C

Conduit Search Browser Hijacker: Removal for Chrome, Edge, and Firefox

Conduit Search is associated with browser-hijacking toolbars and unwanted settings changes. Learn the symptoms, complete removal steps, and how to stop redirects returning.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 Signs of a Conduit browser hijacker
02 How Conduit gets installed
03 Remove Conduit from the operating system first
04 Remove Conduit from Chrome
05 Remove Conduit from Microsoft Edge
06 Remove Conduit from Firefox
07 If Conduit keeps coming back
08 After removal
09 Frequently asked questions

Conduit Search refers to a family of browser toolbars, search pages, and settings-changing software historically associated with Conduit. Security products may classify related components as a potentially unwanted application or browser hijacker. It can replace the homepage, new-tab page, or default search engine and may return after one setting is corrected.

Conduit is not a required part of Chrome, Edge, Firefox, Windows, or macOS. Remove it when you did not intentionally install it or cannot control the affected browser settings.

01 Signs of a Conduit browser hijacker

- New tabs or the homepage open a Conduit-branded or unfamiliar search page.
- Address-bar searches pass through an unexpected site before reaching another search engine.
- An unknown toolbar or extension appears in one or more browsers.
- The default search engine, startup pages, or notification permissions change again after correction.
- The browser reports "Managed by your organization" on a personal device.
- Search results contain unusually aggressive ads or redirects.
- The same unwanted settings reappear after browser synchronization.

02 How Conduit gets installed

Older Conduit components were commonly bundled with free software and toolbar installers. Similar browser hijackers still arrive through:

- installers that include preselected optional offers;
- fake updates, download buttons, codecs, converters, and cracked software;
- extensions installed from unofficial sources;
- notification prompts that imitate a download or verification step;

- browser policies or profiles added by unwanted software.

03 Remove Conduit from the operating system first

1. Disconnect browser synchronization temporarily if it immediately restores the unwanted extension or settings.
2. Open the installed-applications list and sort by installation date.
3. Uninstall unfamiliar toolbars, search protectors, download managers, and applications installed with the first redirect.
4. Review startup applications and scheduled tasks for the same publisher or installation path.
5. Run an updated full security scan and quarantine related unwanted software.
6. Restart normally before repairing browser settings.

Do not delete random registry keys or system files based only on the word "Conduit." Record the publisher and path and create a backup before changing unfamiliar system configuration.

04 Remove Conduit from Chrome

1. Open **Extensions → Manage extensions** and remove unknown search, toolbar, coupon, converter, or new-tab extensions.
2. Open **Settings → Search engine** and select the intended provider. Remove unwanted entries from site search where possible.
3. Check **On startup** and remove unfamiliar pages.
4. Check **Privacy and security → Site settings → Notifications** and revoke suspicious permissions.
5. If redirects continue, use **Reset settings → Restore settings to their original defaults**.

05 Remove Conduit from Microsoft Edge

1. Open **Extensions → Manage extensions** and remove unwanted items.
2. Open **Settings → Privacy, search, and services → Address bar and search** and restore the desired search engine.
3. Check **Start, home, and new tabs** for unfamiliar pages.
4. Review notification permissions under cookies and site permissions.
5. Use **Reset settings** if the configuration still returns.

06 Remove Conduit from Firefox

1. Open **Add-ons and themes → Extensions** and remove unknown add-ons.
2. Open **Settings → Search** and restore the default search engine.
3. Check **Home** for altered homepage and new-window settings.
4. Review notification permissions under **Privacy & Security**.
5. If necessary, use Firefox's troubleshooting-information page to **Refresh Firefox**.

07 If Conduit keeps coming back

Persistence source	What to check
Browser sync	Extensions and settings on every synchronized device; remove the unwanted item before turning sync back on.
Installed software	Applications, startup entries, services, and scheduled tasks that rewrite browser preferences.
Managed browser policy	Policy pages in the browser and device-management profiles. On a work device, contact the administrator rather than deleting policy.

Persistence source	What to check
Shortcut modification	The browser shortcut target should end with the legitimate browser executable, not an added URL or script.
Proxy or DNS change	Unexpected proxy, DNS, VPN, or hosts-file configuration.

If every browser redirects in the same way, investigate system-level software, proxy, DNS, and network configuration rather than repeatedly reinstalling each browser.

08 After removal

- Update the browser and operating system.
- Clear unwanted site permissions and cookies for the redirecting domains.
- Change passwords only if you entered them on a suspicious page or evidence indicates credential theft; use a clean device when compromise is possible.
- Re-enable synchronization carefully and confirm the unwanted extension does not return.
- Install future software with optional offers disabled and verify the publisher.

09 Frequently asked questions

Is Conduit Search a virus?

It is more accurately described as a browser hijacker or potentially unwanted application than a self-replicating computer virus. Related installers can still expose users to unsafe redirects and additional software.

Will resetting the browser remove Conduit?

A reset can repair browser settings, but it may not remove the installed application, policy, scheduled task, or synchronized extension that changed them. Check the operating system and all synced devices.

Why does the redirect affect more than one browser?

The cause may be a system-level application, proxy, DNS setting, managed policy, or software installed into several browsers. Correcting only one browser leaves the shared cause active.

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