

[Using protection](#)

Use Web Protection with VPN and Private DNS settings

Resolve conflicts with another VPN, a custom Android Private DNS provider, or a browser that uses its own encrypted DNS.

PUBLISHER

Gridinsoft Support

UPDATED

Oct 7, 2026

READ TIME

2 min

CONTENTS

In this guide

01 Another VPN is already active**02** A custom Private DNS provider is selected**03** A browser uses its own Secure DNS

Web Protection uses Android's VPN facility to handle DNS requests. It is a DNS-only connection: normal web traffic is not routed through a location-changing VPN.

01 Another VPN is already active

Android permits one active VPN per user profile. A VPN app, firewall or ad blocker using that facility can conflict with Web Protection. Connecting another VPN may disconnect Gridinsoft, and starting Gridinsoft may require switching away from the other connection.

1. Check Android's VPN settings and identify the currently active connection.
2. If you want to use Web Protection, disconnect the other VPN through its app or Android settings.
3. Return to Web Protection, start it, and verify **Protection is ON**.

On a work-managed phone, ask your administrator before changing a required VPN. If you need that VPN to remain active, these two connections cannot be used together in the same profile.

02 A custom Private DNS provider is selected

A manually specified Android Private DNS hostname prevents Web Protection from starting. Search Android Settings for **Private DNS**. If you choose to use Gridinsoft, change the custom provider setting to **Automatic** or **Off**, then retry protection. Android menus differ between manufacturers. Gridinsoft's own DNS connection still uses HTTPS.

03 A browser uses its own Secure DNS

Some browsers and apps send DNS directly to a provider chosen in their own settings. Those requests can bypass the system DNS route. Check the affected browser's **Secure DNS** or DNS provider setting; turn off its custom DNS override if you want that browser to use the system route.

Reload or restart the affected app after changing settings. Previously cached addresses and existing connections can remain usable for a while. Do not visit a known dangerous site to test coverage.

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](https://support.gridinsoft.com)