

Configure Adlists

To enhance Pi-hole's ability to block unwanted ads, trackers, and malicious content, you can add custom adlists. Below is a step-by-step guide to add adlists in Pi-hole, followed by a comprehensive list of popular adlists.

Step 1: Access Pi-hole's Web Interface

1. Open a web browser and navigate to your Pi-hole admin page. If you set up Pi-hole to run at a specific IP and port (e.g., 888), you can visit the following URL:

```
http://my-server-ip:888/admin/groups-adlists.php
```

2. Log in using your Pi-hole admin password.

Step 2: Navigate to the Adlists Section

1. Once logged in, go to the **Group Management** tab.
2. Select the **Adlists** option from the sidebar.

Step 3: Add New Adlists

1. In the **Adlists** page, you'll see an option to **Add a new adlist**.
2. Enter the URL of the adlist you wish to add in the "Address" field.
3. Add a comment or label for future reference (e.g., Default).
4. Click on **Add**.

Adlists with **7.303.876 Domains** on the Adlists:

```
https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts https://big.oisd.nl
https://nsfw.oisd.nlhttps://raw.githubusercontent.com/PolishFiltersTeam/KADhosts/master/KADhosts.txt
https://raw.githubusercontent.com/FadeMind/hosts.extras/master/add.Spam/hosts
https://v.firebog.net/hosts/static/w3kbl.txt https://raw.githubusercontent.com/matomo-org/referrer-spam-
blacklist/master/spammers.txt https://someonewhocares.org/hosts/zero/hosts
https://raw.githubusercontent.com/VeleSila/yhosts/master/hosts https://winhelp2002.mvps.org/hosts.txt
https://v.firebog.net/hosts/neohostsbasic.txt https://raw.githubusercontent.com/RooneyMcNibNug/pihole-
```

stuff/master/SNAFU.txt <https://paulgb.github.io/BarbBlock/blacklists/hosts-file.txt> <https://adaway.org/hosts.txt>
<https://v.firebog.net/hosts/AdguardDNS.txt> <https://v.firebog.net/hosts/Admiral.txt>
<https://raw.githubusercontent.com/anudeepND/blacklist/master/adservers.txt>
<https://v.firebog.net/hosts/Easylist.txt>
<https://pgl.yoyo.org/adservers/serverlist.php?hostformat=hosts&showintro=0&mimetype=plaintext>
<https://raw.githubusercontent.com/FadeMind/hosts.extras/master/UncheckyAds/hosts>
<https://raw.githubusercontent.com/bigdargon/hostsVN/master/hosts>
<https://raw.githubusercontent.com/jdlingyu/ad-wars/master/hosts> <https://v.firebog.net/hosts/Easyprivacy.txt>
<https://v.firebog.net/hosts/Prigent-Ads.txt>
<https://raw.githubusercontent.com/FadeMind/hosts.extras/master/add.2o7Net/hosts>
<https://raw.githubusercontent.com/crazy-max/WindowsSpyBlocker/master/data/hosts/spy.txt>
<https://hostfiles.frogeye.fr/firstparty-trackers-hosts.txt> <https://www.github.developerdan.com/hosts/lists/ads-and-tracking-extended.txt> <https://raw.githubusercontent.com/Perflyst/PiHoleBlocklist/master/android-tracking.txt>
<https://raw.githubusercontent.com/Perflyst/PiHoleBlocklist/master/SmartTV.txt>
<https://raw.githubusercontent.com/Perflyst/PiHoleBlocklist/master/AmazonFireTV.txt>
<https://gitlab.com/quidsup/notrack-blocklists/raw/master/notrack-blocklist.txt>
<https://raw.githubusercontent.com/DandelionSprout/adfilt/master/Alternate%20versions%20Anti-Malware%20List/AntiMalwareHosts.txt> <https://osint.digitalside.it/Threat-Intel/lists/latestdomains.txt>
<https://v.firebog.net/hosts/Prigent-Crypto.txt>
<https://raw.githubusercontent.com/FadeMind/hosts.extras/master/add.Risk/hosts>
https://bitbucket.org/ethanr/dns-blacklists/raw/8575c9f96e5b4a1308f2f12394abd86d0927a4a0/bad_lists/Mandiant_APT1_Report_Appendix_D.txt
https://phishing.army/download/phishing_army_blocklist_extended.txt <https://gitlab.com/quidsup/notrack-blocklists/raw/master/notrack-malware.txt> <https://v.firebog.net/hosts/RPiList-Malware.txt>
<https://v.firebog.net/hosts/RPiList-Phishing.txt> <https://raw.githubusercontent.com/Spam404/lists/master/main-blacklist.txt> <https://raw.githubusercontent.com/AssoEchap/stalkerware-indicators/master/generated/hosts>
<https://urlhaus.abuse.ch/downloads/hostfile/> <https://malware-filter.gitlab.io/malware-filter/phishing-filter-hosts.txt>
<https://v.firebog.net/hosts/Prigent-Malware.txt> https://zerodot1.gitlab.io/CoinBlockerLists/hosts_browser
https://raw.githubusercontent.com/chadmayfield/my-pihole-blocklists/master/lists/pi_blocklist_porn_top1m.list
<https://v.firebog.net/hosts/Prigent-Adult.txt>
<https://raw.githubusercontent.com/anudeepND/blacklist/master/facebook.txt>
<https://raw.githubusercontent.com/xxcriticxx/.pl-host-file/master/hosts.txt>
https://raw.githubusercontent.com/Gooler/1024_hosts/master/hosts <https://tgc.cloud/downloads/hosts.txt>

Conclusion

By adding these adlists, you can extend Pi-hole's capabilities to block a wider variety of ads, trackers, and malicious content. This can significantly improve browsing speed, privacy, and security across your network. Make sure to regularly update Pi-hole's Gravity to keep the adlists up to date.

Revision #4

Created 8 September 2024 17:55:26 by aeoneros

Updated 10 October 2024 23:16:00 by aeoneros