chrome enterprise

M89 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 March 9, 2021

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 89

Chrome Browser updates

Single words will not be treated as intranet locations by default

By default, Chrome will improve user privacy and reduce load on DNS servers by avoiding DNS lookups for single keywords entered into the address bar. This change may interfere

with enterprises that use single-word domains in their intranet. That is, a user typing "helpdesk" will no longer be directed to "https://helpdesk/".

You will be able to control the behavior of Chrome using the IntranetRedirectBehavior enterprise policy, including preserving the existing behavior (**value 3**: Allow DNS interception checks and did-you-mean "http://intranetsite/" infobars.).

Some users saw this change in Chrome 88; a full rollout is planned in Chrome 89.

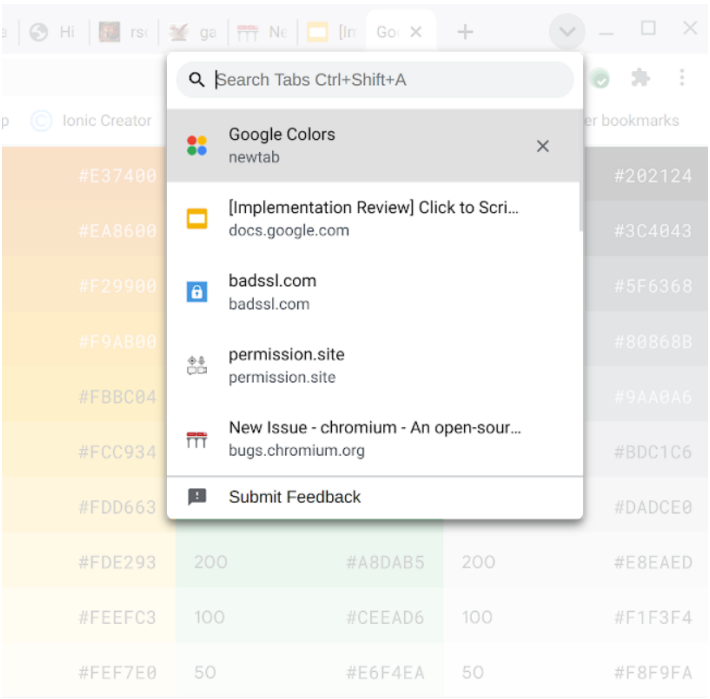
Chrome will prefer https to http when not specified in the address bar

When a user types an address into the address bar without specifying the protocol, Chrome will attempt to navigate using *https* first, then fallback to *http* if *https* is not available. For example, if the user navigates to *example.com*, Chrome will first attempt to navigate to **https**://*example.com*, then fallback to **http**://*example.com* if required.

Some users on Windows, Mac, Linux, and Android will see this change in Chrome 89, and all users should see this change in Chrome 90.

Users can search open tabs

Users can search for open tabs across windows, as shown in this screenshot:



Enterprise realtime URL checking enabled by BeyondCorp Enterprise

Chrome 89 will introduce new security capabilities enabled by BeyondCorp Enterprise allowing checking URLs for phishing attacks in realtime for BeyondCorp Enterprise customers.

Chrome profiles for separating users or accounts

Chrome 89 will add new features to help different users keep their browsing data like bookmarks, history, and settings separate.

Users will be given the option to create a new Chrome profile and move their account over, when they sign in to a profile where another account is already signed in.
If a user signs in with an account that is already signed in to another profile, they're offered to switch. Users who have multiple profiles set up will see a profile picker on startup.

You will be able to control whether Chrome offers to create or switch profiles with the SigninInterceptionEnabled enterprise policy and ProfilePickerOnStartupAvailability enterprise policies.

Certain features are available to users who have signed in without having to enable Chrome Sync

Some users who have signed into Chrome may be able to access and save payment methods and passwords stored in their Google Account without Chrome Sync being enabled.

You can control users' access to payment methods on Chrome on Android using the AutofillCreditCardEnabled enterprise policy. You can control access to passwords on Chrome on desktop by either setting the SyncDisabled enterprise policy to disabled, or by including "passwords" in SyncTypesListDisabled.

Chrome on Android will require the device to be certified

Chrome on Android will only be able to run on devices that are Play Protect certified. This affects all instances of Chrome including PWAs, but does not include WebView.

Chrome on VMs and emulators will continue to work if an emulator is emulating an approved device or the emulator is Google-developed.

See the Android Help Center article for details on how to verify a device's certification status.

Version pinning for self-hosted extensions & apps

To increase the stability in high-reliability environments, Chrome 89 will facilitate the pinning of extensions and apps to a specific version. Administrators will self-host the extension or app of their choice, and will instruct Chrome to use the update URL from the extension forcelist instead of the extension manifest. This will be via a new boolean parameter in ExtensionSettings policy. As a result, extensions & apps will not be updated via the updateURL that was originally configured in their manifest, and will stay on one specific version.

Chrome will introduce privacy-preserving APIs to replace some of the functionality of third-party cookies

Several changes are coming in Chrome 89 to build a more private web. We originally announced these changes in the Chromium Blog.

FLoC, an interest-based targeting API will be introduced as an origin trial. This API allows working with cohorts—groups of users with similar interests. **Users cannot be individually identified.**

An event-level conversion API will continue in the origin-trial stage for Chrome 89. This API enables the correlation of an ad click on a website with a subsequent conversion on an advertiser site (a sale, a sign-up, etc). **Users cannot be individually identified.**

Platform-provided trust tokens will be introduced to the ongoing Trust Token API Origin Trial. This experiment will be used to ascertain the value of tokens incorporating on-device state as a mechanism for anti-spam and anti-abuse systems, and to evaluate the feature's performance relative to standard "web-issued" trust tokens.

First party sets will be introduced as an origin trial. This allows a collection of related, commonly-owned domains to declare themselves as a first party set, so that browsers can consider this relationship when applying cross-site communication policies.

Schemeful Same-Site, which evolves the definition of "same-site" to include the URL scheme, will be fully rolled out and available to all audiences.

User Agent Client Hints will also be full rolled out and available to all audiences.

See the chromium privacy sandbox page for details on these APIs and the privacy sandbox.

Chrome will require SSE3 for Chrome on x86

Chrome 89 and above will require x86 processors with SSE3 support. This change does not impact devices with non-x86 (ARM) processors. Chrome will not install and run on x86 processors that do not support SSE3. SSE3 was introduced on Intel CPUs in 2003, and on AMD CPUs in 2005.

Chrome introduces BrowsingDataLifetime and ClearBrowsingDataOnExitList policies

Chrome gives you more control over data in your environment by introducing two policies that clear browsing data after a specified amount of time, or once Chrome has been closed: BrowsingDataLifetime and ClearBrowsingDataOnExitList. These policies are useful for customers that have strict regulatory requirements around data being stored on client devices.

Metrics reporting can be disabled by the user even if admin has it turned on

To improve user privacy, end users will be able to turn off metrics reporting for themselves, even if you have set **MetricsReportingEnabled** to true. If you set **MetricsReportingEnabled** to false, users will not be able to enable metrics.

Chrome introduces the Serial API

The Serial API will provide a way for websites to read and write from a serial device through script. You can read an explainer on the Serial API here.

You will be able to control access to the Serial API using the DefaultSerialGuardSetting policy. You can also use the SerialAskForUrls and SerialBlockedForUrls policies to control serial device access on a site-by-site basis.

Chrome on iOS introduces biometric authentication for Incognito tabs

Users will have a setting to enable access control for their Incognito tabs. When this setting is turned on, users will be prompted to re-authenticate themselves with biometric authentication when they return to Incognito tabs after closing Chrome on iOS.

Chrome OS updates

Extended auto-update blockout windows

Already as of today, the Chrome OS auto update blockout window device policy allows admins to block updates for their kiosk devices during certain business hours. This helps to save bandwidth in cases where Chromebooks are located at sites with limited network connectivity. From Chrome 89 on (official launch March 9th, 2021), the auto update blockout window policy will be extended. (1) Instead of only applying to kiosk sessions, it will also apply to user sessions & managed guest sessions (MGS). (2) Instead of only influencing the start of an update download, it will also pause previously started updates during blockout windows.

Due to the extended impact of the auto-update blockout window policy, an adjustment of your policy settings might be required to guarantee continuous updates of your devices.

Scaled Print Server Support

Admins can now assign any number of IPP based print servers to be remotely configured from the admin console. Users will now select a specific print server to connect to if the user has more than 16 print servers assigned. If there are less than 16 configured, Chrome OS will automatically query all assigned print servers simultaneously.

Scanning support

Chrome OS now supports the scanning functionality of compatible multifunction printers. Access to the Scan app on Chrome OS can be controlled by Admins.

QR code scanning support

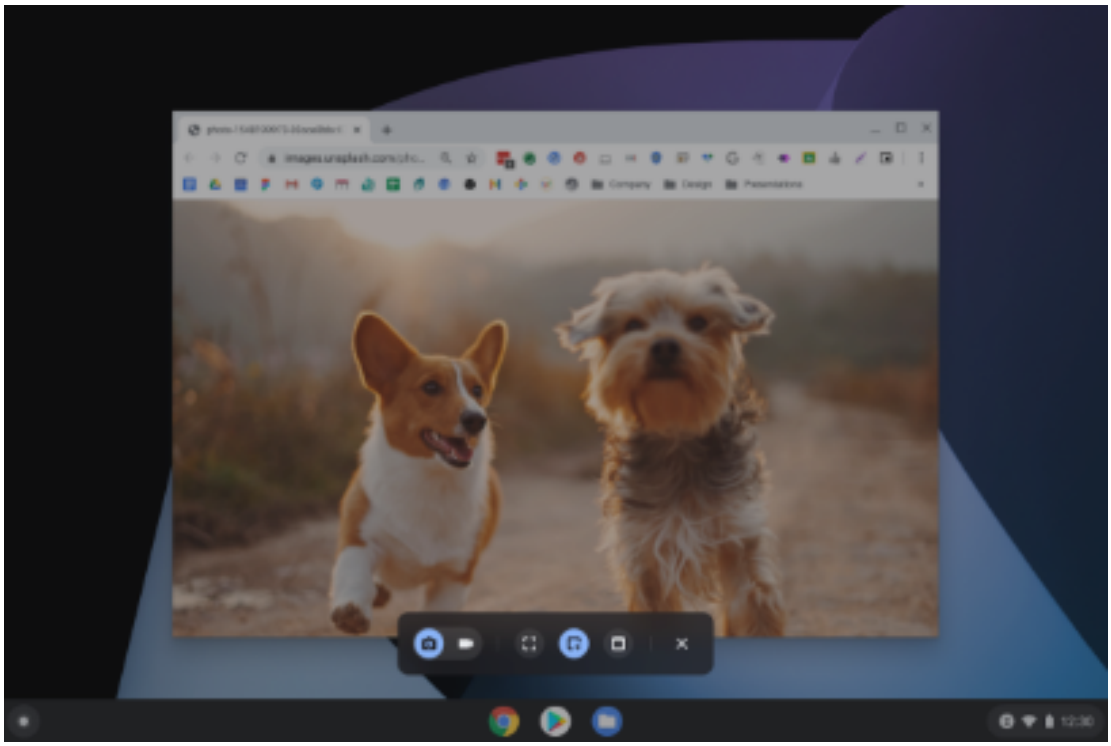
You will be able to scan QR codes with the Chrome OS Camera app. Just point your camera at a QR code and the results will automatically be scanned.

Switch Access settings Improvements

Switch Access settings will allow you to use any key or external switch and makes setting up your switches easier by replacing the drop down menu with just pressing the switch you want to use.

Enhanced Screen Capture

Chrome OS screen capture just got better. Screen capture functionality is now always accessible via quick settings. A new capture mode provides users with an intuitive UI to switch between functionality. After taking a partial screenshot, you can adjust the selection to perfect your capture. New screen recording functionality lets you capture and share motion.



Desk improvements

Improvements for frictionless smart creation and management of multiple workspaces (restore desks for browser, send to desk, and virtual desk improvements).

Wi-Fi Sync improvements

Wi-Fi Sync is now even more powerful, with added support for Wi-Fi network sharing between Chrome OS and Android.

Clipboard: visual clipboard history

Chrome OS introduces an extended clipboard to quickly transfer multiple pieces of content. Transfer everything you need with speed and ease.

Tote: quick access to recent and important Files

Quickly access your recent screenshots and downloads. Pin your important Files to launch, copy, or drag with one click.

Improved Media Controls

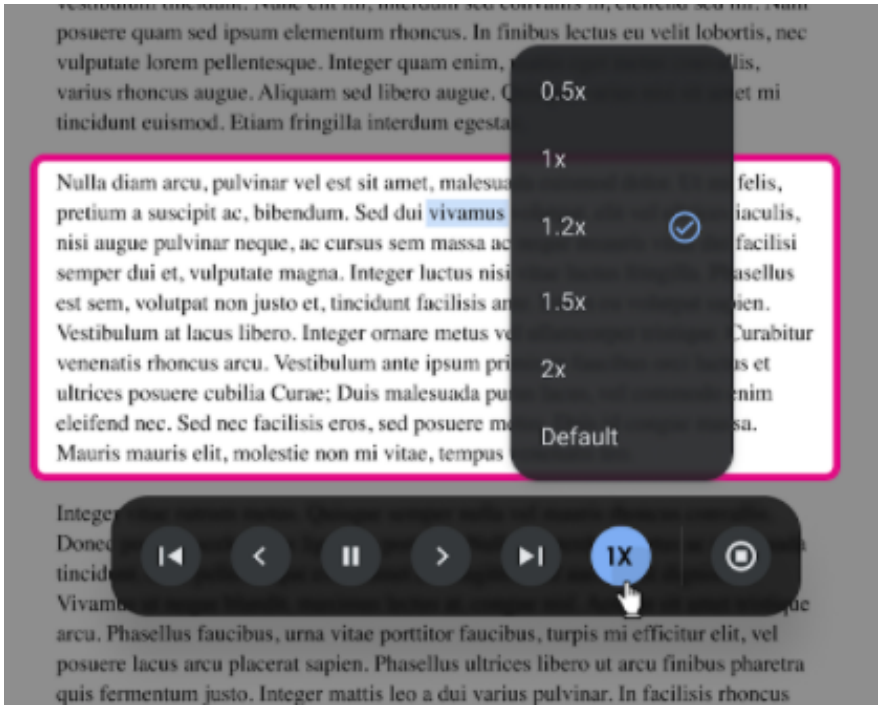
Brings unified media controls to quick settings. Access all your media sources in one place quickly.

App icon refresh

The icons for the built-in apps on your Chromebook have a fresh new look, making it easier for you to distinguish between the core essential apps (e.g. Canvas, Explore) that are made for Chrome OS and third-party apps that you've downloaded.

Enhanced Select-to-speak to better support users with Dyslexia

Improve the **Select-to-speak** accessibility service with navigation controls (play/pause, navigate sentences and paragraphs, adjust speed in context).



Admin console updates

Apps & Extension Usage Report

The Apps & Extension Usage Report report allows admins to get a comprehensive view of the apps and extensions installed across their fleet of ChromeOS and Chrome Desktop devices. Refer to the View app and extension usage details article on how to enable it.

Reports API

The Reports API enables you to generate reports that give you aggregate information on your managed Chrome OS device / Chrome Browser deployment. Please see the documentation here on how to use it.

Additional policies in the Admin console

Many new policies are available in the Admin console, including:

Policy name	Pages	Supported On	Category / Field
NTPContentSuggestionsEnabled	User & Browser Settings	Android	Startup / New Tab page content suggestions
RestrictAccountsToPatterns	User & Browser Settings	Android	User experience / Visible Accounts / Restrict accounts that are visible in Chrome to those matching one of the patterns specified
MediaRecommendationsEnabled	User & Browser Settings	Chrome OS, Windows, Mac, Linux	User experience / Media Recommendations
AllowFileSelectionDialogs	User & Browser Settings	Windows, Mac, Linux	User experience / File selection dialogs
AllowWakeLocks	User & Browser Settings; Managed Guest Session Settings	Chrome OS	Power and shutdown / Wake locks
IntranetRedirectBehavior	User & Browser Settings; Managed Guest Session Settings	Chrome OS, Windows, Mac, Linux	Network / Intranet Redirection Behavior

New and updated policies (Chrome Browser and Chrome OS)

Policy	Description
BrowsingDataLifetime	Browsing Data Lifetime Settings
ClearBrowsingDataOnExitList	Clear Browsing Data on Exit
EnableDeprecatedPrivetPrinting	Enable deprecated privet printing
ManagedConfigurationPerOrigin	Sets managed configuration values to websites to specific origins
PhoneHubTaskContinuationAllowed *Chrome OS only*	Allow Phone Hub task continuation to be enabled
PhoneHubAllowed *Chrome OS only*	Allow Phone Hub to be enabled
PhoneHubNotificationsAllowed *Chrome OS only*	Allow Phone Hub notifications to be enabled
ProfilePickerOnStartupAvailability *Browser only*	Profile picker availability on startup
RemoteAccessHostAllowRemoteAccessConnections *Browser only*	Allow remote access connections to this machine
RemoteAccessHostMaximumSessionDurationMinutes *Browser only*	Maximum session duration allowed for remote access connections
SigninInterceptionEnabled *Browser only*	Enable signin interception

Coming soon

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

Chrome is moving to a 4-week stable channel and introducing an 8-week extended stable channel as early as Chrome 94

Chrome on mobile, Windows, Mac, and Linux will move from its current 6-week release cycle to a 4-week release cycle, allowing security features, new functionality and bug fixes to reach users more quickly.

No action is required for most enterprises, but if you manually update or test new releases of Chrome and prefer a slower release cadence, you'll be able to switch Chrome to an extended stable channel, with a new release every 8 weeks instead. More details can be found on our blog post at blog.chromium.org.

Chrome OS is also planning changes to the release cycle during the same release. As always, Chrome OS will prioritize the latest security updates, and maintain a high quality and stable experience for users, customers, partners, and developers.

Upcoming Chrome Browser changes

Chrome 90 will block port 554

Port 554 will be added to the restricted ports list and traffic through it will be blocked. This should have no effect on customers using standard ports, but custom configurations (for example, delivering PAC scripts) using non-standard ports may be affected. You should instead use standard ports for your use case (for example, delivering PAC scripts via HTTPS through port 443).

Launch of PDF XFA forms in Chrome 90

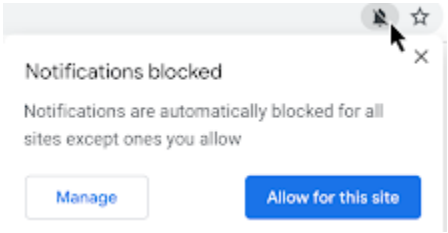
PDF XFA forms will be partially supported in Chrome 90, expanding the range of PDF documents that can open directly in Chrome.

Managed profile sign-in popup will be more clear in Chrome 90

Chrome 90 will update the notice when users sign into a managed profile. The new notice has more clear language and the available actions have been simplified

Some permission requests will be less intrusive in Chrome 90

Permission requests that the user is unlikely to allow will be automatically blocked. A less intrusive UI will allow the user to manage permissions for each site.



Chrome 90 will support Intel CET

Chrome 90 will support Intel's Control Flow Enforcement Technology (CET), known as Hardware-enforced Shadow Stacks on Windows. This will only affect Chrome running on hardware that supports CET. While no issues are expected, you can manage CET by manipulating Image File Execution Options (IFEO) through group policy.

Chrome 90 will introduce initial_preferences

As part of Chrome's move to using more inclusive naming, Chrome will support an admin using a file to control the browser's initial preferences, named initial_preferences. This file behaves the same way as, and will eventually replace the master_preferences file that exists

today. To minimize any disruption, master_preferences will continue to be supported in Chrome 90 and more notice will be given before support for master_preferences is removed.

AllowNativeNotifications updated to AllowSystemNotifications in Chrome 90

As part of Chrome's move to using more inclusive policy names, AllowNativeNotifications will be renamed to AllowSystemNotifications. The existing AllowNativeNotifications policy will be available until Chrome 95.

Extension settings will load from the same place for all channels on Mac in Chrome 90

All Chrome channels will read the extension policies from the same .plist file. For example, the extension Password Alert will always load its policies from com.google.Chrome.extensions.noondiphcddnnabmjcihcjfbhfklnnep.plist instead of com.google.Chrome.canary.extensions.noondiphcddnnabmjcihcjfbhfklnnep.plist in Chrome Canary.

Chrome will save data with Lite videos in Chrome 90

To reduce the data-cost and improve the experience of videos on metered and limited data connections, Chrome on Android will reduce the effective bitrate of videos for Lite mode users on cellular connection. You will be able to control this feature using the DataCompressionProxyEnabled policy.

Data Saver: Chrome compresses public HTTPS images in Chrome 90

Public HTTPS images are compressed when Chrome lite mode is enabled, to further provide a rich web experience to users with unreliable internet connections.

Security key enterprise attestation in Chrome 90

Chrome will support device-unique attestation of security keys without needing policy configured. This is useful in situations where security keys are distributed by an enterprise to personnel who may use them on non-policy-managed computers. This requires specially-manufactured security keys—talk to your security key vendor if this sounds useful.

Launch WebXR capability - Depth Sensing API in Chrome 90

The WebXR Depth Sensing API allows Chrome to measure distance from the user's device to real world geometry in the user's environment. With this, Chrome will be able to power immersive experiences in WebXR-powered apps (e.g. for physics, and lifelike occlusion for augmented reality).

You will be able to control access to WebXR and other augmented reality APIs using the WebXRImmersiveArEnabled enterprise policy.

Partition Network State in Chrome 90

Today, some network objects are shared globally for performance reasons, but this makes it possible to fingerprint users and track them across sites. To protect user privacy, Chrome will partition many network objects by topmost frame domain and iframe domain. A comprehensive description is available here.

No impact is expected other than minor performance changes, but you can test the change in advance by using the command line flag:

```
--enable-features=PartitionConnectionsByNetworkIsolationKey,PartitionExpectCTStateByNetworkIsolationKey,PartitionHttpServerPropertiesByNetworkIsolationKey,PartitionNelAndReportingByNetworkIsolationKey,PartitionSSLSessionsByNetworkIsolationKey,SplitHostCacheByNetworkIsolationKey
```

Legacy Browser Support for Edge in IE Mode will be available in Chrome 90

For organizations accessing legacy web content in Microsoft Edge's IE mode, Chrome 90 will allow admins to configure Legacy Browser Support (LBS) to switch between Microsoft Edge in IE mode and Chrome. You can already use LBS to switch directly between Microsoft Internet Explorer and Chrome.

The Network Service on Windows will be sandboxed in Chrome 91

The network service, already running in its own process, will be sandboxed on Windows in Chrome 90 to improve the security and reliability of the service. As part of this, third party code that is currently able to tamper with the Network Service will be prevented from doing so. This may cause problems when connecting to software such as:

- Custom Authentication Packages.
- Custom SSO (Single Sign-on) providers.
- Custom Winsock Namespace/transport providers.
- Data Loss Prevention software.
- NTLM with Windows integrated authentication.

Enterprises are encouraged to try the sandboxed network stack on Dev and Canary channel and report any issues via crbug.com. You'll be able to disable the change with an enterprise policy when it becomes available.

Lock in address bar will be replaced in Chrome 91

The lock in the address bar will be replaced with a new icon. Chrome is moving to security messaging that highlights known security issues, and shows neutral messaging otherwise. Showing an icon that implies safety based solely on the connection's encryption may lead to a false sense of security.

Quantum computer resistant security will be enabled in Chrome 91

Chrome will start supporting a post-quantum key-agreement mechanism in TLS when communicating with some domains. This increases the size of TLS handshake messages which, in rare cases, may cause issues with network middleboxes that incorrectly assume that TLS messages will fit in a single network frame.

The **CECPQ2Enabled** policy can be set to disable this. It will also be disabled if the ChromeVariations policy is set to a non-default value.

For more details on this rollout, see https://www.chromium.org/cecpq2.

Insecure public pages no longer allowed to make requests to private or local URLs in Chrome 91

Insecure pages will no longer be able to make requests to IPs belonging to a more private address space (as defined in CORS-RFC1918). For example, **http**://public.page.example.com will not be able to make requests targeting IP 192.168.0.1 or IP 127.0.0.1. You will be able to control this behavior using the **InsecurePrivateNetworkRequestsAllowed** and **InsecurePrivateNetworkRequestsAllowedForUrls** enterprise policies.

The address bar may show the domain rather than the full URL as early as Chrome 90

To protect your users from some common phishing strategies, Chrome will test showing only the domain in the address bar for some users. This change makes it more difficult for malicious actors to trick users with misleading URLs. For example, **https://example.com/secure-google-sign-in/** will appear only as **example.com** to the user.

Although this change is designed to keep your users' credentials safe, you can revert to the old behavior through the ShowFullUrlsInAddressBar policy.

This change has been enabled for some users, with a potential full rollout in a later release.

The SSLVersionMin policy will not allow TLS 1.0 or TLS 1.1 in Chrome 91

The SSLVersionMin enterprise policy allows you to bypass Chrome's interstitial warnings for legacy versions of TLS. This will be possible until Chrome 91 (May 2021), then the policy will no longer allow TLS 1.0 or TLS 1.1 to be set as the minimum.

We previously communicated that this would happen as early as January 2021, but the deadline has since been extended.

Chrome will maintain its own default root store as early as Chrome 92

In order to improve user security, and provide a consistent experience across different platforms, Chrome intends to maintain its own default root store. If you are an enterprise admin managing your own certificate authority, you should not have to manage multiple root stores.We do not anticipate any changes to be required for how enterprises currently manage their fleet and trusted enterprise CAs, such as through group policy, macOS Keychain Access, or system management tools like Puppet.

SyncXHR policy will no longer be supported on Chrome 93

The AllowSyncXHRInPageDismissal enterprise policy will be removed in Chrome 93. For any apps that rely on the legacy web platform behavior, be sure to update them before Chrome 93. This change was previously planned for Chrome 88, but delayed to provide more time for enterprises to update legacy applications.

Old policies with non-inclusive names will be removed in Chrome 95

Chrome 86 through Chrome 90 introduced new policies to replace policies with less inclusive names (for example, whitelist, blacklist). In order to minimize disruption for existing managed users, both the old and the new policies currently work. This transition time is to ensure it's easy for you to move to and test the new policies in Chrome.

This transition period will end in Chrome 95. A full list of the policies to be removed will be provided closer to the removal date. If you're managing Chrome via the Google Admin Console (for example, Chrome Browser Cloud Management), no action is required; the Google Admin Console will manage the transition automatically.

Upcoming Chrome OS changes

Deprecation of AMR and GSM audio codecs in Chrome OS 90

AMR-NB, AMR-WB, and GSM audio codecs will be deprecated as part of this release. Affected users should file bugs here and may temporarily rollback this change via the use of chrome://flags/#deprecate-low-usage-codecs. Users with long-term need for these codecs may use stand-alone applications found in the Google Play Store.

Upcoming Admin Console changes

Sending Extension Requests for Chrome Browser and Chrome OS

As an admin, you can block users from installing extensions and the Chrome Web Store will now have a “Request” button so that you can see their requests from within the Admin Console and take an action to allow or to block the extensions.

Sending Remote Commands for Chrome Desktop

As an admin, you can use your Google Admin console to remotely send actions to managed Chrome Desktop Browsers (Win/Mac/Linux). For example, you will be able to delete browser cache or cookies remotely.