



Setup Guide AdGuard Pi-Hole Technitium DNS

Public

Introduction

In today's world, keeping your network secure is super important. DNS blackholes are great tools for protecting your network. They can filter DNS using external dynamic lists of threat indicators, known as Indicators of Compromise (IoCs).

Q-Feeds provides dynamic, up-to-date lists of these IoCs, designed specifically for use with security controls like DNS blackholes. By integrating Q-Feeds into your DNS blackhole installation, you can improve your network's protection against new and emerging threats. This means your DNS server can automatically block harmful traffic and stay updated with the latest threat information.

This manual will show you how to set up and use Q-Feeds with your DNS blackhole setup, so you can get the best security possible. You'll learn how to configure the DNS blackhole, import Q-Feeds, and ensure everything is working correctly. With these steps, you'll be able to enhance your network's defenses and keep your data safe from cyber threats.

Table of Contents

Introduction	1
<i>Using Q-Feeds for Enhanced Network Security.....</i>	3
Available Lists of Indicators	3
<i>Setup Q-Feeds on AdGuard</i>	4
<i>Setup Q-Feeds on Pi-Hole</i>	5
<i>Setup Q-Feeds on Technitium DNS.....</i>	7

Using Q-Feeds for Enhanced Network Security

Q-Feeds provides dynamic lists of Indicators of Compromise (IoCs) to enhance your network security controls. These lists, based on Q-Feeds Threat Intelligence Data Feeds, are regularly updated with various types of IoCs such as IP addresses and domains. By using these lists, you can monitor and block user access to dangerous network resources effectively.

Available Lists of Indicators

Q-Feeds offers the following types of indicators:

Name	Type	Description	URI
Malware Domains	Domain	List of malicious domains	https://api.qfeeds.com/api?feed_type=malware_domains&api_token=XXXXXX&limit=XXXXXX

To optimize system performance and prevent unnecessary strain on our infrastructure, please schedule updates at the standard interval of 20 minutes. Setting the interval to less than 20 minutes is not beneficial.

Accessing the lists—including direct downloads into your network security solutions—requires an API token from Q-Feeds. You can request this token through your account manager or by registering at <https://tip.qfeeds.com/>

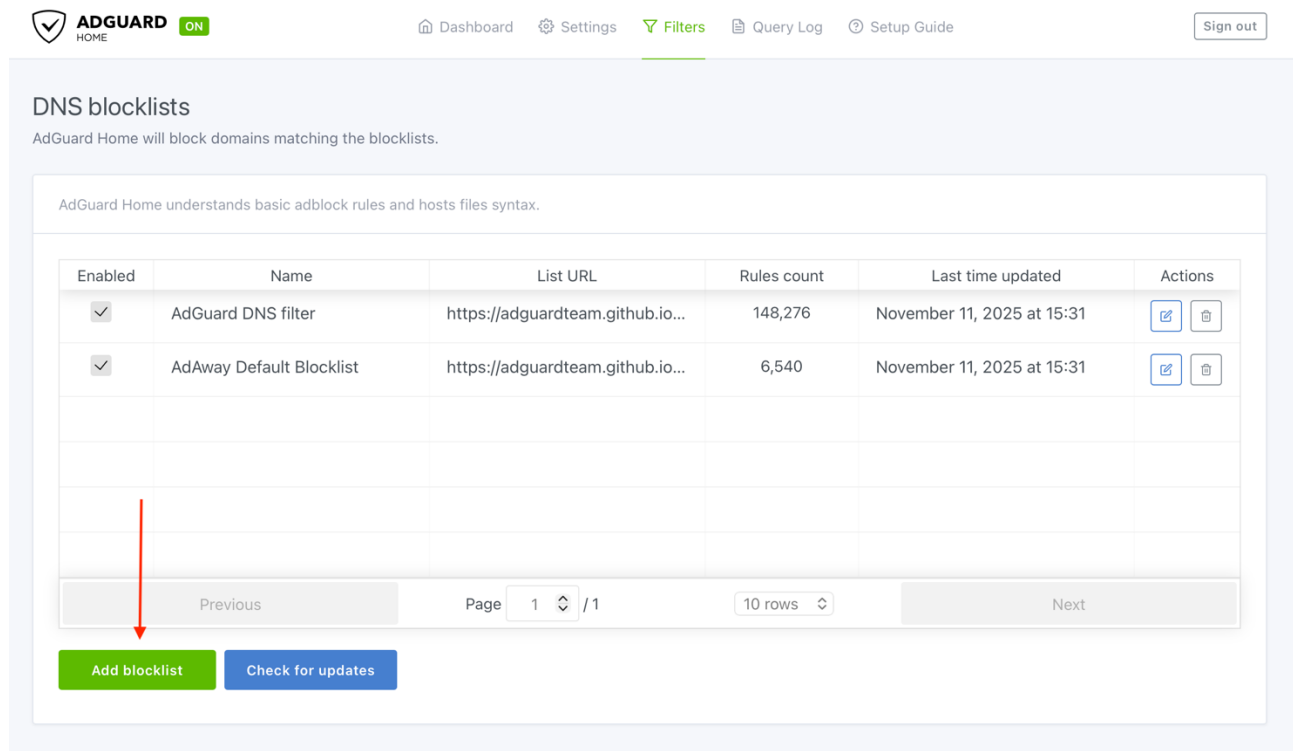
We have multiple types of keys available from Free (community edition) to Plus and Premium. You can find more information on <https://qfeeds.com/licenses>

To test downloading the lists, you can use the cURL utility. Here is the syntax for Linux systems:

```
curl -v -u api_token:XXXXX https://api.qfeeds.com/api?feed_type=malware_domains&limit=XXXXX
```

Setup Q-Feeds on AdGuard

In your AdGuard management console head to **Filter → DNS Blocklists**:



ADGUARD HOME ON

Dashboard Settings **Filters** Query Log Setup Guide Sign out

DNS blocklists

AdGuard Home will block domains matching the blocklists.

AdGuard Home understands basic adblock rules and hosts files syntax.

Enabled	Name	List URL	Rules count	Last time updated	Actions
☒	AdGuard DNS filter	https://adguardteam.github.io...	148,276	November 11, 2025 at 15:31	Edit Delete
☒	AdAway Default Blocklist	https://adguardteam.github.io...	6,540	November 11, 2025 at 15:31	Edit Delete

Previous Page 1 / 1 10 rows Next

Add blocklist Check for updates

Click **Add Blocklist** and select **Add a custom list**:

New blocklist
×

Choose from the list
Add a custom list

Cancel

Give your list a recognisable name and copy the link as described on page 2 of this manual. Don't forget to **replace the API token with your token** which you can obtain on our Threat Intelligence Console (<https://tip.qfeeds.com>).

New blocklist
×

Q-Feeds Domain List

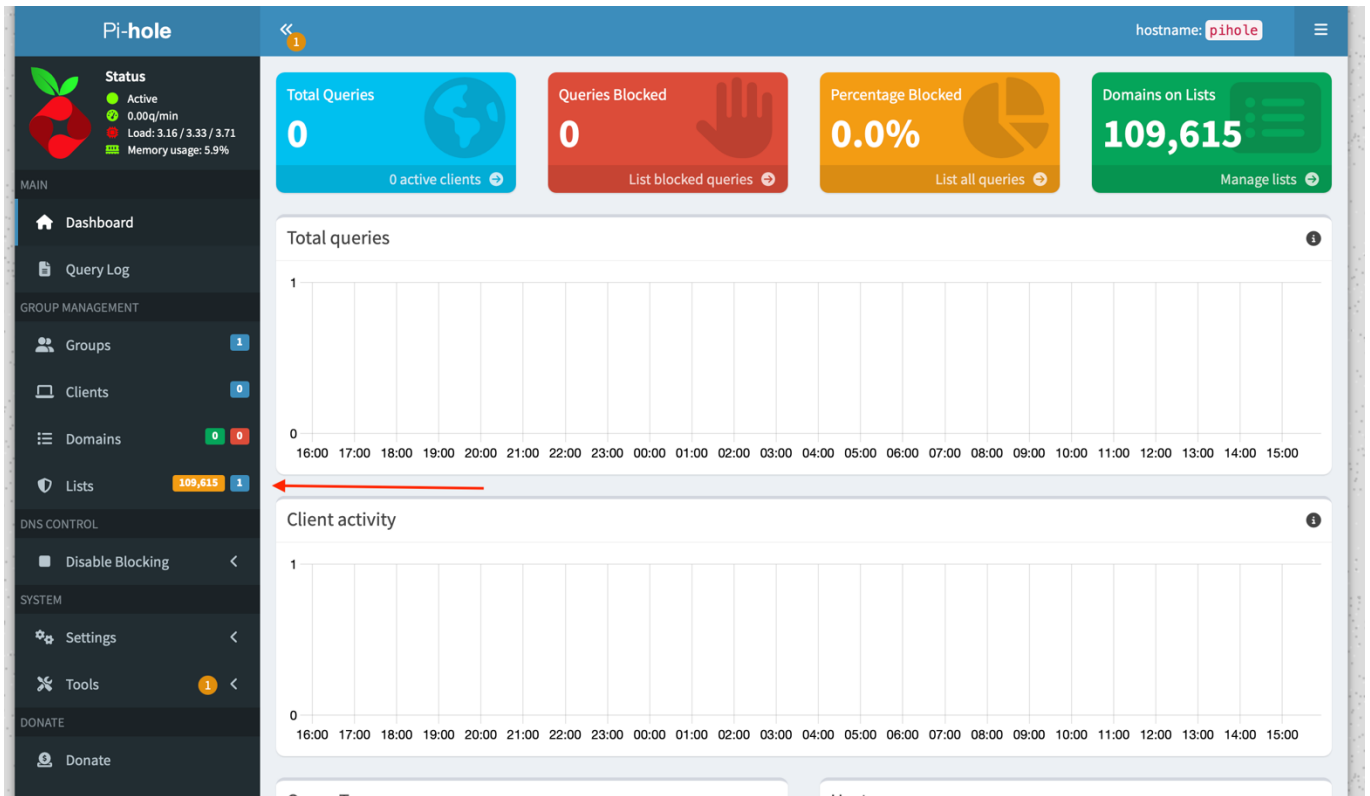
https://api.qfeeds.com/api.php?feed_type=malware_domains&a

Enter a valid URL to the blocklist.

Cancel
Save

Setup Q-Feeds on Pi-Hole

Head to your Pi-Hole instance and click on **Lists**



On the next screen fill in the URL as shown on page 2 of this manual and provide a recognizable comment. **Don't forget to fill in your api_token in the url!** Then click **Add blocklist**:

Subscribed lists group management

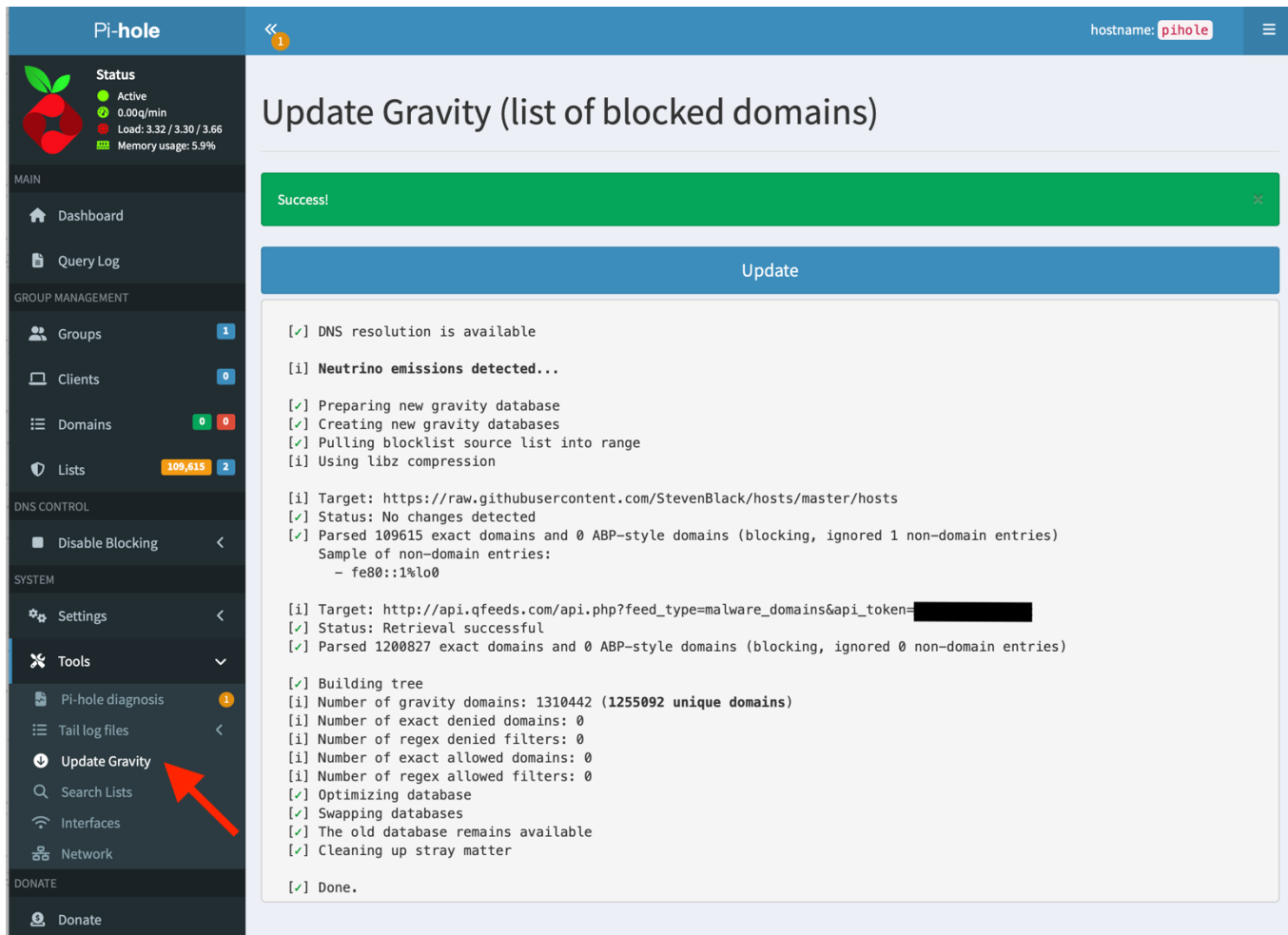
Add a new subscribed list

Address:	Comment:	Group assignment:
<input "="" type="text" value="http://api.qfeeds.com/api.php?feed_type=malware_domains&api_token="/>	Q-Feeds Blocklist	Default

Hints:

1. Please run `pihole -g` or update your gravity list [online](#) after modifying your lists.
2. Multiple lists can be added by separating each *unique* URL with a space or comma
3. Click on the icon in the first column to get additional information about your lists. The icons correspond to the health of the list.

To force update the blocklist you need to go to **Tools → Update Gravity** and click on **Update**:



Pi-hole hostname: **pihole**

Status

- Active
- 0.00q/min
- Load: 3.32 / 3.30 / 3.66
- Memory usage: 5.9%

MAIN

- Dashboard
- Query Log

GROUP MANAGEMENT

- Groups 1
- Clients 0
- Domains 0 0
- Lists 109,615 2

DNS CONTROL

- Disable Blocking <

SYSTEM

- Settings <
- Tools >
- Pi-hole diagnosis 1
- Tail log files <
- Update Gravity**
- Search Lists
- Interfaces
- Network

DONATE

- Donate

Update Gravity (list of blocked domains)

Success!

Update

```
[✓] DNS resolution is available
[i] Neutrino emissions detected...
[✓] Preparing new gravity database
[✓] Creating new gravity databases
[✓] Pulling blocklist source list into range
[i] Using libz compression

[i] Target: https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts
[✓] Status: No changes detected
[✓] Parsed 109615 exact domains and 0 ABP-style domains (blocking, ignored 1 non-domain entries)
Sample of non-domain entries:
- fe80::1%lo0

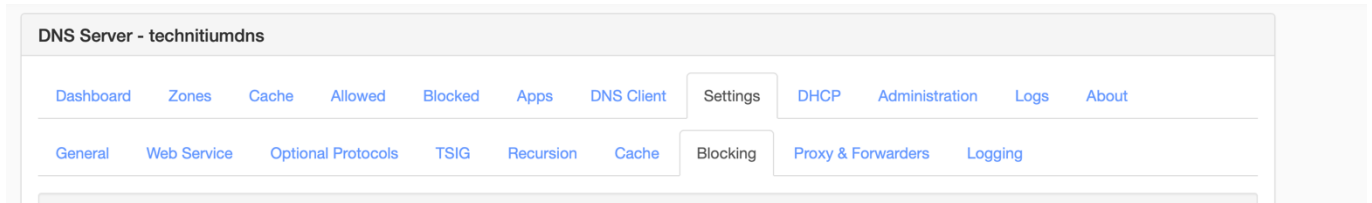
[i] Target: http://api.qfeeds.com/api.php?feed_type=malware_domains&api_token=
[✓] Status: Retrieval successful
[✓] Parsed 1200827 exact domains and 0 ABP-style domains (blocking, ignored 0 non-domain entries)

[✓] Building tree
[i] Number of gravity domains: 1310442 (1255092 unique domains)
[i] Number of exact denied domains: 0
[i] Number of regex denied filters: 0
[i] Number of exact allowed domains: 0
[i] Number of regex allowed filters: 0
[✓] Optimizing database
[✓] Swapping databases
[✓] The old database remains available
[✓] Cleaning up stray matter

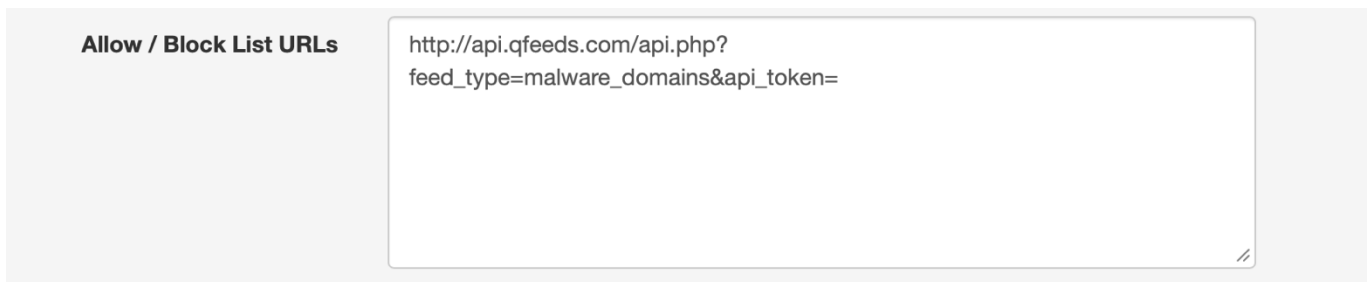
[✓] Done.
```

Setup Q-Feeds on Technitium DNS

Head to your Technitium DNS instance and go to **Settings → Blocking**



Scroll down to **Allow / Block List URLs** and paste in the link as described on page 2 of this manual. Don't forget to fill in your `api_token`.



Depending on your license (<https://qfeeds.com/licenses/>) you can set the update interval to a shorter interval. Click **Update Now** to force pull in our DNS blocklist.

