chrome enterprise

M71 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 December 13, 2018

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 71

Chrome Browser updates

- **Change to using PAC scripts to configure proxy settings in Chrome**
  If you're using a Proxy Auto Config (PAC) script to configure Chrome's proxy settings, you might be affected by this change. This is especially so if your PAC script depends on anything other than the scheme, host, or port of incoming URLs.

  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/`.

This policy will change the default value from False to True to improve security. If you already set this policy to True, there's no impact. If you set it to False, there's no immediate impact. If you haven't set this policy and are relying on the default, test this change to see how your PAC scripts operate.

This policy will be removed in a future release when PAC stripping becomes the default for Chrome.

- **Deprecate trust in remaining Legacy Symantec PKI Infrastructure**
  This change is present in all release channels: Canary, Dev, Beta, and Stable. Users observing the distrust in Chrome 70 should experience the exact same behavior in Chrome 71 and later. For a small percentage of users, Chrome 71 will be the first time they experience the distrust, which could result in more problems involving related errors.

  Find instructions on how to determine whether a site is affected and any corrective action needed, as well as a description of past changes.

Chrome OS updates

- **Fingerprint and PIN enrollment in Chrome device Out of Box Experience (OOBE)**
  For tablets that support fingerprint and/or PIN, users can enroll a fingerprint or set up a PIN while signing in to the device for the first time.

- **Connect to your Android phone**
  Users can connect with their Android phone using a single setup flow to enable Smart Lock, instant tethering, and Android Messages PWA. Android Messages PWA gives users the ability to see, reply to, and start text messages.

- **Android Messages for Chrome OS**
  Users can text from their Chrome OS by connecting with their Android phone.

- **Print multiple pages per sheet on native (CUPS) printing**
  Native printers using CUPS now support rendering multiple pages of content onto a single sheet of paper. Previously only available for Cloud Print printers, this is now available for all printing destinations.

Admin console updates

- **Managing site isolation policies**
  Site isolation policies on the desktop get updated to reflect that they're on by default. (They include controls to turn off site isolation or add specific site rules.) New policies are added to the Admin console for Chrome on Android. For more, see Protect your data with site isolation.

New and updated policies

Policy	Description
AllowWakeLocks *Chrome OS only*	Allow wake locks. Specifies whether wake locks are allowed. Wake locks can be requested by extensions through the power management extension API and by ARC apps.
NetworkFileSharesPreconfiguredShares *Chrome OS only*	List of preconfigured network file shares.
NTLMShareAuthenticationEnabled *Chrome OS only*	Network File Share feature. This policy controls enabling NTLM as an authentication protocol for SMB mounts.
SmartLockSigninAllowed *Chrome OS only*	Allow Smart Lock Sign-in to be used.
VpnConfigAllowed *Chrome OS only*	Allow the user to manage VPN connections.
WebUsbAllowDevicesForUrls	Automatically grant permission to these sites to connect to USB devices with the given vendor and product IDs.

Deprecations

- **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. Support would be removed in January 2019 at the latest, which corresponds to 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.

- **SupervisedUserCreationEnabled policy (deprecated in Chrome 70)**

Read about consumer supervised users.

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

- **The Chrome Cleanup Tool will quarantine—instead of deleting—files it detects as malicious**
  The Chrome Cleanup Tool helps users remove unwanted software on their computers. The removal process includes deleting malicious files in the system. However, to lessen the risk of safe files being erroneously deleted, files will be moved into quarantine instead of getting deleted permanently. For more, learn about removing unwanted programs and the Chrome Cleanup Tool policy.

- **PacHttpsUrlStrippingEnabled policy (scheduled to be deprecated in Chrome 74)**
  See the above note on Change to using PAC scripts to configure proxy settings in Chrome.

- **SSLVersionMax policy (scheduled to be deprecated in Chrome 75)**
  SSLVersionMax can be used as a short-term workaround 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.

- **Third-party code injection**
  The Chrome 70 release notes stated that in Chrome 71, third-party code blocking will be enabled by default for everyone, including domain-enrolled users. However, due to an issue with anti-virus file scanning, we're delaying this change until we have a solution that better covers customers' needs.

- **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.

  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.

  Why is this change happening?
  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.

Upcoming Chrome OS changes

- **Always-on VPN for managed Google Play**
  Admins can install Android VPN apps on Chromebooks. However, users have to start the VPN app manually.

  Soon, admins can 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. If the connection fails, all user traffic is blocked until the VPN connection is re-established. VPNs in Chrome OS don't apply to any system traffic, such as OS and policy updates to prevent security exploits.

- **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. Dates and affected devices haven't been announced. We'll include more information in future release notes when it comes available.

Upcoming Admin console changes

- **Native printer-management improvements**
  The 20 printer maximum cap will be raised to allow for several thousand printers for each organizational unit in the Google Admin console.

- **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.