chrome enterprise

M68 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 29, 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 M68

New and updated policies

Policy	Description
ArcBackupRestoreServiceEnabled *Chrome OS only*	Controls Android backup and restore service
ArcGoogleLocationServicesEnabled *Chrome OS only*	Controls Android Google location services
ChromeCleanupEnabled *Windows only*	Enables Chrome Browser Cleanup on Windows
ChromeCleanupReportingEnabled *Windows only*	Controls how Chrome Browser Cleanup reports data to Google
DeveloperToolsAvailability	Controls where Developer Tools can be used
IsolateOriginsAndroid *Android only*	Enables Site Isolation on Chrome Browser for specified origins on Android devices
SafeBrowsingWhitelistDomains	For configuring the list of domains which will not trigger Safe Browsing warnings
SitePerProcessAndroid *Android only*	Enables Site Isolation for every site
WebUsbAskForUrls	Allows WebUSB on these sites
WebUsbBlockedForUrls	Blocks WebUSB on these sites

Chrome Browser updates

Unencrypted sites to show “not secure” indicator

For the past several years, we’ve advocated that sites adopt HTTPS encryption for greater security. Within the last year, we’ve also helped users by marking a larger subset of HTTP pages as “not secure”. Beginning in July 2018 with the release of Chrome 68, Chrome will mark all HTTP sites as “not secure”.

Chrome offers a policy to control this warning on your domain.

Chrome Canary on Mac policy list update

Chrome Canary on Mac reads the same policy file (com.google.chrome.plist) as the Dev, Beta, and Stable channels of Chrome. We're deprecating the separate policy file com.google.chrome.canary.plist.

Block a locally installed, hardcoded CA for Mitel VoIP products

In M68, we plan to blacklist a hardcoded Certificate Authority (CA) and shared private key that's installed with certain Mitel® VoIP products. The products contain both the public and private key for the Mitel IP Communications Platform (ICP) CA, which can be installed and trusted for a wide range of certificate purposes, including website SSL and TLS certificates. We've observed evidence of this CA being used to maliciously issue Man-in-the-Middle (MITM) certificates, including www.google.com. While this CA is not publicly trusted as a part of the web PKI, it warrants protecting Chrome users by blocking trust in it. For more details, see Mitel's security advisory.

Certificate transparency

M68 requires that all new publicly trusted certificates issued after April 30, 2018 have several Certificate Transparency logs. This update does not affect existing certificates or certificates from locally trusted CAs, such as Enterprise CAs or those used with antivirus or security products. For more information, see Certificate Transparency.

Chrome OS updates

PIN sign-in support

Users can now sign in to their device using a numeric PIN. Previously, users could only use a PIN to unlock their device after first signing in with a password. Policy to control this feature in the Admin console will arrive in a future release. When the policy is added, it will allow an admin to enable or disable their end users from setting a PIN for the Chrome device. Once enabled, the

user has to set the PIN themselves. The PIN only works on that device and it won't sync to other devices.

Video capture service

Video capture from internal and external cameras in Chrome (including on Chrome OS and Chromebox for meetings devices) has traditionally been run as part of the main Chrome Browser process. With the rollout of the video capture service, this functionality is now a separate process to enable isolation in services. There are no user-facing changes in functionality.

802.11v and 802.11r Fast BSS Transition support added

These changes allow Chrome OS customers to more quickly connect to a network. Specifically, the 802.11r Fast BSS Transition enables a faster handoff for devices roaming in areas with many access points (APs). For enterprise users with 802.11r-enabled APs, the time-to-associate with APs while mobile is improved. 802.11v enables clients to be topology aware. This can allow clients to transition to APs, which increase throughput and QoS.

Accessibility improvements

Chrome OS M68 comes with a number of accessibility improvements.

To enable the ChromeVox screen reader:

1. Press and hold the 2 side volume buttons for 5 seconds.
   After a few seconds of holding these 2 buttons, an audio tone will play.
2. Continue holding.
   The screen reader will start speaking.

Additionally, we're launching new shortcuts to toggle accessibility features:

- Select Ctrl + Search + M to enable/disable the full screen magnifier.
- And select Ctrl + Search + D to enable/disable the new docked magnifier.

We're adding new functionality to our Select to Speak feature, which allows users to select certain parts of the screen to be spoken aloud through a synthesized voice. With M63, we launched this feature by pressing the Search key, then clicking an item or dragging a box around content to have that content read aloud.

With M67, we introduced the ability to highlight specific text, then press Search + D to have only that text spoken aloud.

With M68, it's now possible to use the Select to Speak feature with a touch screen, mouse, or stylus (in addition to or instead of the keyboard and touchpad). This adds a button in the status area that a user can click or touch, then select an area to be spoken aloud.

Introduction of display size and refresh rates to display settings

As of M68, we are rolling out a new display-zoom setting for primary display and adding resolution, along with refresh rates for external displays.

- While disconnected from external display, users will be able to manipulate the size of objects on the screen.
- When connected to external display, we are adding an option to set resolution, which determines sharpness of text and images.

The goal of these changes is to give users more control over UI scale and look.

Admin console updates

Automatic re-enrollment (Forced re-enrollment enhancement)

A new feature allows a managed Chrome OS device that is wiped or recovered to automatically re-enroll after it connects to a network. With the previous Forced re-enrollment feature, a user had to enter their username and password to complete the re-enrollment step. But this new feature allows an admin to remove that requirement and automatically complete re-enrollment. This feature will be rolled out incrementally starting in July, 2018 and will become the default for new customers, as well as for existing customers who have not changed the default Forced re-enrollment setting.

Admins can still require users to enter their credentials to re-enroll wiped or recovered devices and make use of enrollment permissions to prevent specific users from re-enrolling through that process.

Device off-hours feature

Admins can set up schedules to customize when sign-in restrictions and guest-mode policies are needed. For instance, schools can allow guardians and family members to sign in to Chrome devices with their personal accounts after school hours on managed devices.

Native printer-management improvements

A new policy to block users from manually adding printers is targeted for this release. With this policy, users will be limited to using printers assigned by their admin.

Coming soon

Upcoming Chrome Browser features

CRX2 deprecation (M69)

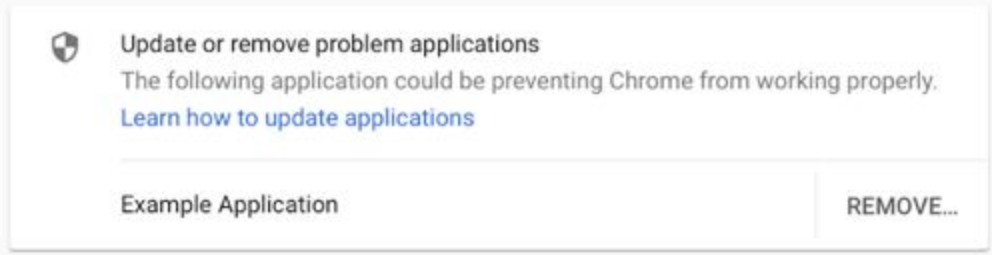
Starting in M69, all non-force-installed extensions must be packaged in the CRX3 format. Extensions signed and hosted in Chrome Web Store have been automatically converted, but privately hosted extensions that were packaged using a custom script or a version of Chrome prior to Chrome 64.0.3242.0 must be repackaged. Starting in M75, this restriction will also apply to force-installed extensions.

Reduce Chrome crashes caused by third-party software (M69)

In M66, Chrome began showing a warning to users after a crash that displays third-party software that is injecting code into Chrome, guiding them to update or remove that software. In M69, Chrome will begin blocking third-party software from injecting code into Chrome processes.

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

You can enable or disable third-party software blocking with the ThirdPartyBlockingEnabled policy. The policy will be deprecated in approximately one year (Chrome 77).



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

Voice dictation from anywhere (M69)

Voice to type has been available on Chromebooks for some time through the on-screen accessibility keyboard or the virtual keyboard's microphone icon. However, a number of users have requested the ability to use dictation as a standalone feature, separate from needing to pull up the accessibility keyboard. Soon, we will launch dictation as a separate accessibility feature. With this enabled, a small button will appear in the status area. When focus is in an edit field, users can either click the button to start dictating or press the keyboard command Search + D, then use their voice to input text.

Enable key remapping for external keyboards (M69)

The new feature allows users to remap Search/Command/Windows keys on external keyboards through keyboard settings. If an Apple® keyboard is attached to Chromebook, the external keyboard setting defaults to Control. Other external keyboards default to Search/Launcher.

Files app improvements (M69)

Native support for Team Drives in Files app is currently targeted for M69. The team is also working toward making ARC++ files available as read/write with the Files app and will be updating the UI to improve the organization of local vs. cloud file storage.

Policy to show PIN pad on sign-in and lock screen for TouchView devices

The Policy to show PIN feature will allow admins to show the PIN pad on the sign-in screen. This is intended to make sign-in easier on tablets in domains where the administrator has made all user passwords only digits.

Visual updates for enterprise device enrollment flow

The device enrollment flow will be updated to match the visual styling of the rest of the Chrome OS out-of-box experience (OOBE). These are only style changes and will not affect functionality. Customers who automate OOBE using USB devices should update their automation steps as appropriate.

Night Light support on Chromebooks

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

Upcoming Admin console features

Native printer-management improvements

A change is coming to the Admin console to remove the 20-printer limit for each organizational unit.

Sign-in Within the Browser policy

Admins can restrict users who sign in to Chrome OS from adding additional Google Accounts in the browser.

Public session support for managed Google Play on Chrome OS

A setting is coming to the Admin console that will allow you to run Android apps in public sessions. Currently, Android apps can only run in a signed-in session.