chrome enterprise

M70 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 October 24, 2018

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

Call for Trusted Testers

New in M70

- New and updated policies
- Chrome Browser updates
- Chrome OS updates
- Admin console updates

Deprecations

Coming soon

- Upcoming Chrome Browser features
- Upcoming Chrome OS features
- Upcoming Admin console features

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!

Chrome 70

New and updated policies

Policy	Description
BrowserSignin	Controls the sign-in behavior of Chrome Browser.
DeviceLocalAccountManagedSessionEnabled *Chrome OS only*	Allows managed session behavior on a device configured for public sessions.
NetBiosShareDiscoveryEnabled *Chrome OS only*	Controls Network File Share discovery through NetBIOS.
NetworkFileSharesAllowed *Chrome OS only*	Controls whether the Network File Share feature for Chrome OS is allowed for a user.
PowerSmartDimEnabled *Chrome OS only*	Specifies whether a smart dim model is allowed to extend the time until the screen is dimmed.
PrintHeaderFooter	Specifies whether users can print headers and footers.
ReportMachineIDData *Desktop only*	Controls whether to report information that can be used to identify machines. Learn more about reporting on Chrome.
ReportPolicyData *Desktop only*	Controls whether to report policy data and the time of a policy fetch. Learn more about reporting on Chrome.
ReportUserIDData *Desktop only*	Controls whether to report information that can be used to identify users. Learn more about reporting on Chrome.
ReportVersionData *Desktop only*	Controls whether to report Chrome OS version information. Learn more about reporting on Chrome.
WebRtcEventLogCollectionAllowed	Specifies whether to allow or block Chrome OS from collecting WebRTC event logs from Google services.

Chrome Browser updates

Sign-in policy change

Starting in Chrome 70, the BrowserSignin policy will control the "Allow Chrome sign-in" setting for your users on Chrome Browser. It allows you to specify if the user can sign in with their account and use account-related services, such as Chrome sync.

If the policy is set to "Disable browser sign-in", then the user cannot sign in to the browser and use account-based services. In this case, account-bound features, such as Chrome sync, cannot be used and will be unavailable.

If the policy is set to "Enable browser sign-in", then the user can sign in to the browser, but they're not forced to do so. The user can't disable signing in to the browser. To control the availability of Chrome sync, use the SyncDisabled policy.

If the policy is set to “Force browser sign-in”, then the user has to sign in to Chrome before using the browser. The default value of BrowserGuestModeEnabled will be set to false. Existing profiles that are not signed in will be locked and inaccessible after enabling this policy.

If this policy is not set, then the user can decide if they want to enable the browser sign-in option and use it as they see fit.

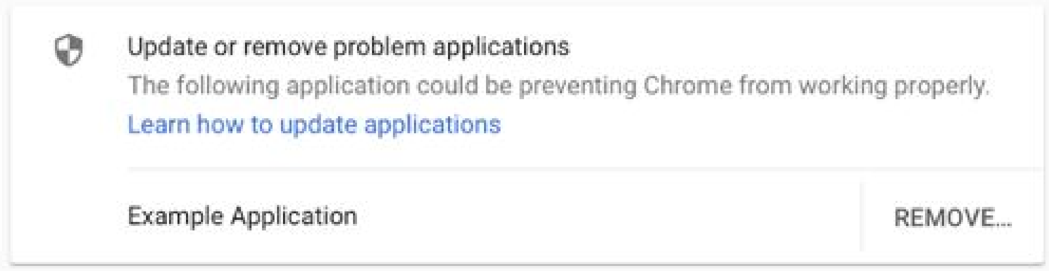
Cookie behavior change

With Chrome 70, when a user clears cookies in Chrome Browser, Google's authentication cookies will be deleted along with all other cookies, except for the cookie used for the Chrome sync account. Users are automatically signed out of all accounts *not* being used for Chrome sync. Users will still be signed in to any account used for Chrome sync so they can delete their browsing data from other devices as well.

Reduce Chrome crashes caused by third-party software

Third parties can 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.

Here's the warning users see on their computers if the ThirdPartyBlockingEnabled policy is enabled:



Update or remove problem applications

The following application could be preventing Chrome from working properly.

Learn how to update applications

Please note that this blocking feature was previously scheduled for M68 and M69, but is now launching in Chrome 70.

In Chrome 70, third-party code is now blocked by default for *consumer* users of Chrome. **However, there is a different default behavior for enterprises. If you (the admin) do not block third-party code, third-party code will not be blocked for domain-enrolled enterprise users in Chrome 70.**

In Chrome 71, third-party code blocking will be enabled by default for everyone, including domain-enrolled users.

To prepare for this change, if you still use software that injects code into browser processes, you can temporarily enable access using the new ThirdPartyBlockingEnabled policy.

To test Chrome's third-party software warning and blocking features on Windows, see these instructions, which will walk you through how to use the diagnostic tool at chrome://conflicts.

Deprecate trust in remaining legacy Symantec PKI infrastructure

Following previous announcements, Chrome 70 marks the final stage of distrusting the Symantec legacy PKI certificates.

Beginning with Chrome 70:

- All certificates, regardless of issuance date, issued from the Symantec legacy PKI are distrusted in the Canary and Dev release channels.
- Trust in the Symantec legacy PKI has begun phasing out for the Beta and Stable release channels.
- Temporary periods of distrust, increasing in length, will identify any outstanding breakages caused by sites that have not replaced their TLS certificates. Complete and final distrust can occur regardless of Chrome release dates. You are strongly encouraged to replace affected certificates as soon as possible to avoid site breakage.

What you need to do:

- Determine if your site is affected and replace your TLS certificate with one unaffected by the change. To find out if your site is affected, see the instructions in our blog post on the deprecation.
- Enterprises with a critical dependency on Symantec TLS certificates can configure temporary trust in the Symantec legacy PKI. This policy is a temporary measure and will expire January 01, 2019. For details, see the EnableSymantecLegacyInfrastructure policy.

Update to TLS 1.3

We shipped draft 23 of TLS 1.3 in Chrome 65. In Chrome 70, we are now updating to the final revision. For details, see TLS 1.3 and Chromium.org. We will not be shipping anti-downgrade protections in Chrome 70 due to bugs in several middlebox vendor's TLS implementations. Administrators of Cisco® Firepower® devices can update to Firepower version 6.2.3.4 to avoid incompatibilities with a future Chrome version. If needed, admins can use the SSLVersionMax policy to control TLS 1.3.

New UI support for WebAuthn

Chrome 70 comes with a new UI for WebAuthn and FIDO authenticators. Developers no longer have to implement these user authentication flows themselves. In Chrome 70, when a user invokes WebAuthn, Chrome will guide the user through their FIDO-compatible authenticator, such as a security key.

Form autofill policy changes

With the AutoFillEnabled policy deprecated, it's being replaced with 2 more granular policies, which control autofilling address and credit card information into forms online. For Chrome devices running Chrome 70 and later, you need to update the AutofillAddressEnabled and AutofillCreditCardEnabled policies.

Autofill policies

The AutofillAddressEnabled and AutofillCreditCardEnabled policies allow users to enter address and credit card information in web forms using previously stored information or information from their Google Account.

If AutofillAddressEnabled is disabled, address information is not suggested or filled in. Additional address information that’s entered in web forms by the user will not be saved.

If AutofillCreditCardEnabled is disabled, credit card information is not suggested or filled in. Additional credit card information that’s entered in web forms by the user will not be saved.

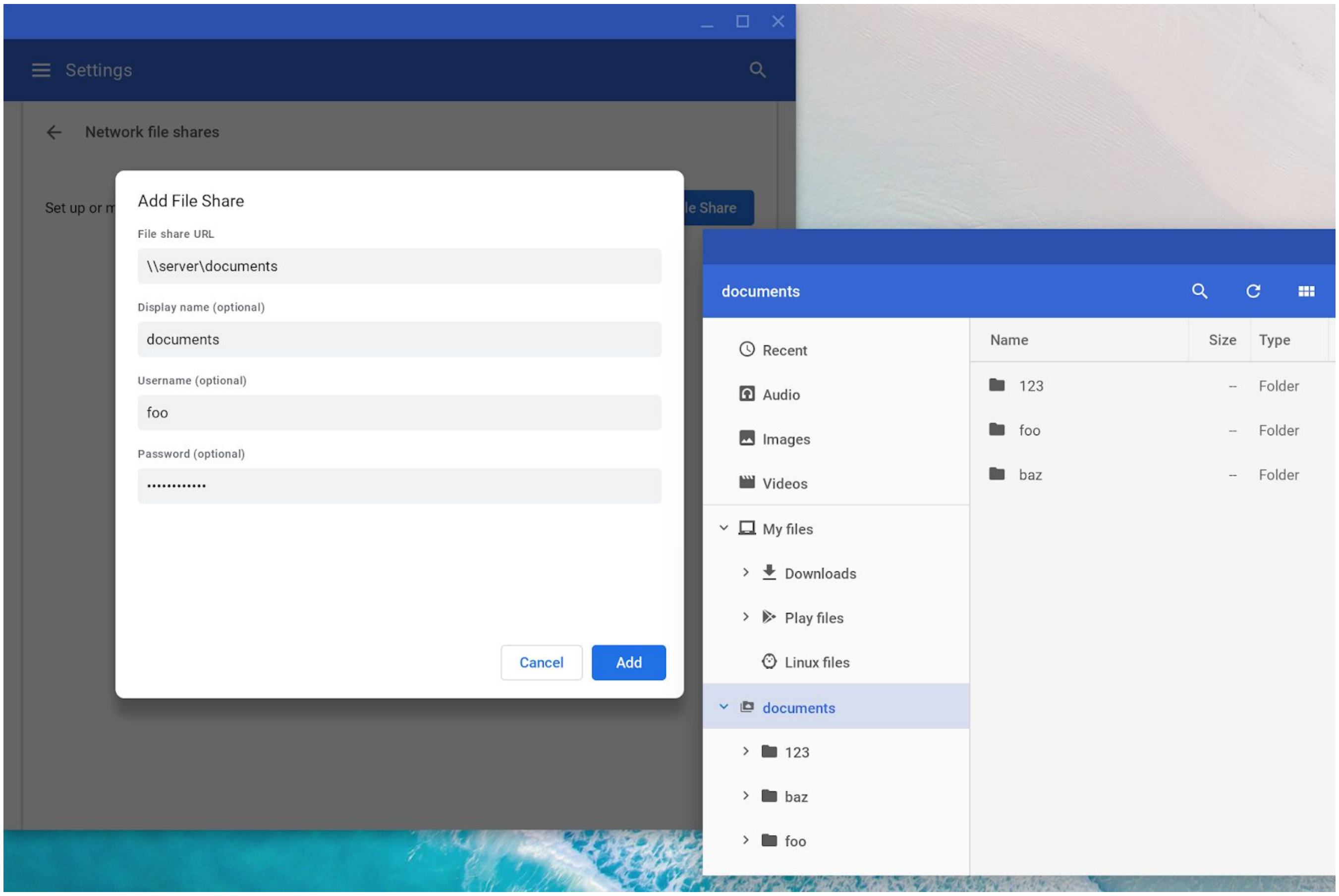
If either the AutofillAddressEnabled or AutofillCreditCardEnabled setting is enabled or has no value, the user will be able to control autofill for addresses or credit card information, respectively.

Chrome OS updates

Native SMB file share support

SMB file shares (Windows file shares) are now supported natively on Chrome OS. Remote paths can be mounted as a root in the Files app. Supported authentication methods include Kerberos, Microsoft® Active Directory®, and NTLM version 2. To initiate a SMB file share:

1. Open a Chrome Browser window and at the top right, click More ⋮ > **Settings**.
2. Next to **Network file shares**, click **Add File Share.**
3. Enter the required information and click **Add**.
4. Open the Files app and browse the shared folder.



Add File Share

File share URL: \\server\documents

Display name (optional): documents

Username (optional): foo

Password (optional): ••••••••••••

Name	Size	Type
123	--	Folder
foo	--	Folder
baz	--	Folder

Camera app updates

The Camera app has a refreshed UI. Photos and videos taken with the Camera app are now stored in the Downloads folder in the Files app.

Enable key remapping for external keyboards

Users can now remap the Search, Command, and Windows keys on external keyboards in the 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.

Floating virtual keyboard

For touch-enabled Chrome devices, you can use a floating keyboard to enter text with one finger. You can use this keyboard on a touchscreen, similar to how you use a smartphone keyboard.

Restriction policy for native CUPS printing

Admins can restrict users to color or black-and-white printing with CUPS printing. Users will not be able to manually change the setting on the device.

Admin console updates

Manage sign-ins in Chrome Browser and Chrome OS

In the Google Admin console, you can restrict which domains users can use to access Google products, such as Gmail. The setting applies in Chrome Browser and on Chrome OS devices. For example, you might want to prevent employees from signing in to their personal Gmail accounts on a corporate-owned Chromebook. The setting combines the AllowedDomainsForApps and SecondaryGoogleAccountSigninAllowed policy.

Support for certificate transparency enforcement exceptions

A collection of 3 new user policies have been added to allow enterprises to provide exceptions to certificate transparency requirements. These can be found in the admin console under **Device management > Chrome management > User Settings > Security**.

These settings are from these Chrome policies:

- CertificateTransparencyEnforcementDisabledForCas
- CertificateTransparencyEnforcementDisabledForLegacyCas
- CertificateTransparencyEnforcementDisabledForUrls

Improved developer tools policy

You can use the new DeveloperToolsAvailability policy to allow developer tools *except* for force-installed extensions. This behavior is the new default and is useful for organizations that want to allow the general use of developer tools, but prevent tampering with force-installed extensions. For details, see the DeveloperToolsAvailability policy.

Auto-updates over LTE policy control

You can use the DeviceUpdateAllowedConnectionTypes policy to control which connection types a device can receive automatic updates over. There is now an option to enable automatic updates over all connection types, including LTE, as opposed to only WiFi and Ethernet. For details, see the DeviceUpdateAllowedConnectionTypes policy. This feature will be rolled out over the coming weeks in the Admin console under **Device management > Chrome management > Device settings > Device Update Settings > Auto Update Settings**.

Lock screen control

After a defined idle time, you can now set a lock screen on users' devices running Chrome OS. This setting is in the Google Admin console under **Device management > Chrome management > User settings > Security > Idle Settings**.

Deprecations

AutoFillEnabled policy deprecation

The AutoFillEnabled policy is deprecated in Chrome 70. It's being replaced with 2 more granular policies, which control autofilling address and credit card information into forms online. For Chrome devices running Chrome 70 and later, you need to update the AutofillAddressEnabled and AutofillCreditCardEnabled instead (see "Form autofill policy changes" below).

UnsafelyTreatInsecureOriginAsSecure policy deprecation

The UnsafelyTreatInsecureOriginAsSecure policy was deprecated in Chrome 69. Use OverrideSecurityRestrictionsOnInsecureOrigin instead.

Gmail Offline app discontinued

In December 2018, the Gmail Offline app will be removed from the Chrome Web Store. You can now get offline functionality in Gmail. For details, see Use Gmail offline.

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.

Starting with Chrome 75, this restriction will also apply to force-installed extensions. 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 do not repackage them, they will 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 computationally feasible, so an attacker might intercept the extension update and inject arbitrary code into it. CRX3 uses a stronger algorithm without this risk.

Coming soon

***Note:** The items listed below are experimental or planned updates. They may be changed, delayed, or canceled before launching to the Stable channel.*

Upcoming Chrome Browser features

Change to using PAC scripts to configure proxy settings in Chrome Browser

If you're using a Proxy Auto Config (PAC) script to configure Chrome's proxy settings, you might be affected by this change, especially 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.

In Chrome OS version 71, this policy will change the default value from FALSE to TRUE to improve security. If you already set this policy to TRUE, there will be no impact. If you set it to FALSE, there will be no immediate impact. If you have not set this policy and are relying on the default, you should test this change to see how your PAC scripts operate.

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

CRX2 deprecation

For details on what's happening with CRX2-packaged extensions in Chrome 75, see CRX2 deprecation (above).

Upcoming Chrome OS features

Android 9.0 Pie

Devices running Chrome OS that currently support Android 7.0 Nougat will be upgraded to support Android 9.0 Pie. Dates and affected devices have not yet been announced. We will include more information in future release notes when it comes available.

Always-on VPN for managed Google Play

Admins can already install Android VPN apps on Chromebooks. However, users have to start the VPN app manually. Soon, admins can set a VPN app to start a connection when a device is turned on and direct all traffic through that connection. If the connection fails, all traffic is blocked until the VPN connection is reestablished.

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.

Managed guest session support for managed Google Play

Soon, there will be a setting in the Google Admin console that allows Android apps to run in managed guest sessions (previously known as public sessions). Currently, Android apps can only run in a signed-in session.