chrome enterprise

M72 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 January 31, 2019

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

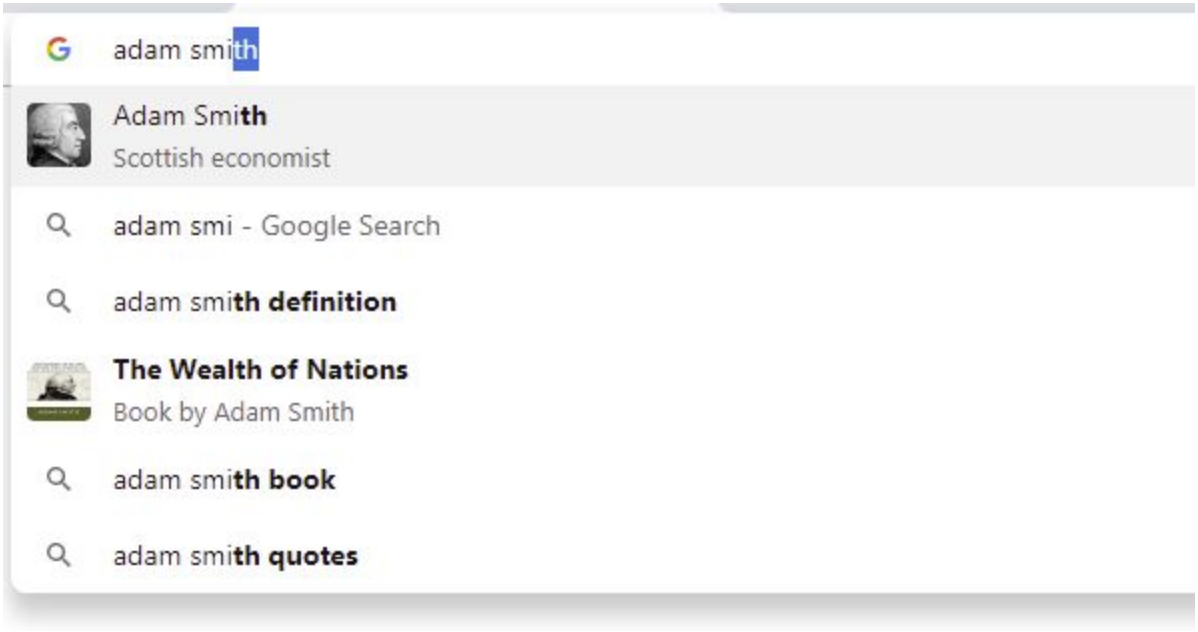
Sign up **here** for our email distribution for future releases.

Chrome 72

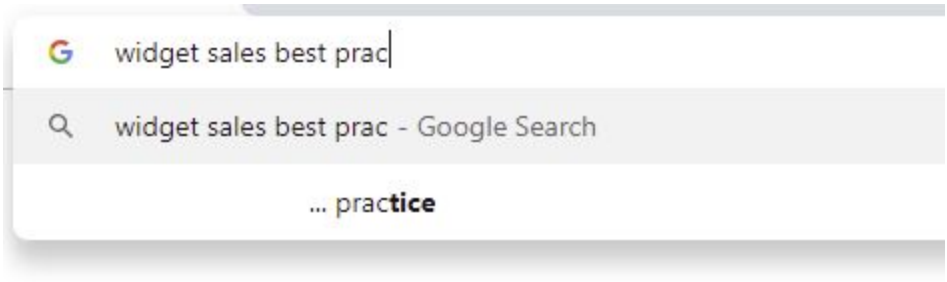
Chrome Browser updates

- **New search result types**

  In Chrome 72, you'll get 2 new types of search results when you search from the address bar. You'll get results based on entities—people, things, places, and so on. These results will contain the search text, an image of the entity you're searching for, and a short description.



You'll also get suggestions to complete the end of a search string. For example, if you search for "widget sale best prac…", you'll get a suggestion for "practice" as a completion to your search.



- **Cleanup tool quarantines—instead of deleting—files it detects as malicious**
  If you use the Chrome Cleanup tool on Microsoft® Windows® computers, files detected as malicious will now be quarantined rather than deleted. This update will help lessen the risk of safe files being mistakenly deleted. Learn more about removing unwanted programs and the Chrome Cleanup tool policy.

- **Save payment information to a Google Account**
  In Chrome 72, users who are signed in to their managed Google Account will now see an option to save their payment information to their Google Account. As an administrator, you can turn off this feature (Sync Service setting) in the Google Admin console or by using the AutofillCreditCardEnabled policy.

- **Support for Windows 10 U2F and web authentication APIs**
  If you use the most recent version of Windows 10, you'll have added support for Universal 2nd Factor (U2F) and WebAuthn—standards that enable web authentication through security keys instead of passwords. U2F and WebAuthn are only supported on the most recent versions of Windows 10: either current Insider Preview builds or the forthcoming 19H1 release ("Redstone 6"). Integration with these APIs enables Windows Hello support through WebAuthn and support for NFC tokens. USB and Bluetooth Low Energy (BLE) devices should continue to work, although Windows UI will now be displayed. Any

organizations that depend on U2F or WebAuthn, and are using sufficiently recent Windows builds, should verify that this feature works correctly before rolling it out.

- **EnableSha1ForLocalAnchors policy**
  Enterprises that needed time to migrate following the 2014 announcement to sunset SHA-1 were able to configure an enterprise policy to enable support for SHA-1 for locally installed, privately trusted Certificate Authorities. This support has now been removed in Chrome 72. Enterprises that rely on server certificates that use the SHA-1 algorithm in the certificate chain will find that Chrome 72 will refuse to connect, presenting an untrusted certificate error. These certificates should be replaced with SHA-2 certificates to avoid any disruption.

- **New welcome experience (Windows)**
  When you start Chrome Browser for the first time on Windows, you'll see a new welcome page, unless you're on a device that's joined to a Microsoft® Active Directory® domain.

- **Changes to sign-in behavior with Chrome 72**
  In Chrome 72, a small percentage of users will now see the following changes to the Chrome sign-in behavior. A wider roll-out of these features will happen in Chrome 73:
    - When a user turns Chrome sync on, they now get additional features, including "Enhanced spell check" and "Safe browsing extended reporting."
    - The Chrome settings page includes a new section—Sync and Google services—which lists all of the settings related to data collected by Google in Chrome Browser. Many of these settings were previously under "Privacy".
    - A new setting, "Make searches and browsing better" will appear under "Sync and Google services" on the settings page. This allows users to control whether features within Chrome can collect anonymized URLs.

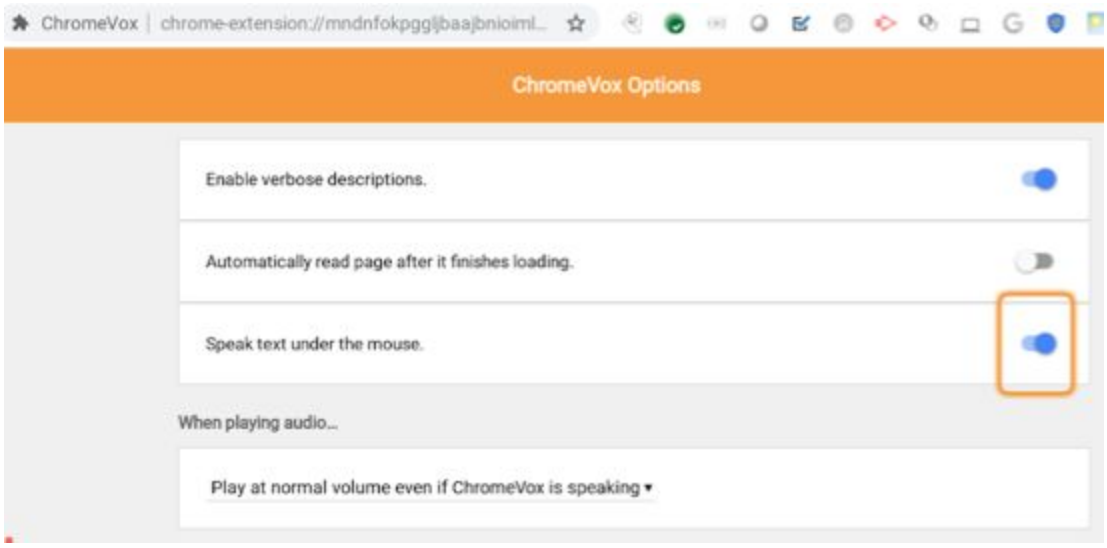
Chrome OS updates

- **USB connections on locked devices**
  Chrome 72 will offer initial support to ignore some types of USB connections on locked devices that are running Chrome OS including printers, scanners, and storage devices. USBGuard is on by default beginning with Chrome 72. If issues are detected, admins can disable this feature through chrome://flags.

- **Android app shortcuts in launcher search**
  Users can now search for app shortcuts in the launcher search. For example, users can search for Compose and be taken to the exact related app, such as a new blank message in Gmail.

- **New drawing app for Chromebooks**
  Chromebook users now have the Canvas app for drawing.

- **ChromeVox screen reader update**
  ChromeVox users with low vision can now opt to have the screen reader read anything under their mouse cursor. This feature can be enabled through the setting “Speak text under the mouse” in the ChromeVox options page.



- **Android 9.0 support coming to certain Chrome devices**
  Devices running Chrome OS that currently support Android 7.0 Nougat will be upgraded to support Android 9.0 Pie. We’ll include more information in future release notes when it comes available.

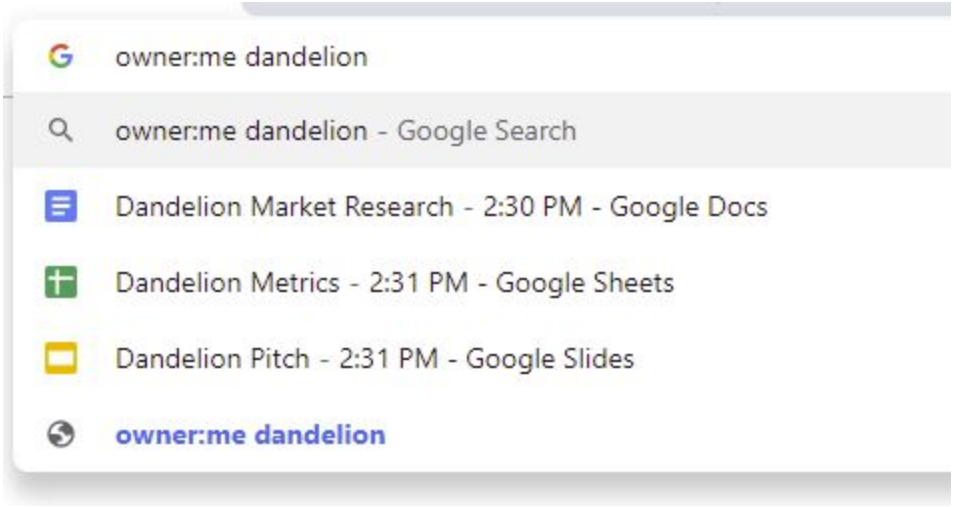
Coming soon

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

- **Drive search results in the address bar**

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



- **Roll back Chrome Browser version with policy**

  Many enterprise customers have asked Google to provide a version rollback mechanism. We are working on a policy to roll back Chrome Browser while retaining account and profile information. This will allow administrators to enable a rollback in conjunction with the existing TargetVersionPrefix ADMX policy. If the Chrome version updater cannot rollback the browser, the chrome://policy page will contain an error message and the existing release will continue to function. Only the latest release of Chrome is officially supported, so if an admin rolls back to an older version they do so at their own risk. You can provide feedback to the engineering team on this feature on Chromium.

- **Deprecated policies will remain in the ADMX templates**

  Deprecated policies will be placed in a dedicated folder in the ADMX templates and have the same description. This change will make it easier for administrators to delete policies after they're deprecated. Learn more about Deprecated Chrome policies.

- **Changes to the sign-in behavior with Chrome 73**

  The updates described above in Changes to the sign-in behavior with Chrome 72 will be rolled out for all users in Chrome 73.

- **PacHttpsUrlStrippingEnabled policy will be removed in Chrome 74**

  The 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. For example, `https://www.example.com/account?user=234` will be stripped to `https://www.example.com/`. If you set this policy to True or leave it on its default value, then there will be no change. However, in Chrome 74, you will no longer be able to set it to False.

- **EnableSymantecLegacyInfrastructure policy will be removed in Chrome 74**
  The EnableSymantecLegacyInfrastructure policy will be removed in Chrome 74. This policy is intended 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 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 was a short-term work-around while TLS 1.3 is rolled out. This allows time for middleware vendors to update their TLS implementations. The policy will be removed in Chrome 75.

- **All extensions must be packaged with CRX3 format by Chrome 75**
  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.This change has been made because CRX2 uses SHA1 to secure updates to the extension. Breaking SHA1 is technically possible. So, an attacker might intercept the extension update and inject arbitrary code into it. CRX3 uses a stronger algorithm, avoiding this risk.

  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. New installations of the extension will fail.

- **Site isolation will be enforced on Chrome 75 (Desktop)**
  Before shipping Site Isolation in Chrome 67, we introduced enterprise policies that enterprises could use to opt in to Site Isolation early or opt out of Site Isolation if they 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 using the SitePerProcess or IsolateOrigins policies on desktop. We tentatively plan to move Chrome 75 to the stable channel in June 2019.

  Notes:
  - This change only applies to desktop platforms. On Android, SitePerProcessAndroid and IsolateOriginsAndroid policies will continue to have the ability to disable Site Isolation.
  - If you run into any issues with the SitePerProcess or IsolateOrigins policies, file a bug in Chromium.

Upcoming Chrome OS changes

- **External camera support for Camera app**
  External USB cameras will be supported by the Google Camera app.

- **Users can allow notifications on lock screen**
  When looking for notifications, a message saying that notifications are hidden will show up. Next to it is a button to enable notifications, which will require the user to authenticate and give permission to show notifications on lock screen. A full password will be required, even if other authentication methods, such as a PIN or fingerprint, are available.

- **Always-on VPN for managed Google Play**
  Currently, Admins can install Android VPN apps on Chromebooks, however, users have to start the VPN app manually. Soon, admins will be able to set an Android VPN app to start a connection when a device is turned on and direct all user traffic (Chrome OS and Android) through that connection.

- **User account / Filename in IPP Headers**
  If enabled by policy, all print jobs can include the requesting user account and file name printed in the IPP header. This new feature will provide additional information about print jobs that enable third-party printing features, such as secure printing and print-usage tracking.

- **Annotations in PDF Viewer**
  When viewing a PDF in Chrome, you will be able to tap a button to add notes to the PDF with a pen and highlighter tools.

- **Linux container support for USB devices**
  From the Chrome Shell (crosh), you will be able to attach a USB device to Linux running on Chrome devices (Crostini) so that Linux applications can access the Linux instance.

Upcoming Admin console changes

- **Native printing (CUPS) improvements**
  - **Printing limit lifted**—The 20 printer maximum cap will be raised to allow for several thousand printers for each organizational unit in the Google Admin console.
  - **Set default for 2-sided and black and white printing**—Controls are coming for administrators to manage printing capabilities for their users around 2-sided printing and black and white printing. Admins will be able to set defaults or restrict these print options with CUPS (native printing).

- **Managed guest session support for managed Google Play**
  A setting in the Google 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.