

AdGuard Home

AdGuard Home is self-hosted network-wide DNS filtering software that blocks ads, trackers, and certain unwanted domains for every device using your network. It works as a DNS server (often on your router, NAS, VPS, or a small board like a Raspberry Pi) and gives you a web UI to manage filters, logs, and parental controls.

Key facts

- **Type:** Self-hosted DNS sinkhole / DNS filtering software
- **License:** Free and open source (GPL)
- **Scope:** Network-wide (covers all devices using its DNS)
- **Primary functions:** Ad & tracker blocking, parental control, basic security
- **Deployment targets:** Router, Raspberry Pi, server/VPS, many Linux-based systems
- **Website:** [AdGuard](https://adguard.com)

How it works

AdGuard Home runs as a DNS resolver on your network. When a device asks for a domain (like `ads.example.com`), AdGuard Home checks the request against its filter lists. If the domain is on a blocklist, it returns a “sinkhole” or invalid address, so the connection to that ad or tracker never happens. If not blocked, it forwards the query to upstream DNS servers you choose (e.g., AdGuard DNS, Cloudflare, etc.).

Features and capabilities

- **Ad/tracker blocking:** Uses filter lists similar to browser ad-blockers (EasyList, AdGuard filters, etc.).
- **Parental control & safe search:** Can block adult content and enforce safe search on major search engines.
- **Malware & phishing protection:** Optional lists to block malicious domains.
- **Per-client rules:** Different devices (kids' tablets, smart TVs, work laptop) can have different policies.

- **DNS privacy:** Supports encrypted upstream DNS (DoH/DoT/DoQ via compatible resolvers), reducing ISP snooping.

Typical deployment and use cases

Common setups include running AdGuard Home on a home router, on a Raspberry Pi, or in a container on a home server. You then point your router's DNS to it so every device (phones, laptops, IoT gadgets, TVs) benefits without installing extra apps. It's often compared with Pi-hole; both are DNS sinkholes with web dashboards, but AdGuard Home leans into a more polished UI and integrated parental-control and DNS-privacy options.

Limitations

Because filtering happens at DNS level, it can't block everything: same-domain ads (e.g., `example.com/ads.js`), in-app native ads, or some CDN-heavy sites may still show ads. It also doesn't replace a full firewall or IDS; it's best seen as a strong first layer of network-wide content and tracking control rather than a complete security solution.

Revision #1

Created 2026-02-25 12:59:32 UTC by Carsten

Updated 2026-02-25 13:00:30 UTC by Carsten