chrome enterprise

Chrome 96 Enterprise release notes

For administrators who manage Chrome browser or Chrome devices for a business or school.

We are in the process of improving the release notes and we would love to hear your feedback. Please fill out [this survey](#) to let us know what you think.

These release notes were last updated on December 06, 2021.

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

Release summary

Place a check (✓) in the appropriate category.

Chrome browser updates	Security	User productivity /Apps	Management
Chrome on Android no longer supports Android Lollipop			✓
Apps shortcut in the bookmarks bar defaults to off		✓	
Network data moves to a new folder on Windows	✓		
New security events for BeyondCorp Enterprise Threat and Data Protection	✓		
Feature flag to force the Chrome Major Version number to 100			✓
DNS-based HTTP to HTTPS redirect	✓		
Chrome shows Journeys in the History page		✓	
Chrome starts deprecating the U2F security key API	✓	✓	
Chrome on Android shows reuse warnings for Google passwords	✓		
Chrome sync ends support for Chrome 48 and earlier			✓
Google Toolbar for Internet Explorer no longer available		✓	
Chrome installer for macOS now available as a single *universal* version		✓	
New and updated policies in Chrome browser			✓
Chrome OS updates			
Long-term support channel			✓
Cloud Based Certificate Provisioning using SCE	✓		✓
SAML password change : Chrome Device Token API	✓		
Terms of Service for managed user sessions			✓
Side Search on Chrome OS		✓	

	Security	User productivity /Apps	Management
Nearby Share from ARC++ sharesheet		✓	
Switch Access Setup Guide		✓	
New preference setting for Link capturing		✓	
Add clipboard suggestions to Virtual Keyboard		✓	
Chrome Wallpaper app migration		✓	
Move Notifications to Chrome OS Settings		✓	
Admin console updates	**Security**	**User productivity /Apps**	**Management**
New interface for selecting Chrome apps and extensions		✓	✓
New policies in the Admin console			✓
Upcoming Chrome browser changes	**Security**	**User productivity /Apps**	**Management**
Launch Control Flow Guard for Windows	✓		
Network Service on Windows will be sandboxed	✓		
Certificate Transparency enabled on Chrome for Android	✓		
CORS Authorization mishandling	✓		
Chrome will maintain its own default root store	✓		
Chrome will no longer allow TLS 1.0 or TLS 1.1			✓
Chrome autofill will be more predictable		✓	
New Manifest V2 extensions not accepted after January 17, 2022	✓	✓	
Different-origin iframes JavaScript dialogs deprecation has been postponed indefinitely	✓		
Upcoming Admin console changes	**Security**	**User productivity /Apps**	**Management**
Browser list data downloadable in CSV format			✓

Read-only privilege for managed browsers			✓
Reports overview page			✓
Insights report: Devices that need attention			✓

Current Chrome version release notes

Chrome browser updates

Chrome on Android no longer supports Android Lollipop

Chrome 96 does not support or ship to users running Android Lollipop.

The last version of Chrome that supports Android Lollipop is Chrome 95, and it included a message to affected users informing them to upgrade their operating system.

Apps shortcut in the bookmarks bar defaults to off

The Apps shortcut in the bookmarks bar now defaults to off. Chrome also updates the current state for all users who have not changed their setting to the new default (off).

Network data moves to a new folder on Windows

Data that is needed by the network service, including cookies and other data files, is now stored in a subdirectory underneath the previous location called *Network*. This is to support the upcoming Network Sandbox (see below). This migration happens automatically and transparently. No action is required, however, you might need to update any scripts that rely on the location of these files.

New security events for BeyondCorp Enterprise Threat and Data Protection

Chrome 96 adds two new security events to [BeyondCorp Enterprise Threat and Data Protection](#): Password leak and login. This functionality allows admins to understand enterprise credential usage, to shadow IT within their organization, and to stay ahead of potential security incidents regarding passwords exposed in data breaches.

Feature flag to force the Chrome Major Version number to 100

Starting in Chrome 96, users and site owners can experiment with the upcoming three-digit (Chrome 100) major release version number in the User-Agent string by turning on the *ForceMajorVersion100InUserAgent* flag. This forces the browser to send 100 as the major version number. When browsers went from version 9 to 10, the increase in the number of digits in the major version number uncovered many issues in User-Agent string parsing libraries. With this feature flag, we can uncover and address these issues before Chrome 100 rolls out. We encourage admins to submit any issues encountered [here](#).

DNS-based HTTP to HTTPS redirect

Chrome queries [DNS for HTTPS records](#) (alongside traditional A and AAAA queries). When a website has deployed an HTTPS DNS record and Chrome receives it, Chrome always connects to the website via HTTPS ([Chrome Status](#)). This was previously enabled for 50% of users on the Canary, Dev, and Beta channels.

Chrome shows Journeys in the History page

For some users, Chrome 96 clusters local browsing activity on the History page into Journeys to make it easier to find prior activity and continue it with related search suggestions. For keywords typed into the Omnibox that match a cluster, an action chip displays for seamless access to the Journeys view. Users can delete clusters and disable Journeys, if desired. Additionally, admins will have the option to disable this feature using the **HistoryClustersVisible** policy, starting in Chrome 97.

Chrome starts deprecating the U2F security key API

The U2F API is Chrome's legacy API for interacting with USB security keys. It has been superseded by the W3C Web Authentication API (WebAuthn). Beginning with Chrome 96, when sites make U2F API requests, users might see a prompt that includes a notice about the U2F API's deprecation. In Chrome 98, Chrome will disable the U2F API by default. With Chrome 104, the U2F API will be removed from Chrome.

Sites can continue to use the U2F API beyond Chrome 98 if they enroll in an Origin Trial. Using the Origin Trial also suppresses the deprecation prompt on the enrolled pages. The Origin Trial will end on July 26, 2022, shortly before the release of Chrome 104.

Enterprises can suppress deprecation related changes, and keep the U2F enabled, by using the U2fSecurityKeyApiEnabled enterprise policy. This enterprise policy will be removed from Chrome, together with the U2F API, in Chrome 104.

If you run a website that still uses this API, please refer to the deprecation announcement and blog post for more details.

Chrome on Android shows reuse warnings for Google passwords

Similar to Chrome on other platforms, Chrome on Android now shows warnings if it detects that your Google passwords were reused on a malicious website. You can control this behavior using the PasswordProtectionWarningTrigger enterprise policy.

Chrome sync ends support for Chrome 48 and earlier

As previously communicated, Chrome sync no longer supports Chrome 48 and earlier. You need to upgrade to a more recent version of Chrome if you want to continue using Chrome sync.

Google Toolbar for Internet Explorer no longer available

The Google Toolbar for Internet Explorer is being phased out. As of mid-November, it will no longer be available for download.

Chrome installer for macOS now available as a single "universal" version

The `.dmg` installer available to users on macOS now contains both the x86_64 and the arm64 versions of the product. When installing, users no longer have to choose the CPU architecture. Existing Chrome installations will be updated to universal automatically. This may increase the size of Chrome on disk.

Note that the enterprise-specific `.pkg` installer was already a universal installer.

New and updated policies in Chrome browser

Policy	Description
SyncDisabled (new on iOS)	Control Chrome sync.
U2fSecurityKeyApiEnabled	Allow use of the deprecated U2F Security Key API.
CloudUserPolicyOverridesCloudMachinePolicy	Allow user cloud policies to override Chrome Browser Cloud Management policies.
SandboxExternalProtocolBlocked	Allow Chrome to block navigations toward external protocols in sandboxed iframes.
BrowsingDataLifetime (new on Android)	Configure (per data-type) when data is deleted by the browser.
WebSQLInThirdPartyContextEnabled	Temporarily re-enables WebSQL in third-party contexts.
PromptOnMultipleMatchingCertificates	Prompt for the client certificate when multiple certificates match.
NetworkServiceSandboxEnabled	Controls whether or not the network service process runs sandboxed.

Chrome OS updates

For over a decade, Chrome OS has delivered new milestone releases every six weeks, providing users and IT with a secure, speedy, and stable experience. Earlier this year, we announced that Chrome OS would switch to a 4-week stable release, starting with Chrome 96. This shift allows us to deliver features and security updates more quickly.

Long-term support channel

From Chrome 96, Chrome OS provides an option for organizations to use a new Long-term support (LTS) channel, with feature milestone updates every six months. Devices on the LTS channel will still receive frequent security updates. Admins can easily switch from LTS to other channels if desired. For more details, see this article.

Cloud Based Certificate Provisioning using SCEP

Chrome OS provides a new way to provision and renew certificates on managed devices in Microsoft Active Directory Certificate Service (ADCS) environments using the Simple Certificate Enrollment Protocol (SCEP). The new provisioning flow, for device-based certificates, enables automated certificate deployment and renewals that occur with no end user interaction and before user sign-in. For more details, see this article.

SAML password change : Chrome Device Token API

Chrome 96 supports password updates on Chrome OS devices after a user's password is changed on a third-party Identity Provider (IdP). This helps to increase the convenience for the end user, and to enforce corporate policies on Chrome OS devices. Admins can use the Chrome Device Token API to allow IdPs to notify Chrome OS devices that users have changed their password. API documentation is available, and this article (step 4/5) has been updated with guidance for administrators.

Terms of Service for managed user sessions

Admins can now display their Terms of Service to users at the beginning of every managed user's session. This functionality was previously available for managed guest sessions only.

Side Search on Chrome OS

To make it easier to compare search results and find what you're looking for more quickly in Chrome browser, there's a new side panel in Chrome OS. You can now view a page and the search results at the same time. This lets you view a page right in your main browser window without needing to navigate back and forth or losing your search results. Admins can disable this feature via the **SideSearchEnabled** policy.

Nearby Share from ARC++ sharesheet

This feature allows users to use Nearby Share from Android Runtime for Chrome (ARC++). Prior to this Nearby Share has been available in Files app, PWAs and other system apps. Nearby Share allows users to easily share content across devices, for example, from Chromebook to a device running Chrome browser, such as an Android phone or aWindows PC.

Switch Access setup guide

Switch Access is an alternate input method that enables users to control their device with just one or more buttons. As of Chrome 96, Switch Access users will now have a setup guide which will help walk new users through the process of setting up and using their switches.

New preference setting for link capturing

This adds a new preference to Apps settings that allows users to set apps as the default handler of supported links. For example, the Zoom PWA can become the default handler for *zoom.us* links.

Add clipboard suggestions to on-screen keyboard

Chrome 96 suggests recently copied items in the [on-screen keyboard](#) or Virtual Keyboard suggestion row to simplify your paste actions. If you copy an item and open your Virtual Keyboard you should see that item as an option in the top row. Click it to paste. Previously, Chrome 94 made clipboard items accessible from the virtual keyboard. Chrome 96 adds clipboard items copied within the last two minutes to the suggestion row in the virtual keyboard for even easier access.

Chrome Wallpaper app enhancements

TheChrome OS wallpaper picker now has a more visual UI that helps users to select from a variety of wallpaper collections or their own images. Users can open it from the home screen using right-click > **Set wallpaper**.

Notification settings move to Chrome OS Settings

Chrome 96 includes a new dedicated Notifications page in Chrome OS Settings. In earlier releases, Notifications were accessed from the Quick Settings menu.

Admin console updates

New interface for selecting Chrome apps and extensions

The Admin console now uses the same user interface as the Chrome Web Store for selecting new Chrome apps and extensions.
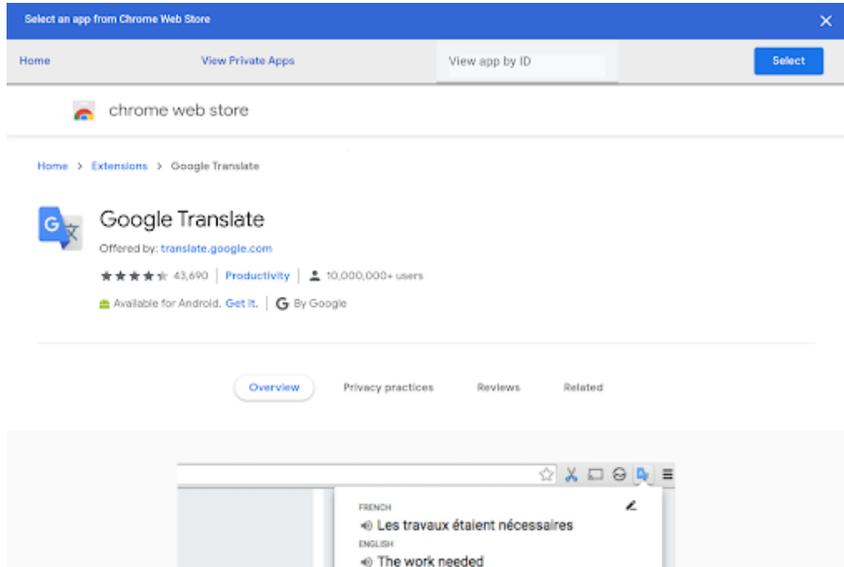
New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
DevicePciPeripheralDataAccessEnabled	Device Settings	Chrome OS	Other settings > Data access protection for peripherals
InsecurePrivateNetworkRequestsAllowed	User & Browser Settings; Managed Guest Session Settings	Chrome Chrome OS Android	Content > Request from insecure websites to more-private network endpoints
VirtualKeyboardFeatures	Device Settings	Chrome OS	Kiosk settings > Kiosk virtual keyboard features
AllowedInputMethods	User & Browser Settings; Managed Guest Session Settings	Chrome OS	User experience > Allowed input methods
DisplayCapturePermissionsPolicyEnabled	User & Browser Settings; Managed Guest Session Settings	Chrome Chrome OS	Security > Insecure Media Capture
AllowedLanguages	User & Browser Settings; Managed Guest Session Settings	Chrome OS	User experience > Allowed chrome OS languages
SpellcheckLanguage	User & Browser Settings; Managed Guest Session	Chrome Chrome OS	User experience > Spell check > Enforced spellcheck languages

	Settings		
SpellcheckLanguageBlocklist	User & Browser Settings; Managed Guest Session Settings	Chrome Chrome OS	User experience > Spell check > Disabled spellcheck languages
CrossOriginWebAssemblyModuleSharingEnabled	User & Browser Settings	Chrome Chrome OS	Content > Allow WebAssembly cross-origin
LockScreenReauthenticationEnabled	User & Browser Settings	Chrome OS	Security > SAML single sign-on password synchronization flows
SamlInSessionPasswordChangeEnabled	User & Browser Settings	Chrome OS	Security > SAML single sign-on password synchronization > Password synchronization between third-party SSO providers and Chrome devices
SamlPasswordExpirationAdvanceWarningDays	User & Browser Settings	Chrome OS	Security > SAML single sign-on password synchronization > How many days in advance to notify SAML users when their password is due to expire
ManagedAccountsSigninRestriction	User & Browser Settings	Chrome	Sign-in settings > Separate profile for managed Google Identity
ArcAppToWebAppSharingEnabled	User & Browser Settings	Chrome OS	Android applications > Sharing from Android apps to Web apps

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.

Upcoming Chrome browser changes

Launch Control Flow Guard for Windows

As early as Chrome 97, Chrome will make security improvements by introducing Control Flow Guard (CFG) for Windows. This change might cause interoperability issues with software that injects code into Chrome's process space, such as Data Loss Prevention software. Please file a [bug](#) to let us know if you encounter issues.

As CFG affects how Chrome is compiled, it will not be possible to control it via enterprise policies, but you can test it in the Dev and Beta channels for Chrome 97.

Network Service on Windows will be sandboxed

As early as Chrome 97, to improve security and reliability, the network service, already running in its own process, will be sandboxed on Windows. As part of this, third-party code that is currently able to tamper with the network service may be prevented from doing so. This might cause interoperability issues with software that injects code into Chrome's process space, such as Data Loss Prevention software. An enterprise policy has been added to allow early testing of the new sandbox, and to disable the sandbox if incompatibilities are discovered. You can test the sandbox in your environment using [these instructions](#) and report any issues you encounter.

Certificate Transparency will be enabled on Chrome for Android

[Certificate Transparency](#) is already enforced on desktop platforms, and will be enforced for some users on Chrome 97 for Android, with a wider release planned for a later version. You can selectively disable Certificate Transparency using the [CertificateTransparencyEnforcementDisabledForCas](#),

CertificateTransparencyEnforcementDisabledForLegacyCas, and
CertificateTransparencyEnforcementDisabledForUrls enterprise policies.

CORS Authorization mishandling

When scripts make a cross-origin network request via `fetch()` and `XMLHttpRequest` with an Authorization header, the header should be explicitly allowed by the Access-Control-Allow-Headers header in the CORS preflight response (Chrome Status). The wildcard symbol (*) in the Access-Control-Allow-Headers should not work. This has not been implemented correctly, and the wildcard symbol has taken effect. This will be fixed in Chrome 97.

Note that Authorization headers attached by Chrome during the authentication process are out of scope for this change.

Chrome will maintain its own default root store

As early as Chrome 98, 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 (CA), you should not have to manage multiple root stores. We do not anticipate any changes will 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.

Chrome will no longer allow TLS 1.0 or TLS 1.1

The SSLVersionMin policy no longer allows setting a minimum version of TLS 1.0 or 1.1. This means the policy can no longer be used to suppress Chrome's interstitial warnings for TLS 1.0 and 1.1. Administrators must upgrade any remaining TLS 1.0 and 1.1 servers to TLS 1.2. In Chrome 91 we announced that the policy no longer works, but users could still bypass the interstitial. In Chrome 98, it will no longer be possible to bypass the interstitial.

Chrome Autofill will be more predictable

Chrome Autofill will be more visible with a new menu position. It will also add dynamic highlighting to show precisely what fields will be filled automatically.

New Manifest V2 extensions not accepted after January 17, 2022

As part of the gradual deprecation of Manifest V2, the Chrome Web Store will stop accepting submissions of *new* Manifest V2 extensions after January 17, 2022. This applies to all new extension submissions with visibility set to Public or Unlisted.

The change will not affect updates to already published extensions. Also, it will not impact extensions with visibility set to Private. The change is not expected to affect the operation of any existing extensions already deployed in Chrome.

Note that the next phase of deprecation in June of 2022, is expected to expand this restriction to extensions with Private visibility, which may have a more significant impact on Enterprise extension workflows.

For more details, refer to the [Manifest V2 support timeline](#).

Different-origin iframes JavaScript dialogs deprecation has been postponed indefinitely

Previously, we announced a planned change that would cause Chrome to prevent iframes from triggering prompts (`window.alert`, `window.confirm`, `window.prompt`), if the iframe is a different origin from the top-level page. This change was originally planned for Chrome 92, but has been postponed indefinitely due to the feedback we received on this change. We will provide advance notice in the future if we decide to re-enable this change.

You can test if this future change will affect applications now by setting the *enable_features=SuppressDifferentOriginSubframeJSDialogs* flag.

Upcoming Admin console changes

Browser list data downloadable in CSV format

As early as Chrome 97, Chrome will introduce an optional CSV format to download the browser list data from the Admin console.

Read-only privilege for managed browsers

As early as Chrome 97, Chrome will introduce a read-only privilege for managed browsers. Admins will be able to easily create custom admin roles with read-only access to managed browsers in the Admin console.

Reports overview page

A new reports overview page will provide a summary of all the reports available. The new page will be available under the **Device** > **Chrome** > **Reports** menu.

Insights report: Devices that need attention

A new report will highlight categories of devices that require attention. The new report will be available under the **Device** > **Chrome** > **Reports** > **Insights** menu.

The categories are:

- Devices that have not synched policies in 28 days
- Devices that have not seen user activity in 28 days
- Devices that are pending OS updates
- Devices that are not compliant with the OS version that was set by policy
  - For example, if a device policy requires Chrome 94 running on devices, but several devices are on Chrome 90
- Devices that are unable to apply a policy due to an OS mismatch
  - For example, if a set policy due to be applied has a minimum supported Chrome OS version of Chrome 96, but devices are on Chrome 90

Clicking on the category will take you to the device list page with filters applied according to the category.

For more details, see this Help Center article

Previous release notes

Chrome version & targeted Stable channel release date	PDF
Chrome 95: October 19, 2021	PDF
Chrome 94 OS: October 14, 2021	PDF
Chrome 94: September, 2021	PDF
Chrome 93: August, 2021	PDF
Archived release notes	

Additional resources

- For emails about future releases, sign up here.
- To try out new features before they're released, sign up for the trusted tester program.
- Connect with other Chrome Enterprise IT admins through the Chrome Enterprise Customer Forum.
- 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
- Developers: Learn about changes to the web platform and features planned for upcoming releases.

Still need help?

- Google Workspace, 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

Google and related marks and logos are trademarks of Google LLC. All other company and product names are trademarks of the companies with which they are associated.