



M75 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 June 5, 2019

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

[Chrome 75](#)

[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 Admin console changes](#)

Sign up [here](#) for our email distribution for future releases.

Chrome 75

Chrome Browser updates

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

This change was originally planned for Chrome 75 but it's now scheduled for 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](#). 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.

Roll back to Chrome 72 or later on Windows

Chrome 75 on Microsoft® Windows® will allow administrators to roll back to Chrome 72 or a later version.

To make sure that users are protected by the latest security updates, we recommend that users are on the latest version of Chrome Browser. Running earlier versions of Chrome Browser exposes your users to known security issues. Before using this policy, see [Roll back Chrome Browser to a previous version](#) for important information about preserving user data.

Use policy to remove extensions (rather than just disable)

Starting in Chrome 75, extensions can now be removed by modifying the `installation_mode` setting in the Extension Settings policy and setting the "remove" flag. For details, see [Chromium](#).

PacHttpsUrlStrippingEnabled policy removed

As we announced in the Chrome 74 release notes, the `PacHttpsUrlStrippingEnabled` policy has now been removed. If you're using a Proxy Auto Config (PAC) script to configure Chrome's proxy settings, you might be affected by this change, especially if your PAC script depends on anything other than the scheme, host, or port of incoming URLs.

PAC HTTPS URL stripping removes 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/`. This behavior will now be enforced in Chrome 75.

EnableSymantecLegacyInfrastructure policy removed

As we announced in the Chrome 74 release notes, the `EnableSymantecLegacyInfrastructure` policy

has now been removed. The policy was used as a short-term workaround to continue trusting certificates issued by the Legacy PKI Infrastructure formerly operated by Symantec Corporation. The workaround allowed time to migrate any internal certificates that are not used on the public internet.

Certificates issued from the Legacy PKI Infrastructure should have been replaced with certificates issued by public or enterprise-trusted Certificate Authorities (CAs).

SSLVersionMax policy removed

As we announced in Chrome 74 Release Notes, the SSLVersionMax policy has now been removed. This policy was used as a short-term workaround while TLS 1.3 was rolled out to allow time for middleware vendors to update their TLS implementations.

Policy to control Signed HTTP Exchange

You can use Signed HTTP Exchange to safely make content portable or available for redistribution by other parties, while keeping the content's integrity and attribution. Portable content has many benefits, such as enabling faster content delivery, facilitating content sharing between users, and simpler offline experiences.

Starting in Chrome 75, you can enable or disable Signed HTTP Exchange using the [SignedHTTPExchangeEnabled](#) policy.

CompanyName and LegalCopyright fields updated

Chrome 75 changes the CompanyName and LegalCopyright fields in the version resource of Windows binaries (for example chrome.exe and chrome.dll). "Google Inc." is now "Google LLC" and "Copyright 2018 Google Inc. All rights reserved." is now "Copyright 2019 Google LLC. All rights reserved."

Control precedence between Chrome Browser Cloud Management and platform policies

You can use CloudPolicyOverridesPlatformPolicy to control how policies from Chrome Browser Cloud Management interact with policies set at the platform level (for example, through the Group Policy Management Editor). This policy can be useful if you're transitioning from managing browsers through Group Policy Object (GPO) to Chrome Browser Cloud Management.

When set to false (default), the order of precedence is Machine platform > Machine cloud > User platform > User cloud.

With the policy set to true, the order of precedence is Machine cloud > Machine platform > User platform > User cloud.

The policy can only be set as a machine platform policy. For more details, see [Chromium](#).

Merge list policies from multiple sources

You can now merge policies that take a list of values that are set from multiple sources, including the cloud and by platform and Microsoft® Active Directory®. Before, if multiple lists from different sources conflicted, only one list was applied. For details, see [PolicyListMultipleSourceMergeList](#).

Chrome Remote Desktop on the web now available

You can now use Chrome Remote Desktop on the web. In turn, **the Chrome Remote Desktop app will not be supported after June 30, 2019**. New and existing users can switch to the new version on the web.

To set it up:

1. Go to [Chrome Remote Desktop](#).
2. In the upper-right corner, click **Remote Access**.
3. Click **Remote Support** to get support from a trusted friend or family member, or to give support to someone else.

You can control whether users can access other computers from Chrome using Chrome Remote Desktop. For details, see [Control use of Chrome Remote Desktop](#).

Improved tab life cycle management

Some users will start to see improved CPU and memory usage as Chrome 75 rolls out. The TabLifeCyclesEnabled policy reduces the CPU usage on browser tabs that haven't been used for a long time. Set the policy to true or leave it unspecified to enable it. For details, see [Chromium](#).

Users can check Chrome Browser and OS management

In Chrome 75 we're enhancing the visibility features for both browser and OS with transparency view, a new view which shows users the extent to which their device and account are managed by their administrators in enterprise environments. The new transparency view focuses on reporting functionality ("Which data is visible to my administrator?") as well as force-installed extensions ("Which data may be accessed by force-installed extensions?").

Chrome OS updates

Linux on Chromebooks:

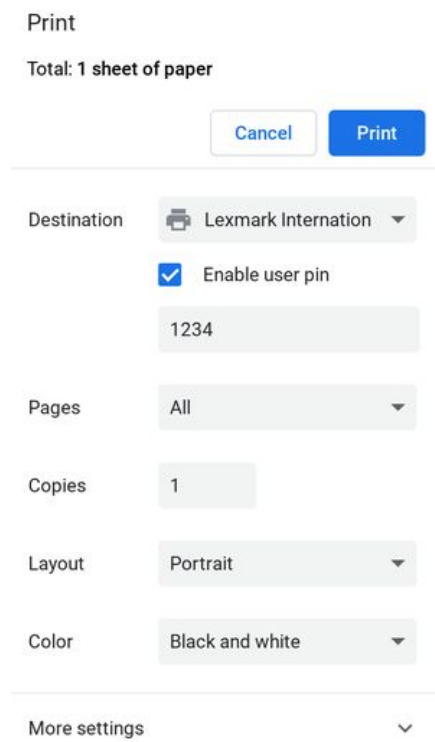
Support for VPN connections—Linux applications can now utilize VPN connections through an existing Android or Chrome OS VPN connection. All traffic from the Linux VM will automatically be routed through an existing (established) VPN connection.

Support for Android devices over USB—Android devices connected over USB can now be accessed by Linux apps. Users must choose to share the USB device with Linux before they can access it.

Add support for PIN code with native printers

PIN code printing will be available which will allow users to enter a pin code when sending the print job, and release the print job for printing when they enter the pin code into the printer keypad. This gives users more control over when a print job is printed so documents aren't lying unattended at the printer. And because a user has to actively request their print job be released, it also reduces waste.

PIN printing will be enabled if the user's Chrome device is managed, and the printer supports IPPS communication and the IPP attribute for "job-password".



Print

Total: 1 sheet of paper

Cancel Print

Destination Lexmark International

Enable user pin

1234

Pages All

Copies 1

Layout Portrait

Color Black and white

More settings

Add support for Document Providers in Files app

To expand support for third-party file providers on Chrome OS, when users install the app of a third-party file provider that implements the DocumentsProvider API, a root for the third-party file provider will appear in the side navigation of the Chrome Files app. For more details, see [Documents Provider](#).

Extending protected content on secondary displays

Digital rights management (DRM)-protected content can now be shown on an external display.

BLE advertising in Chrome apps flag removed

The #enable-ble-advertising-in-apps flag (about://flags) will be removed in Chrome 75. If you or any developers use BLE Advertising APIs, you should debug the functionality in a kiosk session, rather than in a regular user session.

Admin console updates

Force devices to automatically re-enroll after wiping (change to forced re-enrollment behavior)

Starting in June 2019 (with an incremental rollout), you can automatically re-enroll devices if they're wiped. Previously, forced re-enrollment required a user to enter their username and password to complete re-enrollment. A few weeks after the roll out is complete, automatic re-enrollment will be the default for new customers as well as existing customers who have not changed the default forced re-enrollment setting. To control the setting, see [Force wiped Chrome devices to re-enroll](#).

New and updated policies (Chrome Browser and Chrome OS)

Policy	Description
AlternativeBrowserParameters <i>Chrome Browser only</i>	Controls command-line parameters to launch to an alternative browser
AlternativeBrowserPath <i>Chrome Browser only</i>	Controls which command to use to open URLs in an alternative browser
CloudPolicyOverridesPlatformPolicy <i>Chrome Browser only</i>	Cloud policy that overrides Platform policy
PolicyListMultipleSourceMergeList	Allows merging list policies from different sources
SignedHTTPExchangeEnabled	Enables support for Signed HTTP Exchange (SXG)
SpellcheckLanguageBlacklist <i>Windows, Linux, Chrome OS only</i>	Disables unrecognized spellcheck languages

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

Flash blocked by default in Chrome 76

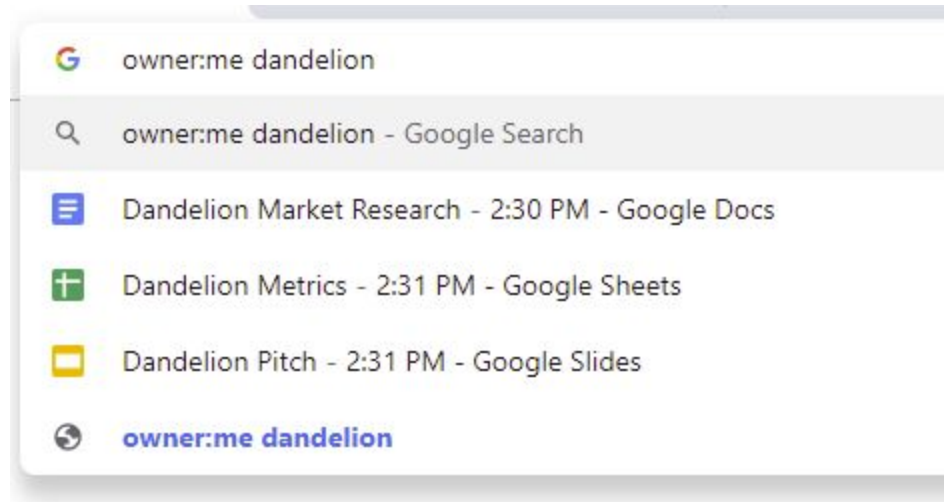
As communicated in the Chromium Flash Roadmap, Adobe® Flash® will be blocked by default in Chrome 76. Users can manually switch back to ASK ("Ask first") before running Flash. This change won't impact existing policy settings for Flash. You can still control Flash behavior using [DefaultPluginsSetting](#),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

Site isolation enforced in Chrome 76

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 and 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. 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](#).

Drive integration in the address bar

Soon, 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](#).



Removing --disable-infobars in Chrome 76

Chrome 76 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 will be added to allow you to disable some security warnings.

Policy atomic groups introduced in Chrome 76

In order to ensure predictable behavior from policies that are tightly coupled with other policies, some policies will be regrouped in atomic policy groups. These groups will help ensure that all the applied policies from a single group come from the same source, which is the source with the highest priority. This change will help prevent unpredictable behavior when mixing multiple sources of policies.

Merge policies with dictionary of values in Chrome 76

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 one dictionary will have an effect. For details, see [PolicyDictionaryMultipleSourceMergeList](#).

Flag removal, starting with Chrome 76

Many flags in `chrome://flags` will be removed in upcoming Chrome versions. You should not use flags to configure Chrome Browser because they are not supported. Instead, configure Chrome Browser for your enterprise or organization using policies.

Improvements to version rollback

A future version of Chrome will improve the rollback experience on Windows by preserving some user data during the rollback process.

Upcoming Chrome OS changes

Print jobs to include user account and file name

If the printer or print service support IPPS with IPP attributes for `requesting-user-name` and `document-name`, you will be able to have print jobs include the user account and file name to help with print tracking and follow-me printing.

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.

Notifications on lock screen

You will be able to set up a requirement for users to 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 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 apps running on a Chromebook, so that Linux applications can access the Linux instance.

Upcoming 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}`.