chrome enterprise

M69 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 August 20, 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.

Call for Trusted Testers

Become a Chrome Enterprise Trusted Tester and test new Chrome features in your environment. You'll provide feedback directly to our product teams so we can develop and prioritize new features. If you'd like for your organization to participate, complete this form. We'll follow up with more details.

We're looking forward to working with you!

New in M69

New and updated policies

Policy	Description
AllowedUILocales *Chrome OS only*	Configures the allowed UI locales in a user session. This policy replaces the AllowedLocales policy.
OverrideSecurityRestrictionsOnInsecureOrigin	Specifies a list of origins (URLs) for which security restrictions on insecure origins will not apply. This policy replaces UnsafelyTreatInsecureOriginAsSecure. The policy now applies to Chrome OS and Android.
PasswordProtectionChangePasswordURL	Configures the change password URL.
PasswordProtectionLoginURLs	Configures the list of enterprise sign-in URLs where the password protection service should capture password fingerprints for reuse detection.
PasswordProtectionWarningTrigger	Configures the password protection warning trigger.
UsageTimeLimit *Chrome OS only*	Configure the time limit for a user session or device usage per day.

Chrome Browser updates

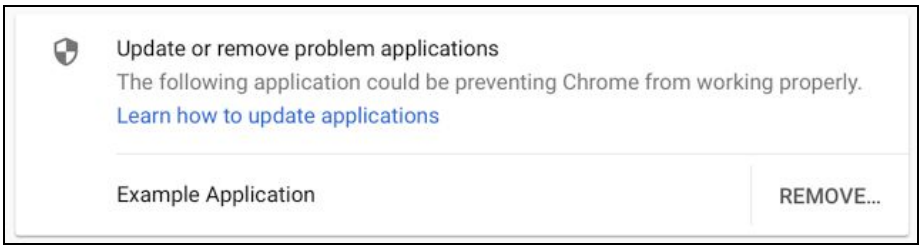
Password Alert policy

Password Alert has been a popular extension with enterprises for the past few years to protect Google Accounts. With the release of Chrome 69, we're adding password alert as a policy for Chrome Browser to allow you to specify both Google and non-Google Accounts. If your users sign-in to websites that aren't whitelisted by your organization or are flagged as suspicious, they'll get a warning that prompts them to reset their password. Preventing password reuse across multiple websites can protect your organization from compromised accounts.

Reduce Chrome crashes caused by third-party software

Third parties can sometimes inject code that disrupts the stability of Chrome Browser. In Chrome 66, we introduced on-screen warnings that alerted users when a third-party injects code. In Chrome 69, third-party code is now blocked by default. If you still use software that injects code into browser processes, you can temporarily enable access using the new ThirdPartyBlockingEnabled policy.

Here is the warning users will see on their computers when this policy is enabled:



Please note that this blocking feature was previously scheduled for M68, but is now scheduled for M69.

On-premise reporting

You can use a new reporting tool for Chrome Browser that provides insight into the browser, its resource consumption, and policy compliance. You can use Chrome Reporting Extension and a companion application on user machines to enable reporting. Use policies to specify what to monitor. Browser data is stored in a local file on disk in JSON format, which you can integrate with on-premise reporting and analytic tools, such as Spunk® or Sumo Logic®. For details, see Track Chrome Browser usage and events.

Browser interface changes

Chrome Browser will have a new design across all operating systems. Highlights include Microsoft® Windows 10® notification-center integration, touchpad gesture navigation on Windows, and autofill updates.

Flash deprecation

Last year, Adobe announced it will stop updating and distributing Adobe Flash™ at the end of 2020. Starting with Chrome 69, every time users restart Chrome Browser, they will have to grant permission for sites to use Flash. This update won't impact your enterprise settings. You can continue to use the DefaultPluginsSetting, PluginsAllowedForUrls, and PluginsBlockedForUrls policies to configure Flash behavior. Only user-configured settings will be impacted. For details, see the Flash roadmap on Chromium.org. Flash will not be supported after December 2020.

Update to Legacy Browser Support extension

The Legacy Browser Support extension for Chrome has been updated to version 5.4. You can now specify more precise rules in URL lists to make managing multiple sites hosted on the same domain simpler. The update also improves support for automatically generated Microsoft® Internet Explorer® site lists. If you deploy the native Legacy Browser Support companion MSI manually, make sure to get the newest extension version to avoid mismatches with the extension version.

Improvements to Chrome management with Intune

Policies that are only available on Microsoft® Windows® instances that are joined to a Microsoft® Active Directory® domain can now be configured with Intune. This applies even on Windows instances not

joined to a domain. This is supported on the Windows 10 Pro and Enterprise editions. For details, see Manage Chrome Browser with Microsoft Intune.

Chrome OS updates

Linux (Beta) for Chromebooks

Important:

- This feature is currently only supported on unenrolled Chrome devices and not available for managed Chrome devices.
- This feature is only available on the latest Chrome devices. See Chromium.org for a list of Chrome device boards that support VMs.

Linux (Beta) for Chromebooks allows developers to use editors and command-line tools by adding support for Linux on a Chrome device. After developers complete the set up, they'll see a terminal in the Chrome launcher. Developers can use the terminal to install apps or packages, and the apps will be securely sandboxed inside a virtual machine.

Try this out on an unmanaged device:

1. Go to **Settings > Linux (Beta)**
2. Click **Turn on**.
    a. Note: If you don't see Linux (Beta) in your Chrome OS settings, either you're using a managed Chromebook, or you haven't yet updated to Chrome OS 69 or later.
3. Click **Install** in the **Set up Linux (Beta) on your Chromebook** dialogue window that appears.
    a. Linux can take a few minutes to install. Once installation is complete, a terminal window will appear.

Voice dictation from anywhere

Voice-to-type functionality has been available on Chromebooks for some time through the on-screen accessibility keyboard or the virtual keyboard's microphone icon. However, many of our users have asked to make dictation a standalone feature separate from the accessibility keyboard. Chrome 69 now offers dictation as a separate accessibility feature. With dictation enabled, a small button will appear at the bottom of the desktop. Also, when input focus is in a text edit area, users can click a button to start dictating or press **Search+D** and use their voice to input text.

Global text-to-speech settings

In Chrome 69, we're launching a new global text-to-speech settings page that's available in your accessibility settings. Users can set a system-wide synthesized voice, language, pitch, and rate. We're also working on making this setting smoother for any users who have non-default voice settings in the ChromeVox screen reader options page or the Select-to-speak options page.

Files app improvements

Native support for Team Drives in the Files app is targeted for Chrome 69. We're also working on making managed Google Play on Chrome OS files available as read/write with the Files app. And, we'll be making updates to improve the organization of local versus cloud file storage.

Night Light support on Chromebooks

To reduce eye strain and improve sleep, users can manage the color of their device displays throughout the day using Night Light. Users can use a preset sunrise and sunset schedule and suggested tint. Or, they customize their daily schedule and color temperature from a spectrum of colors.

Visual updates for enterprise device enrollment

The device enrollment flow will be updated to match the visual styling of the rest of the Chrome OS out-of-box experience (OOBE). Functionality will not be affected. If you automate the out-of-box experience using USB devices, you should update your automation steps as appropriate.

Admin console updates

Support for enterprise mobility management (EMM) coexistence for Android

Previously, domains that had a third-party enterprise mobility management (EMM) provider bound to their domain could not manage Android apps on Chromebooks from the Google Admin console. This caused the **Allow Install** button in the Admin console to be disabled. Also, some users saw an empty Play Store if their company was using an EMM to install Android apps outside of Google Play. With this change, administrators will be able to assign separate sets of Android apps for their Chrome and Android users from their respective consoles. The steps to manage apps remain the same.

Android app installation improvements

The most commonly used Android apps on a Chromebook will see performance improvements now that force-installed apps on Chromebooks can now be kept as cached local copies. This improvement reduces the time it takes to install apps and network traffic usage.

Deprecations

SigninAllowed policy deprecation

The SigninAllowed policy has been deprecated since Chrome 40. It will be removed from Chrome completely in Chrome 71. If you're still using this policy, you need to transition to supported alternatives. For example, you can use the SyncDisabled policy to control the availability of the Chrome Sync feature.

CRX2 deprecation

Starting with Chrome 70, all non-force-installed extensions must be packaged in the CRX3 format. Extensions signed and hosted in the Chrome Web Store have been automatically converted, but 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. Starting with Chrome 75, this restriction will also apply to force-installed extensions.

Coming soon

Upcoming Chrome Browser features

Redirect protection

We're working on a new security feature that blocks redirects from cross-domain iframes. To test if sites used by your organization are affected, you can visit these sites by going to chrome://flags/ and enable the flag #enable-framebusting-needs-sameorigin-or-usergesture.

Upcoming Chrome OS features

Enable key remapping for external keyboards

This feature will allow users to remap the Search, Command, and Windows keys on external keyboards through keyboard settings. If an Apple® keyboard is attached to a Chromebook, the external keyboard setting defaults to the Control key. Other external keyboards default to the Search or Launcher key.

Upcoming Admin console features

Native printer-management improvements

Soon, you can add more than 20 printers for each organizational unit in the Google Admin console.

Manage sign-ins within the Chrome Browser and on Chrome OS

A new setting coming to the Google Admin console will allow you to restrict which domains users can use to access Google products like Gmail or G Suite. This applies for users that are browsing in the Chrome browser and on a Chrome OS device. A common way this setting could be used is to prevent students from signing in to their personal Gmail accounts on a school-owned Chromebook.

Note: This Admin console setting combines these policies:

- AllowedDomainsForApps
- SecondaryGoogleAccountSigninAllowed

Public-session support for managed Google Play on Chrome OS

Soon, there will be a setting in the Google Admin console that allows Android apps to run in public sessions. Currently, Android apps can only run in a signed-in session.