M66 Enterprise Release Notes

Every 6 weeks, Google releases an update to its Chrome Browser. Each release includes thousands of improvements and other changes. The following release notes are intended for IT administrators managing the Chrome Browser in their organization.

These release notes were last updated on April 4, 2018

See the latest version of these release notes online at https://support.google.com/chrome/a/answer/7679408

Additional resources

- How Chrome releases work—Chrome Release Cycle
- Chrome Browser downloads and Chrome Enterprise product overviews—Chrome Browser for Enterprise
- Chrome version status and timelines—Chrome Platform Status | Google Update Server Viewer
- Announcements: Chrome Releases Blog | Chromium Blog

Still need help?

- G Suite, Cloud Identity customers (authorized access, only)—Contact support
- Chrome Browser Enterprise support—Sign up to contact a specialist
- Chrome Administrators Forum
- Chrome Enterprise Help Center

Release notes for Chrome 66

Security updates

Continuation of distrust of Symantec Certificates
Following our announcement to gradually phase out trust in Symantec's PKI, Chrome continues to remove trust in Symantec-issued certificates issued before June 1, 2016.

The Google Security Blog published a guide for impacted site operators. The EnableSymantecLegacyInfrastructure enterprise policy allows administrators to temporarily remove Chrome's distrust of the Symantec PKI. The policy expires after Chrome 73 (targeted for release January 2019), giving enterprise admins 3 releases after Chrome's full distrust to migrate off of Symantec certificates. For details, see Migrate from Symantec certificates.

Enterprise features

Chrome relaunch policy: RelaunchNotification
If set to 1, or recommended, the user sees a prompt after days 2, 4, 7, and every 3 days after that. If set to 2, or required, the user sees a prompt at days 2, 4, and 7, with a forced relaunch 3 minutes after the final prompt. The RelaunchNotificationPeriod policy feature will make the period configurable.

Chrome relaunch policy: RelaunchNotificationPeriod (M67)
This feature allows admins to set the time period over which Chrome relaunch notifications are shown to apply a pending update. Over the period based on the setting of the RelaunchNotification policy, the user is repeatedly notified of the need for an update. If RelaunchNotificationPeriod isn't set, the default period of one week applies.

Click to open PDF
For downloading embedded PDF content with an embed or iframe when Chrome's default PDF viewer is disabled (via settings or Enterprise policy) or not present (as on mobile), an Open button appears on the PDF placeholder.

Force sign-in policy: Support for Mac
The ForceBrowserSignin policy is supported on Mac.

Chrome policies

Changes in this release:

Policy	Notes
AutoplayAllowed	This policy allows you to control whether videos with audio content can autoplay (without user consent) in Chrome.
EnableCommonNameFallbackForLocalAnchors	This policy has been deprecated.
EnableSymantecLegacyInfrastructure	When this setting is enabled, Chrome allows certificates issued by Symantec Corporation's Legacy PKI operations to be trusted if they otherwise successfully validate and chain to a recognized CA certificate.
ForceBrowserSignin	Force users to sign in to the profile before using Chrome. Added support for Mac.
RelaunchNotification	Notify users to relaunch Chrome to apply a pending update.
SafeBrowsingExtendedReportingEnabled	This setting enables Chrome's Safe Browsing Extended Reporting and prevents users from changing it.

SafeBrowsingWhitelistDomains	Configure the list of domains Safe Browsing trusts. Safe Browsing won't check for dangerous resources (for example, phishing, malware, or unwanted software) for URLs that match these domains.
SSLVersionMin	If this policy isn't configured, Chrome uses the default minimum version of TLS 1.0.

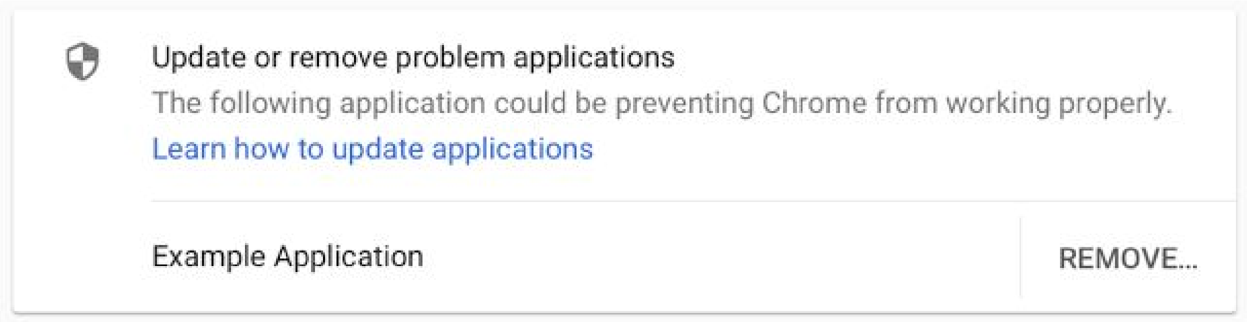
UI changes

Changes to autoplay

Chrome is changing the policy for when sites can autoplay media with sound. Admins will be able to use the AutoplayAllowed policy to control whether Chrome defaults to allowing media to autoplay. For details, see the Autoplay Policy Changes.

Reducing Chrome crashes caused by third-party software

Chrome will begin showing a warning to users after a crash that displays third-party software injecting code into Chrome. It guides them to update or remove that software.



Update or remove problem applications

The following application could be preventing Chrome from working properly.

Learn how to update applications

Example Application

Deprecations

Enable CommonName fallback for local anchors policy

The EnableCommonNameFallbackForLocalAnchors policy was offered to give admins more time to update their local certificates. It removes the ability to allow certificates on sites using a certificate issued by local trust anchors that are missing the subjectAlternativeName extension.

As of Chrome M66, we will be deprecating this policy. If a user running Chrome 66 tries to access a site where the certificate isn't allowed, they will see a warning indicating they can't trust the certificate.

Adobe Flash Deprecation

Adobe announced on July 25, 2017 it plans to deprecate Flash by the end of 2020. See Adobe's announcement and Chrome's blog post regarding the Flash deprecation.