M67 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 May 24, 2018

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

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 M67

New and updated policies

Policy	Description
ArcAppInstallEventLoggingEnabled	Logs events for Android app installs (Chrome OS)
AutoplayWhitelist	Allows media autoplay on a whitelist of URL patterns
CertificateTransparencyEnforcementDisabledForCas	Disables Certificate Transparency enforcement for a list of subjectPublicKeyInfo hashes
CertificateTransparencyEnforcementDisabledForLegacyCas	Disables Certificate Transparency enforcement for a list of Legacy Certificate Authorities
DefaultWebUsbGuardSetting	Controls use of the WebUSB API
DeviceRollbackAllowedMilestones	Specifies the number of milestone rollbacks allowed (Chrome OS)
DeviceRollbackToTargetVersion	Specifies a rollback to a target version (Chrome OS)
MediaRouterCastAllowAllIPs	Allows Google Cast to connect to Cast-ready devices on all IP addresses
RelaunchNotificationPeriod	Sets the period for update relaunch notifications
SafeBrowsingExtendedReportingEnabled	Enables extended reporting for Safe Browsing (added in M66)
TabUnderAllowed	Allows sites to simultaneously navigate and open notifications

Chrome Browser updates

SAML SSO interstitial

Doesn't impact users who sign in to G Suite services directly, those who use G Suite or Cloud Identity as their identity provider, or devices running Chrome OS.

If your users use SAML to sign in to G Suite services, they'll need to complete an extra step to confirm their identity when using the Chrome Browser. After signing in on a SAML provider's website, they'll be brought to a new screen on accounts.google.com to confirm their identity. This screen provides an extra layer of security and helps prevent users from unknowingly signing in to a malicious account.

To minimize disruption, this screen will only be shown once per account per device. We're working on ways to make the feature smarter in the future, meaning users in your organization should see the screen less and less over time.

If you don't want your users to confirm their identity on this interstitial page, you can set the X-GoogApps-AllowedDomains header and identify specific domains where the extra confirmation isn't needed. We assume that if the user is signing in with an account that is in this list of domains, then the account is trusted by the user. You can set the header using the AllowedDomainsForApps group policy.

For more details, see the G Suite Updates blog.

Site Isolation

You can turn on site isolation to create an additional security boundary between websites. When you enable site isolation, content for each open website in Chrome Browser is always rendered in a dedicated process, isolated from other sites. Adding site isolation creates an additional security boundary between websites.

Chrome continues to roll out Site Isolation to a larger percentage of the stable population in M67. For details, see Manage Site Isolation.

Chrome OS updates

Desktop Progressive Web Apps (PWAs)

Desktop PWAs are now supported on devices running Chrome OS starting with M67. Work is underway to include support for Microsoft® Windows® and Apple® Mac®. For more information, see our developer site.

Detachable-base swap detection

Detachable-base swap detection helps prevent hackers from accessing sensitive data. When a keyboard base that has not been used before is attached to a detachable tablet, such as an HP Chromebook X2, the user gets notified. The detection helps prevent hackers from replacing the base with a different one that looks the same but has been modified.

Block symlink traversal

This feature improves verified boot security by preventing symlink traversal attacks, even after restart. This is a defensive measure to prevent attacks against Chromebooks from persisting through restart.

This feature has no observable changes for most users. Developers and power users whose use of developer mode might run into issues, but these can be resolved by disabling this restriction. Learn more about restricting symlink traversal.

Admin console updates

EAP-TLS device-level support

Admins can now configure EAP-TLS network support at a device level. These network settings apply to users across the device, including users in a public session and kiosk mode. Learn more about adding a network configuration.

Managed Google Play on Chrome OS policy update

With this release, the Android user policies Backup & Restore and Google Location Services are disabled by default for the Chrome Enterprise and Chrome Education services. Admins can only turn off these features or let the users configure them. Admins cannot force these on for their users. The policies allow users to easily restore their data and help improve location accuracy on their Android apps.

Admins can block apps from installation

Currently not available for the Chrome Education service
As an administrator, you can specify a blacklist of Android apps for users who have enabled All Access mode for Android on their organization's domain. If a blacklisted app has already been downloaded onto a user's device, it will be uninstalled.

Android app installation reporting

In a new section in the Google Admin console, you and other admins can troubleshoot Android app installations on devices running Chrome OS. You can now see the status of force-install (and uninstall) operations and filter the reports by organizational unit, user, or status. You can also see which devices the status applies to.

Android app bulk purchasing on Education service

As an EDU administrator, you can now bulk purchase one-time payment and perpetual-access apps from the Managed Google Play store and provision them by user and organizational unit in

the Admin console. In the Admin console, you can force install, allow install, and pin apps to taskbar. You can use a credit card and Google Play gift cards. In-app and subscription purchasing is not currently supported.

Coming soon

Upcoming Chrome Browser features

Unencrypted sites to show “not secure” indicator (M68)

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 will offer a policy to control this warning on a per-domain basis.

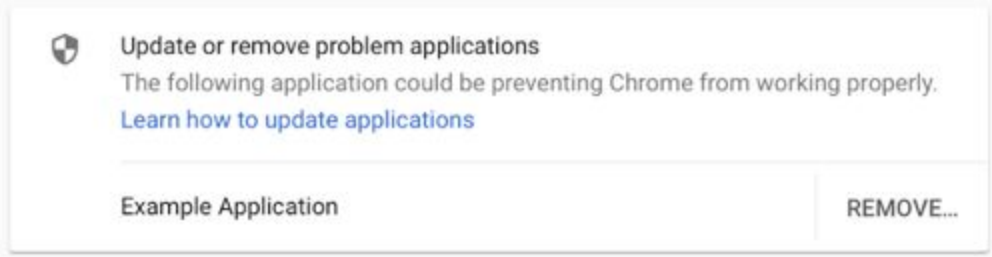
Canary release channel on Mac update (M68)

This change unifies the policy list for all Chrome OS release channels on Mac devices to include the Canary channel, which is consistent with how other platforms operate.

Reduce Chrome crashes caused by third-party software (M68)

In M66, Chrome began showing a warning to users after a crash that will display third-party software that is injecting code into Chrome, guiding them to update or remove that software. In M68, Chrome 68 will begin blocking third-party software from injecting into Chrome processes.

You can enable or disable third-party software blocking with the ThirdPartyBlockingEnabled policy.



Block a locally-installed hardcoded CA for Mitel VoIP products (M68)

In M68, we intend 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)

M68 will require 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.

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

PIN sign-in support (M68)

Users will now be able to 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.

Video capture service (M68)

Video capture from internal and external camera devices 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 roll out of the video capture service, this functionality is now a separate process to help enable better isolation. There are no user-facing changes in functionality.

Upcoming Admin console features

Automatic re-enrollment (Forced re-enrollment enhancement) (M68)

A new feature allows a Chrome OS device that is wiped or recovered to automatically re-enroll once it connects to a network. In the past, a user had to sign in to complete the re-enrollment step. But with the new feature, user credentials are no longer required to complete re-enrollment.

Admins can still require users to sign in to re-enroll wiped or recovered devices.

Native printer management improvements

There will be 2 new improvements for native printer management:

- A new policy for user and device settings to remove the 20-printer limit per organizational unit.
- A new policy to block users from manually adding printers is targeted for M68.

Sign-in Within the Browser policy

Admins can restrict users who are signed in to the Chrome Browser from adding additional Google Accounts in the browser.

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 OS devices with their personal accounts after school hours on managed devices.

Public session support for managed Google Play on Chrome OS

You will soon be able to run Android apps in public sessions. Currently, Android apps can only run in a signed-in session.