B

How to Remove a Browser Hijacker from Chrome, Edge, or Firefox

Remove browser redirects, unwanted search changes, extensions, and persistent settings safely from Chrome, Edge, or Firefox on Windows.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 Signs that the browser is hijacked

02 1. Scan Windows before resetting the browser

03 2. Remove suspicious apps and extensions

04 3. Reset the affected browser

05 4. Check what can make the hijacker return

06 After cleanup

07 If redirects continue

08 How to prevent another browser hijacker

A browser hijacker changes your search engine, homepage, new-tab page, extensions, notifications, proxy, or browser shortcuts without clear permission. Resetting the visible setting may help temporarily, but the redirect can return if an unwanted program, managed policy, scheduled task, or modified shortcut remains on Windows.

If the unwanted component is identified as Conduit, Spigot, or Yontoo, its glossary guide can help interpret the name and associated browser changes. Match the installed component or detection evidence before assuming that a redirect belongs to one of these families.

01 Signs that the browser is hijacked

- Searches pass through an unfamiliar site or open unexpected results.
- The homepage or new-tab page changes again after you reset it.
- Chrome, Edge, or Firefox shows an extension or toolbar you did not install.
- Normal pages display extra ads, pop-ups, or notification prompts.
- The browser says it is “managed by your organization” on a personal PC.
- A browser shortcut opens with an extra website address or command-line option.

If the browser opened a fake sign-in or payment page, do not enter any more information until cleanup is complete.

02 1. Scan Windows before resetting the browser

1. Update your installed security software and its threat database.
2. Run a complete system scan, not only a scan of the browser folder.
3. Quarantine detected unwanted programs, adware, browser extensions, and persistence components.
4. Restart Windows if cleanup requests it, then scan again.

With Gridinsoft Anti-Malware, use the PC scanning guide and review each detection before applying an action. Quarantine is safer than manually deleting unknown registry entries or system files.

03 2. Remove suspicious apps and extensions

Open **Windows Settings → Apps → Installed apps** and sort by installation date. Remove software that appeared when the redirects began, especially unknown download managers, search assistants, PDF tools, media converters, or “browser protection” utilities.

Then inspect browser extensions:

- **Chrome:** Menu → Extensions → Manage extensions.
- **Edge:** Menu → Extensions → Manage extensions.
- **Firefox:** Menu → Add-ons and themes → Extensions.

Remove extensions you do not recognize. Do not keep an extension merely because it has a familiar icon or claims to be installed by an administrator.

04 3. Reset the affected browser

- **Chrome:** Settings → Reset settings → Restore settings to their original defaults.
- **Edge:** Settings → Reset settings → Restore settings to their default values.
- **Firefox:** Help → More troubleshooting information → Refresh Firefox.

A reset normally disables extensions and restores search, startup, new-tab, and content settings. It should not remove bookmarks or saved passwords, but review the browser's confirmation message before continuing. See How to reset browser settings with Gridinsoft Anti-Malware for the assisted cleanup option.

05 4. Check what can make the hijacker return

- **Browser shortcut:** right-click the shortcut, open Properties, and confirm that the Target ends with the legitimate browser executable rather than an added URL.
- **Proxy:** open Windows Settings → Network & internet → Proxy. Disable an unknown manual proxy, but preserve settings required by your workplace or school.
- **Notifications:** remove unfamiliar sites from the browser's allowed notification list.
- **Managed policies:** on a personal PC, unexpected browser policies can indicate remaining software. Do not delete policy or registry entries blindly; scan the system and identify their source.
- **Synchronization:** a bad extension may return from another device. Remove it from the synced browser account before enabling sync again.

06 After cleanup

Test the homepage, new tab, and several searches after another restart. If you entered a password on a redirected or fake page, change it from a clean device, sign out other sessions, and enable multi-factor authentication. Check email and financial accounts for unfamiliar activity.

07 If redirects continue

Do not repeatedly reinstall the browser while an unwanted Windows component is still active. Run another full scan and contact Gridinsoft Support with the redirect address, affected browser, screenshot, scan time, and relevant logs. Do not include account passwords or payment details.

08 How to prevent another browser hijacker

- Download applications and browser extensions only from their official publisher or store.
- Review every installer screen and decline bundled offers.
- Keep Windows and browsers updated.

- Reject unexpected “Allow notifications,” fake update, and codec prompts.
- Avoid cracked software and third-party “activation” tools.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com