chrome enterprise

M78 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 22, 2019

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

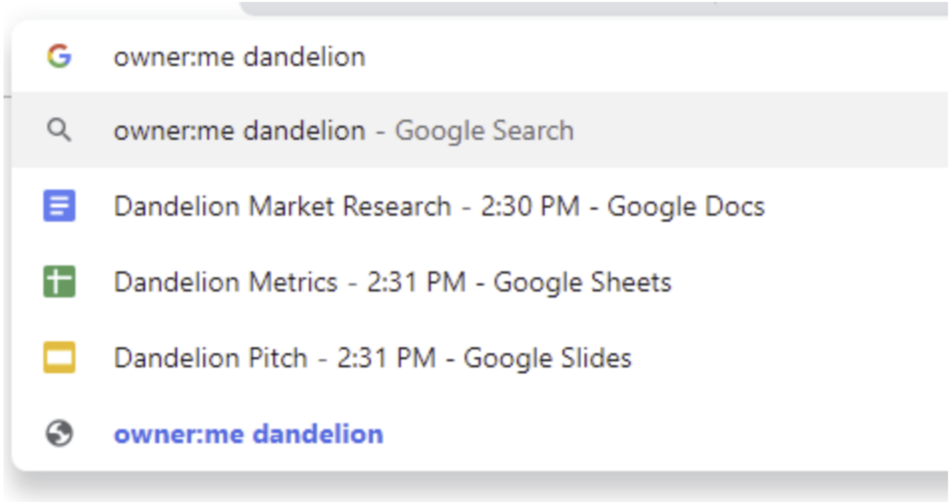
Sign up **here** for our email distribution for future releases.

Chrome 78

Chrome Browser updates

Drive integration in the address bar

Rolling out in the coming weeks, users will be able to search for Google Drive files that they have access to from the address bar. Their input will search through both titles and document contents and the most relevant documents based on their history will appear.



owner:me dandelion

owner:me dandelion - Google Search

Dandelion Market Research - 2:30 PM - Google Docs

Dandelion Metrics - 2:31 PM - Google Sheets

Dandelion Pitch - 2:31 PM - Google Slides

owner:me dandelion

This behavior is on by default and can be controlled with the "Google Drive search suggestions" setting in the G Suite admin console.

Flags are being cleaned up starting in Chrome 78

Many flags in chrome://flags will be removed in upcoming Chrome versions, starting with Chrome 78. As a reminder, don't use flags to configure Chrome Browser because they're not supported. Instead, configure Chrome Browser for your enterprise or organization using policies.

Shared clipboard between computers and Android devices

A limited number of users might see the option to share their clipboard content between their computers and Android devices. To share, they need to have Chrome installed, sign in on both devices with the same account, and enable Chrome Sync.

The text is end-to-end encrypted, and Google can't see the contents.

This functionality will be released to all users in a future version of Chrome. In the full release, admins can control it with an enterprise policy.

Forward a call from Chrome Browser to your Android device

Users can highlight and right-click a phone number link in Chrome Browser and forward the call to their Android device.

Chrome Renderer Integrity protects users

Chrome Renderer Integrity is on by default for users on Microsoft® Windows® 10 version 1511 and later. It prevents unsigned modules from loading in Chrome Browser's renderer processes that deal with user content to prevent certain types of malicious attacks.

Note: There is a known incompatibility between Chrome Renderer Integrity and old versions of Symantec® Endpoint Protection® (14.0.3929.1200 and earlier). We recommend updating to the latest version of Symantec Endpoint Protection (14.2 or later). For a download of the latest version or more details, refer to the Symantec documentation. To help with any incompatibilities, you can temporarily disable Chrome Renderer Integrity using the RendererCodeIntegrityEnabled policy.

Atomic policy groups introduced

Some admins set policies from multiple sources, but need policies that are tightly coupled to all be set together. For example, you might want all of your extension management policies to be applied from the same source to ensure they're working together as planned.

To achieve this, some policies have been regrouped based on atomic policy groups. You can enable atomic policy groups using PolicyAtomicGroupsEnabled. If you do, policies in a single group will all be forced to set their behavior from the same source—the one with the highest priority.

You can see whether there are any conflicting policies from different sources at chrome://policy. If you have multiple policies in the same policy group from different sources, this feature will affect them. For more details, see Atomic Policy Groups and Understand Chrome policy management.

ExtensionAllowInsecureUpdates policy is no longer supported

The policy to allow extensions to update using the previous CRX2 packaging no longer works in Chrome 78. In Chrome 78, all extensions must be packaged in the new CRX3 format to ensure secure delivery of updates to your browsers and devices.

Windows 8-specific welcome page removed

We removed the Windows 8-specific welcome page, along with support for the distribution.suppress_first_run_default_browser_prompt master_preferences setting. For more about master preferences, see Use master preferences for Chrome Browser.

Legacy Browser Support is integrated, the extension is no longer required

We integrated Legacy Browser Support functionality directly into Chrome. As a result, you no longer need the Legacy Browser Support extension, and it's now in maintenance mode. No further updates will be provided for the extension. Deploy the integrated version of the Legacy Browser support policy and manage it either through GPO or Chrome Browser Cloud Management's User Settings.

Chrome OS updates

Virtual Desks

Virtual Desks have arrived on Chrome OS. You can now create up to 4 separate work spaces. Virtual Desks are for focusing on a single project or for quickly switching between multiple sets of windows. Create your first desk by opening Overview and tapping **New Desk**. For details, see (Help Center article, Blog post)

Wake from sleep on USB attach for docking use cases

Chromebook users in an office or home office environment can use some combination of peripherals along with a USB-C+Display docking station to work more productively. This feature makes the transition from sleeping mode directly into a docked mode with external monitors smooth for the user, removing the requirement to wake by lid open.

Crostini backup & restore

If you use Linux apps on a Chromebook, you can now easily back up all of your apps and files. The backup can be saved to your Chromebook's local storage, an external drive, or Google Drive. You can then restore that backup on the same machine to return to a previous state or on a different machine to bring your whole workspace with you.

Crostini GPU support on by default

Linux apps will now be able to use the GPU to provide a crisp, lower-latency experience.

Crostini IME/VK warning

Linux apps do not yet support certain input methods (IMEs) or the virtual keyboard when in tablet mode. This feature will display a message warning if you try to use a Linux app with an unsupported input method or the virtual keyboard.

Files app Visual Signals UX update

We implemented visual improvements to the Files app progress center in Chrome 78, moving the information from the lower left-hand corner to a feedback area in the main window of the app. You should update your internal support documentation to reflect the new UI.

Update printer setting landing page UI

The printer settings page is now updated to streamline the printer setup experience. Users can now view available printers on the landing page and save printers (compatible with IPP/IPPS) with one click.

ChromeVox Dynamic Rich Text Output

There is now an option in ChromeVox that supports the ability to announce text styling. Users have the ability to enable and disable this feature through the ChromeVox Options page.

Chrome OS and Chrome Browser settings split

Settings on Chrome OS now have a more native OS settings experience housed in the Settings app (available through App Launcher or the cog icon in the Quick Settings menu), with Chrome Browser settings available through More in the top-right corner of the app (or at chrome://settings in the address bar). If you block Chrome Browser settings by URL (chrome://settings), you might also want to block the new URL for Chrome OS settings (chrome://os-settings).

YouTube Picture in Picture on ARC++

Picture in Picture (PiP) is now available with the YouTube Android app. This is for watching a video while doing other tasks, such as taking notes during a meeting.

New and updated policies (Chrome Browser and Chrome OS)

(Policy changes as of 2019-10-08 for 78.0.3904.55 - ID:578 -> 604)

Policy	Description
PasswordLeakDetectionEnabled	Enable leak detection for entered credentials
PolicyAtomicGroupsEnabled	Enables the concept of policy atomic groups
RendererCodeIntegrityEnabled *Windows Only*	Enable Renderer Code Integrity
HSTSPolicyBypassList	List of names that will bypass the HSTS policy check
AllowSyncXHRInPageDismissal	Allows a page to perform synchronous XHR requests during page dismissal

Coming soon

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

Upcoming Chrome Browser changes

Trial of autoupgrade for DNS-over-HTTPS in Chrome 79

The DNS requests of some users will autoupgrade to their DNS provider's DNS-over-HTTPS (DoH) service if available. During this trial, DoH will be disabled by default for managed devices running Chrome OS and for desktop Chrome Browser instances that are domain joined or have at least one active policy.

You can disable DNS-over-HTTPS for your users with the DnsOverHttpsMode policy. Setting it to "off" will ensure your users are not affected by DoH.

Users warned if credentials are leaked in Chrome 79

We will notify users if their credentials are part of a known data breach. The system can detect this without sending plain-text passwords to Google. You will be able to enable or disable this feature using the PasswordLeakDetectionEnabled policy.

New policy for controlling memory will be introduced in Chrome 79

We'll introduce a new policy to give admins more control over Chrome's memory usage. It configures the amount of memory that a single Chrome instance can use before starting to discard background tabs. When discarded, the memory used by the tab is freed, and the user will have to reload the tab when switching to it. If the policy is set, Chrome will begin to discard tabs to save memory once the user exceeds the limit. However, there is no guarantee that the browser is always running under the limit. (For example, the active tab is never discarded.) Any value under 2,048 will be rounded up to 2,048. If this policy is not set, the browser will only attempt to save memory after it has detected that the amount of physical memory on its machine is low (available on Windows and Mac).

Tab freezing will be introduced in Chrome 79 on the desktop

Chrome 79 will introduce a new feature to save memory, CPU, and battery for Windows, Mac, Linux, and Chrome OS. Tabs that have been in the background for 5 minutes or more will be frozen, as long as Chrome detects that they are freezable (such as not playing audio). Frozen pages are not able to run any tasks. Web developers can opt their pages out of freezing with an origin trial.

You will be able to disable this behavior with the TabFreezingEnabled policy.

New Chrome UI for legacy TLS versions in Chrome 79 and Chrome 81

Chrome recently announced our updated plans around our deprecation and planned removal of legacy TLS versions (TLS 1.0 and 1.1). Starting on January 13, 2020 in Chrome 79, we will mark sites that use TLS 1.0 or 1.1 as "Not Secure" and no longer show the lock icon for them.

In Chrome 81, we will start showing a full-page interstitial warning telling users that the connection is not fully secure.

If enterprise users have sites affected by these changes and need to opt out, admins can use the existing SSLVersionMin policy to disable the security indicator and interstitial warning on all affected sites. Admins should set it to "tls1" to allow TLS 1.0 and later without additional warnings. This policy will work until January 2021.

CORS implementation will be more secure in Chrome 79

We will switch CORS implementation to be more secure and strict. As a result, the following behavior changes will be introduced:

Behavior changes on Extensions' webRequest API—Before this change, extensions that have the webRequest permission can modify any network request headers and they're ignored by CORS protocol. But after Chrome 79, the CORS protocol inspects modified headers and will trigger CORS preflight request to the destination servers when the modified request doesn't meet the SimpleRequest requirement. Response header modifications also couldn't deceive the CORS checks. Additionally, webRequest API will stop seeing Origin header. Extensions can specify 'extraHeaders' in opt_extraInfoSpec to keep the original behaviors. If enterprise users are using a Chrome extension that's affected by this change, one of the following changes will need to be made:

- Ask the Extension author to upgrade the extension to specify 'extraHeaders' in opt_extraInfoSpec.
- Update the server-side logic to accept the CORS requests correctly. See the Extensions API document for more details.

Behavior changes for headers injected by Chrome—Before this change, headers injected by Chrome for a particular enterprise policy didn't trigger the CORS protocol. But after this change, it will start to be verified by the CORS protocol and will trigger CORS preflight requests. Server implementations might need to be updated to handle CORS preflight requests.

Shared clipboard between computers and Android devices in Chrome 79

Users will have the option to share their clipboard content between their computers and Android devices. To share, they need to have Chrome Browser installed, be signed in on both devices with the same account, and have Chrome sync enabled.

The text is end-to-end encrypted, and Google can't see the contents. This feature will be controllable with an enterprise policy.

Audio sandbox in Chrome 79

The audio service on Windows will be sandboxed in Chrome 79 for added security. We have seen incompatibilities with certain configurations of AppLocker in Chrome 77, although these have been fixed in Chrome 78. Other similar products might also have issues with the sandbox. If your users have issues with audio playing in Chrome 79, you can disable the audio sandbox with the AudioSandboxEnabled policy.

HTTPS pages will only be able to load secure subresources, with changes from Chrome 79 to Chrome 81

In Chrome 79, we'll introduce a new setting to unblock mixed content on specific sites. This setting will apply to mixed scripts, iframes, and other types of content that Chrome currently blocks by default. Users can switch this setting by clicking the lock icon on any https:// page and clicking **Site Settings**.

In Chrome 80, mixed audio and video resources will be autoupgraded to https://, and Chrome will block them by default if they fail to load over https://. Users can unblock affected audio and video resources with the setting described above. Also in Chrome 80, mixed images will still be allowed to load, but they will cause Chrome to show a "Not Secure" chip in the omnibox.

In Chrome 81, mixed images will be autoupgraded to https://, and Chrome will block them by default if they fail to load over https://.

More information on these changes is available in the Chromium blog.

On Linux, server certificate verification will use the built-in certificate verifier instead of NSS, starting in Chrome 79

Chrome on Linux will perform verification of server certificates using the built-in certificate verifier instead of NSS, starting in Chrome 79. The built-in verifier will still use the NSS trust store, so we expect that users won't see this change change. However there are some cases where differences might occur:

- Certificates with invalid encodings: The built-in verifier is stricter about enforcing spec compliance and might reject some certificates that NSS allowed. This should not affect any publicly trusted certificates, but might affect enterprises with internal PKIs.

- Directly trusted end-entity (leaf) certificates: The built-in verifier does not support directly marking server certificates as trusted; certificates must be issued by a CA that is trusted.

The verifier can be toggled using the BuiltinCertificateVerifierEnabled enterprise policy, allowing affected enterprises a chance to update their certificate infrastructure if they are affected by the transition. The policy will be supported through Chrome 82 on Linux to give enterprises sufficient time to update and test their infrastructure. Chrome OS switched to the built-in verifier in Chrome 77, and the policy will be supported on that platform through Chrome 80.

Ambient authentication disabled by default in Incognito mode in Chrome 80

Ambient authentication (NTLM/Kerberos) will be disabled by default in Incognito mode. You will be able to use a policy to revert to the old behavior and allow ambient authentication.

Pop-ups and synchronous XHR requests not allowed on page unload in Chrome 80

Note: These changes were originally planned for Chrome 78.

Pop-ups and synchronous XHR requests won't be allowed on page unload. This change will improve page load time and make code paths simpler and more reliable. If you encounter incompatibilities with legacy software, you will be able to revert to behavior matching Chrome 79 and earlier using the following policies, which will be available until Chrome 82:

- Allow pop-ups on page unload: AllowPopupsDuringPageUnload
- Allow synchronous XHRs on page unload: AllowSyncXHRInPageDismissal

FTP support will be removed in Chrome 80

FTP won't be directly supported in Chrome Browser. Your users should use a native FTP client instead. To help with the transition, you will be able to use the FTPProtocolSupport policy to temporarily re-enable FTP until Chrome 82.

TLS 1.3 hardening measure implemented in Chrome 81

TLS 1.3 includes a hardening measure to strengthen the protocol's protections against a downgrade to TLS 1.2 and earlier. This measure is backward compatible and doesn't require that proxies support TLS 1.3. It only requires that proxies correctly implement TLS 1.2. However, last year, we had to partially disable this measure due to bugs in some noncompliant, TLS-terminating proxies.

The following list contains the minimum firmware versions for affected products that we're aware of:

Palo Alto Networks:

- PAN-OS 8.1 must be upgraded to 8.1.4 or later.
- PAN-OS 8.0 must be upgraded to 8.0.14 or later.
- PAN-OS 7.1 must be upgraded to 7.1.21 or later.

Cisco Firepower Threat Defense and ASA with FirePOWER Services when operating in “Decrypt - Resign mode/SSL Decryption Enabled” (advisory PDF):

- Firmware 6.2.3 must be upgraded to 6.2.3.4 or later.
- Firmware 6.2.2 must be upgraded to 6.2.2.5 or later.
- Firmware 6.1.0 must be upgraded to 6.1.0.7 or later.

Starting in Chrome 79, you will be able to opt in to the new measure to test it and confirm if your proxy is affected, using the TLS13HardeningForLocalAnchorsEnabled policy. If you encounter problems, you should upgrade affected proxies to fixed versions.

Starting in Chrome 81, the new measure will become the default. However, you will be able to use the same policy to opt out if you need extra time to upgrade affected proxies. This proxy will be available until Chrome 86.

Updates to cookies with SameSite in Chrome 80

Starting in Chrome 80 on the Stable channel, cookies that don’t specify a SameSite attribute will be treated as if they were SameSite=Lax. Cookies that still need to be delivered in a cross-site context can explicitly request SameSite=None. The attributes must also be marked Secure and delivered over HTTPS.

This new behavior will also take effect in Chrome 79 on the Beta channel only. Because this change might be disruptive, we recommend you test critical sites on the Chrome 79 Beta channel, which will be available starting Oct. 31. See instructions for testing.

You will be able to revert to the legacy cookie behavior using policies, starting in Chrome 79 in Beta. You can specify trusted domains using LegacySameSiteCookieBehaviorEnabledForDomainList or control the global default with LegacySameSiteCookieBehaviorEnabled. For more details, visit Cookie Legacy SameSite Policies.

Tab groups will be introduced in Chrome 80

Users will be able to organize their tabs by grouping them on the tab strip. Groups can have colors and names. They'll help your users keep track of their different tasks and workflows.

Web Components v0 removed in Chrome 80

The Web Components v0 APIs (Shadow DOM v0, Custom Elements v0, and HTML Imports) were supported only by Chrome Browser. To ensure interoperability with other browsers, late last year, we announced that these v0 APIs were deprecated and will be removed in Chrome 80. You can find more information in the Web Components update.

Upcoming Chrome OS changes

Adding print server support for CUPS

We're working on a feature to add support for Common UNIX Printing System (CUPS) printing from print servers on Chrome OS. You and your users will be able to configure connections to external print servers and print from the printers on servers using CUPS.

Updates for USB devices with Linux

From the Chrome shell (crosh), you'll be able to attach a USB device to Linux apps running on a Chromebook so that Linux apps can access the Linux instance.

Upcoming Google Admin console changes

Managed guest session support for managed Google Play

A setting in the Admin console will allow Android apps to run in managed guest sessions (previously known as public sessions). Currently, Android apps can only run in a signed-in session.

Device host name in DHCP requests

You will be able to configure the device host name used during DHCP requests, including variable substitutions for ${ASSET_ID}, ${SERIAL_NUM}, ${MAC_ADDR}, and ${MACHINE_NAME}.