PasswordManagerEnabled policy controls whether the password manager offers to save passwords. On Android, this policy prevented users from viewing passwords that were already saved. Starting with Chrome 73, Chrome Browser on Android will behave like other platforms and allow the user to view their saved passwords.

Progressive Web App support on Mac

In Chrome 73, Progressive Web Apps (PWAs) can now be installed on Apple® Mac®. For details, see Desktop Progressive Web Apps.

Dark mode for Mac

In Chrome 73, if the system theme is set to dark, Chrome Browser on Mac computers will also use a dark theme. Support for Microsoft® Windows® is planned for a future release.

Accessibility improvements

A number of improvements have been made to accessibility in Chrome Browser, including greater contrast and compatibility with screen readers. Some of the improvements include:

- Improved contrast in pop-up boxes, the search box, and tabs (especially when a tab is not active).
- More pop-up boxes correctly report titles to screen-reader software.

- Tabs are now keyboard-accessible.
- Fixes to the way pressing the F6 or Tab key moves through the order of the Chrome Browser toolbar, and other controls, including access to some new UI elements.
- Screen reader now announces additional information, such as the page zoom level when it’s changed and the number of Find results.
- Misleading screen-reader prompts are fixed to reflect current functionality. For example, the correct key combination is now reported when you want to zoom in on a page.
- If a user draws around an element in the UI, there are now improvements in the contrast and appearance of focus rings.

New policy to force networking code to run in the browser process

The network code we use for Chrome Browser is being moved to a separate process. It’s an internal architectural change that wasn't expected to interact with other products. However, we're aware of one report of the move breaking a third-party product that used to inject code into Chrome Browser's process. If this move is causing any issues in your environment, you can temporarily use the ForceNetworkInProcess policy to force networking to run in the browser process. This is a temporary policy that will be removed in the future; there is currently no specific timeline, but we plan to provide 4 milestones notice before removal.

Notice for web developers: Flexbox rendering

Chrome Browser now follows the recommendation from the World Wide Web Consortium for the box model that’s optimized for a UI. Flex items now get the correct minimum size. If you’re a web developer, we recommend that you set the CSS on your webpages with flex items to **min-height: auto**. For details on the change, see Chromium and the Consortium specification.

Notice for developers: Changes to cross-origin requests in extension content scripts

Chrome 73 includes changes to the behavior of cross-origin requests from content scripts. These changes help site isolation protect Chrome users even if a renderer is compromised, but these changes may break extensions that have not yet adapted to the new security model. For instructions on how to verify if a Chrome extension you’re using is affected or to request adding an extension to a temporary allowlist, see Chromium.org.

Chrome OS updates

Managed guest sessions to replace public sessions

In Chrome 73, public sessions are being replaced with managed guest sessions, which provide additional capabilities. Depending on the configuration of the organizational unit that has managed guest session devices, an existing public session device might have the capabilities automatically activated. If so, all certificates, policies, and extensions of the organization will be applied to the managed guest session of this device in the future and no manual changes are required. Learn more about how to manage guest session devices.

eSpeak for Chrome OS

You can set up text-to-speech in dozens of languages on devices running Chrome OS to enhance accessibility. For details, see eSpeak NG.

Pair Bluetooth braille displays with Chromebooks

In addition to supporting USB-refreshable braille displays, you now have the ability to pair braille displays through Bluetooth®. For details, see Use a braille device with your Chromebook.

Audio focus

On Chrome devices that support Android 9.0 Pie and later, apps using audio focuswill now tell Chrome to pause and resume the audio to create a seamless media experience between websites on Chrome Browser, Chrome apps, and Android apps. For details, see Managing audio focus.

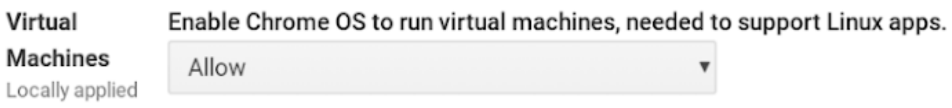
Camera app 5.3 update

Users can now take photos and videos with a 3 or 10-second timer, line up shots with grid options, and use a mirror button that's helpful when using external cameras, such as USB microscopes or document cameras.

Admin console updates

Enable managed Chrome devices to run Linux apps

Last year we announced that consumer users can run Linux apps, including Android Studio on these Chrome devices. With Chrome 73, we're making this feature available on managed devices. Admins can now enable or disable the use of virtual machines that are required to use Linux apps on managed Chrome OS devices. The policy is disabled by default. Admins who want to enable this policy, see Virtual Machines in [Set Chrome device policies](). Users need to follow the steps in [Set up Linux (Beta) on your Chromebook]().



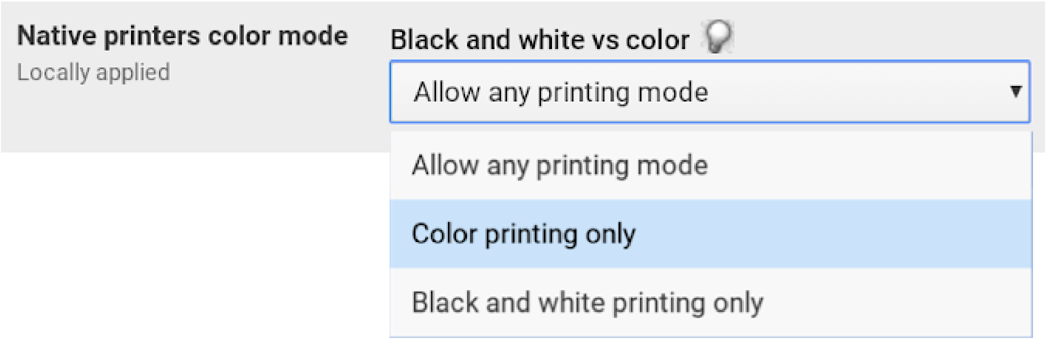
Virtual Machines
Locally applied

Enable Chrome OS to run virtual machines, needed to support Linux apps.

Allow

New default policy for black & white printing (CUPS)

There are new controls for administrators to manage black and white printing capabilities for their users. Controls for 2-sided and color printing are coming soon. If you're interested in getting early access to test printing features, please complete the trusted tester application.



Native printers color mode
Locally applied

Black and white vs color

Allow any printing mode

New and updated policies

Policy	Description
[ExtensionAllowInsecureUpdates]()	Allows insecure algorithms in integrity checks on extension updates and installations. Starting in Chrome 77, this policy will be ignored and treated as disabled.
[DeviceGpoCacheLifetime]() *Chrome OS only*	Specifies the lifetime (in hours) of the Group Policy Object (GPO) cache.
[DeviceAuthDataCacheLifetime]() *Chrome OS only*	Specifies the lifetime (in hours) of the authentication data cache.

ForceNetworkInProcess *Windows only*	Forces networking code to run in the browser process. This policy is disabled by default. If enabled, it leaves users open to potential security issues when the networking process is sandboxed.
ReportDevicePowerStatus *Chrome OS only*	Reports hardware statistics and identifiers related to power.
ReportDeviceStorageStatus *Chrome OS only*	Reports hardware statistics and identifiers for storage devices.
ReportDeviceBoardStatus *Chrome OS only*	Reports hardware statistics for system on a chip (SoC) components.
CloudManagementEnrollmentToken *Browser only*	Enrollment token used for enrolling in cloud management. This replaces the MachineLevelUserCloudPolicyEnrollmentToken policy.
PluginVmLicenseKey *Chrome OS only*	Specifies a PluginVm license key for a device.
ParentAccessCodeConfig *Chrome OS only*	Specifies the configuration that's used to generate and verify a parent access code.

New Chrome OS administrator credential

We are excited to announce the Chrome OS administrator credential. The Chrome OS administrator exam is free and measures the ability to:

- Create, delete, and administer users for a domain
- Configure and manage organizational units
- Manage Chrome devices in the Google Admin console
- Configure and manage security and privacy settings

For details, see Earn your Chrome OS administrator credential.

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.

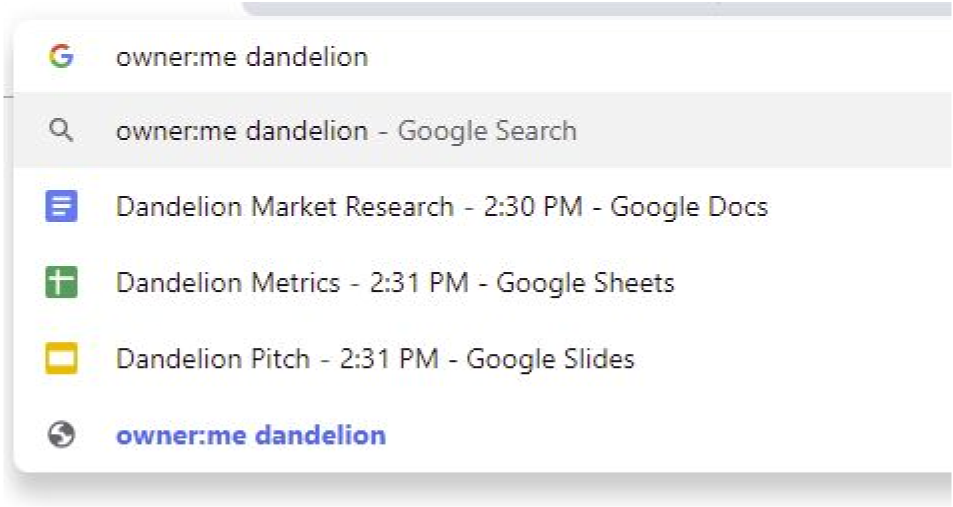
Upcoming Chrome Browser features

Flash blocked by default in Chrome 76

As communicated in the Chromium Flash Roadmap, Adobe® Flash® is planned to be blocked by default in Chrome 76 (stable release beginning end of July 2019). Users will still be able to switch it back to Ask to use Flash by default. This change will not impact enterprises who already configure policy settings for Flash (DefaultPluginsSetting, PluginsAllowedForUrls, PluginsBlockedForUrls). Enterprises will still be able to control this policy as before.

Drive search results in the address bar

Users will see Google Drive results when entering a search in the address bar, including PDFs, Google Sheets, Docs, and Slides.



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

Dark mode for Windows in Chrome 74

In Chrome 74, if the system theme is set to dark, Chrome Browser on Windows computers will also use a dark theme in the UI.

Use a policy to roll back to a previous version of Chrome Browser

We are working on a policy to roll back a Chrome Browser version while retaining account and profile data. The new policy will allow administrators to roll back in conjunction with the existing TargetVersionPrefix ADMX policy. You can send feedback on this feature in the Chromium bug.

Read before using this policy: To make sure that users are protected by the latest security updates, we recommend that they use the latest version of Chrome Browser. **If you roll back to an earlier version, you will expose your users to known security issues.** Sometimes you might need to temporarily roll back to an earlier version of Chrome Browser on Windows computers. For example, your users might have problems after a Chrome Browser version update.

Before you temporarily roll back users to a previous version of Chrome Browser, we recommend that you turn on Chrome sync or Roaming User Profiles for all users in your organization. If you don't, previous versions of Chrome Browser will not use data that was synced from later versions. **Use this policy at your own risk.**

Note: You can only roll back to Chrome Browser version 72 or later

Deprecated policies will remain in the ADMX templates

The ADM and ADMX templates will be modified to keep deprecated and unsupported policies in the output. They will be placed in a dedicated folder and have the same description. The update will make it easier to delete policies after they're deprecated. Learn more about Deprecated Chrome policies.

PacHttpsUrlStrippingEnabled policy will be removed in Chrome 74

If you're using a Proxy Auto Config (PAC) script to configure Chrome's proxy settings, you might be affected by this change. The PacHttpsUrlStrippingEnabled policy strips privacy and security-sensitive parts of https:// URLs before passing them on to PAC scripts used by Chrome Browser during proxy resolution, reducing the chance that sensitive information is unnecessarily exposed. For example, https://www.example.com/account?user=234 would be stripped to https://www.example.com/. If you set this policy to True or leave it on the default value, then there will be no change. If you set this policy to False, you will no longer be able to do so in Chrome 74.

EnableSymantecLegacyInfrastructure policy removed in Chrome 74

The EnableSymantecLegacyInfrastructure policy can be used as a short-term workaround to continue trusting certificates issued by the Legacy PKI Infrastructure formerly operated by Symantec Corporation. This allows time for migrating any internal certificates not used on the public internet. This policy will be removed in Chrome 74. Certificates issued from the Legacy PKI Infrastructure should have replacement certificates issued by public or enterprise-trusted Certificate Authorities (CAs). See Migrate from Symantec certificates.

SSLVersionMax policy will be removed in Chrome 75

The SSLVersionMax policy, which can be used as a short-term workaround while TLS 1.3 is rolled out, will be removed in Chrome 75. This allows time for middleware vendors to update their TLS implementations.

All extensions must be packaged with CRX3 format in Chrome 75

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

Starting with Chrome 75, all force-installed extensions will need to be packaged in the CRX3 format. 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 packaged in CRX2 format and you don't repackage them, they'll stop updating in Chrome 75. And, new installations of the extension will fail. See ExtensionAllowInsecureUpdates.

Site isolation enforced on desktop in Chrome 75

Before shipping site isolation in Chrome 67, we introduced enterprise policies to opt in to site isolation early or opt out of site isolation if users encountered an issue. We've resolved the reported issues and starting with Chrome 75, 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. On Android, the SitePerProcessAndroid and IsolateOriginsAndroid policies will continue to have the ability to disable site isolation. If you run into any issues with the policies, file a bug in Chromium.

ThirdPartyBlockingEnabled deprecation

In the Chrome Enterprise 68 release notes published in July 2018, we announced that the ThirdPartyBlockingEnabled policy will be deprecated in approximately one year (Chrome 77). This announcement was intended as a general deprecation date at some point in the future, but due to feedback and in order to give the ecosystem more time to adapt to the change, the deprecation is currently not targeted for Chrome 77. When a date is set for deprecation, we will announce it in the release notes. We plan to provide 4 notices before removal.

TLS 1.3 downgrade hardening

Chrome Browser enabled TLS 1.3 in Chrome 70. However, due to bugs in some enterprise TLS proxies, a hardening mechanism was temporarily disabled. A future version of Chrome Browser will re-enable this measure. To test networks in Chrome 73:

1. Set **chrome://flags/#enforce-tls13-downgrade Enabled**.
2. Visit a TLS-1.3-enabled server, such as https://mail.google.com.
3. If the connection fails with `ERR_TLS13_DOWNGRADE_DETECTED`, some proxy on the network has the hardening mechanism temporarily disabled.

You should upgrade affected proxies to fixed versions or contact vendors if no fix is available. 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.

Legacy browser support planned to be incorporated into Chrome 75

Legacy browser support functionality is being incorporated into Chrome Browser, and the separate extension will no longer be needed. We will keep the extension in the Chrome Web

Store for the foreseeable future so customers on older versions of Chrome Browser can continue to use legacy browser support. If you're interested in getting early access to test legacy browser support integration, please complete this interest form.

Pop-ups will not be allowed on page unload

In Chrome 74, we will no longer allow pop-ups during page unload. See the removal notice. We've been notified that this might break some enterprise apps so a temporary policy will be made available to allow pop-ups on page unload when Chrome 74 launches. This temporary policy is planned to be removed in Chrome 76.

Upcoming Chrome OS changes

New search feature in Chrome 74

We're adding a search feature so users can access recent queries and suggested apps without having to enter anything. Every time a user moves their cursor to or clicks the search box, but does not start entering text, they will get search suggestions. Users will also be able to remove recent queries that they no longer want to see and use suggested text to complete their query.

Adding print server support for CUPS

We are 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. Users and administrators will be able to configure connections to external print servers and print from the printers on these servers.

Notifications on lock screen

Coming soon, when looking for notifications, a message saying that notifications are hidden will show up. Next to the message, users can click a button to enable notifications. Users must authenticate and give permission to show notifications on lock screen. A full password will be required, even if other authentication methods, such as PIN or fingerprint are available.

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. This added functionality will provide additional information about the print job that enables third-party printing features, such as secure printing and print usage tracking, if supported.

Annotations in PDF viewer

When viewing a PDF on a device running Chrome OS, you will be able to tap a button to annotate the PDF with pen and highlighter tools.

Linux apps USB devices

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

External camera support for the Camera app

External USB cameras will be supported by the Camera app.

Upcoming Admin console changes

Remove 20-printer limit for CUPS print management

Soon, the 20 printer maximum cap will be raised to allow for several thousand printers for each organizational unit in the Google Admin console. If you're interested in testing the new feature, please join our trusted tester program.

New default policies for printing (CUPS)

Soon, there will be new controls for administrators to manage printing capabilities for their users for duplex printing. Admins will be able to set defaults or restrict whether users can or cannot use duplex 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.