AFRIDYNE SYSTEMS · TECHNICAL GUIDE

Pi-hole: Network-Wide Ad Blocking

Block adverts and trackers for every device on your network from one small server.

Updated November 2026 | Debian, Ubuntu, Raspberry Pi OS | Pi-hole v6 | about 15 minutes

Pi-hole is a small DNS server that blocks adverts, trackers and known bad domains for every device on your network, including phones, smart TVs and things that cannot run an ad blocker. It runs happily on a Raspberry Pi, a mini PC or a virtual machine.

> **What it does not do:** Pi-hole blocks by domain name, so it cannot remove adverts served from the same domain as the content (YouTube is the usual example). It is a useful extra layer, not a replacement for antivirus or a firewall.

1. Give it a fixed address

Devices will be told to ask the Pi-hole for DNS, so its address must never change. In your router, create a DHCP reservation for the Pi-hole machine (or set a static address on the machine itself). Note the address; we use `192.168.1.5` below.

2. Install

On the machine that will run Pi-hole:

terminal

```
curl -sSL https://install.pi-hole.net | bash
```

The installer is a guided text screen. Accept the defaults unless you have a reason not to, choose an upstream DNS provider (Cloudflare or Quad9 are fine), and keep the web interface and blocklists enabled. When it finishes, set a password for the dashboard:

terminal

```
sudo pihole setpassword
```

The dashboard is at `http://192.168.1.5/admin` (use your own address).

3. Point your network at it

The best method is in the router: set the DHCP server's DNS to the Pi-hole's address, then reconnect your devices (or wait for their leases to renew).

> **Use the Pi-hole as the only DNS server.** If you add a second public DNS server such as 8.8.8.8, many devices will use it and skip the blocking. The trade-off is that if the Pi-hole is switched off, the internet appears to stop working for everything that relies on it.

If your router will not let you change DNS, set it on individual devices instead, in their network settings.

4. Check it works

Open the dashboard. The query count should climb as devices browse. Then check the service:

terminal

```
pihole status
```

5. Keep it healthy

terminal

```
pihole -g          # refresh the blocklists
pihole -up         # update Pi-hole itself
```

Also keep the operating system updated as normal, with `sudo apt update && sudo apt upgrade`.

When a site or app breaks

Occasionally a blocklist catches a domain a site genuinely needs, such as a checkout page or a banking login. In the dashboard open the **Query Log**, find the blocked domain for that moment, and add it to the allow list under **Domains**. The site works again straight away.

A privacy note

The Pi-hole keeps a log of which device asked for which domain. That is useful for troubleshooting, but in a home with several people or an office, make sure everyone knows it is there. The dashboard lets you shorten how long queries are kept, or hide them completely.