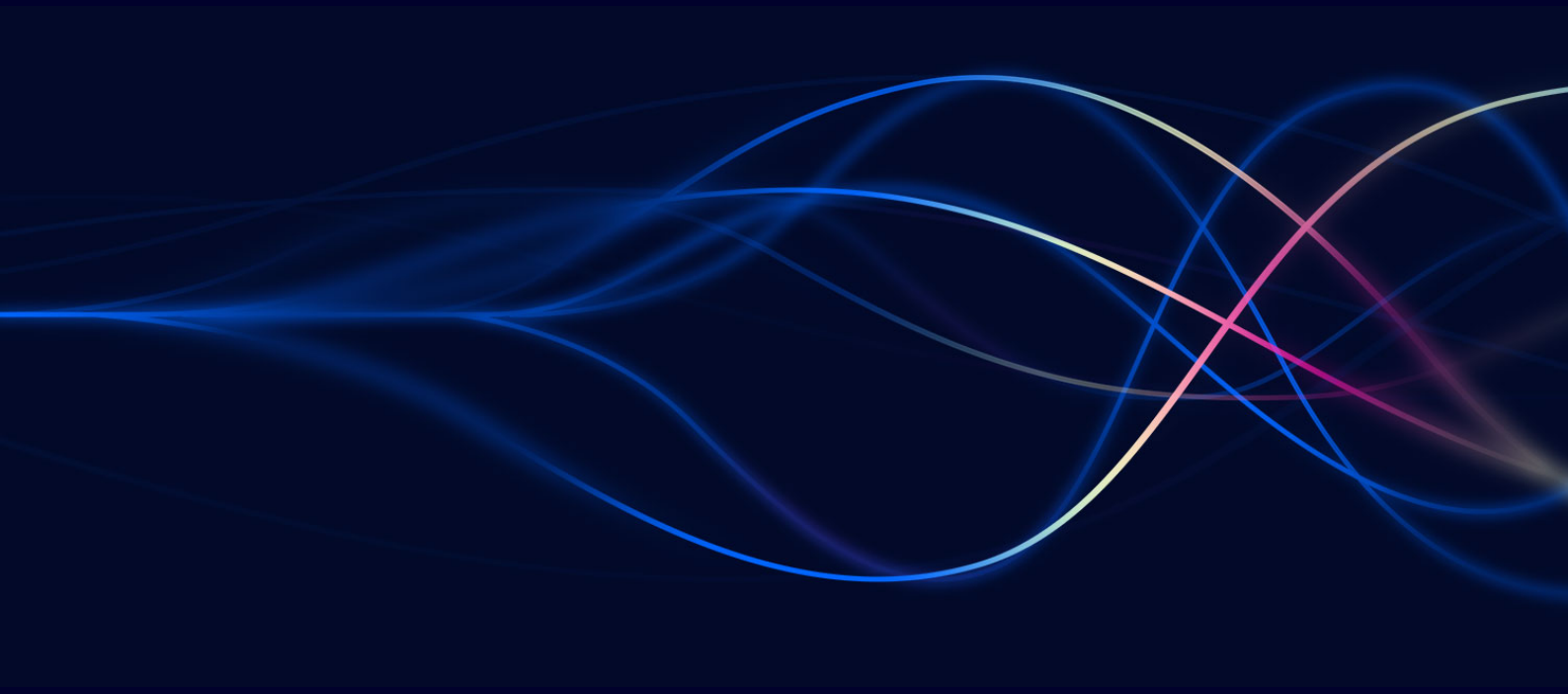
Q-FEEDS

Setup Guide
AdGuard Pi-Hole Technitium DNS

Public



Version 1.0 - 11 November 2025

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.

Q-FEEDS

Table of Contents

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/**

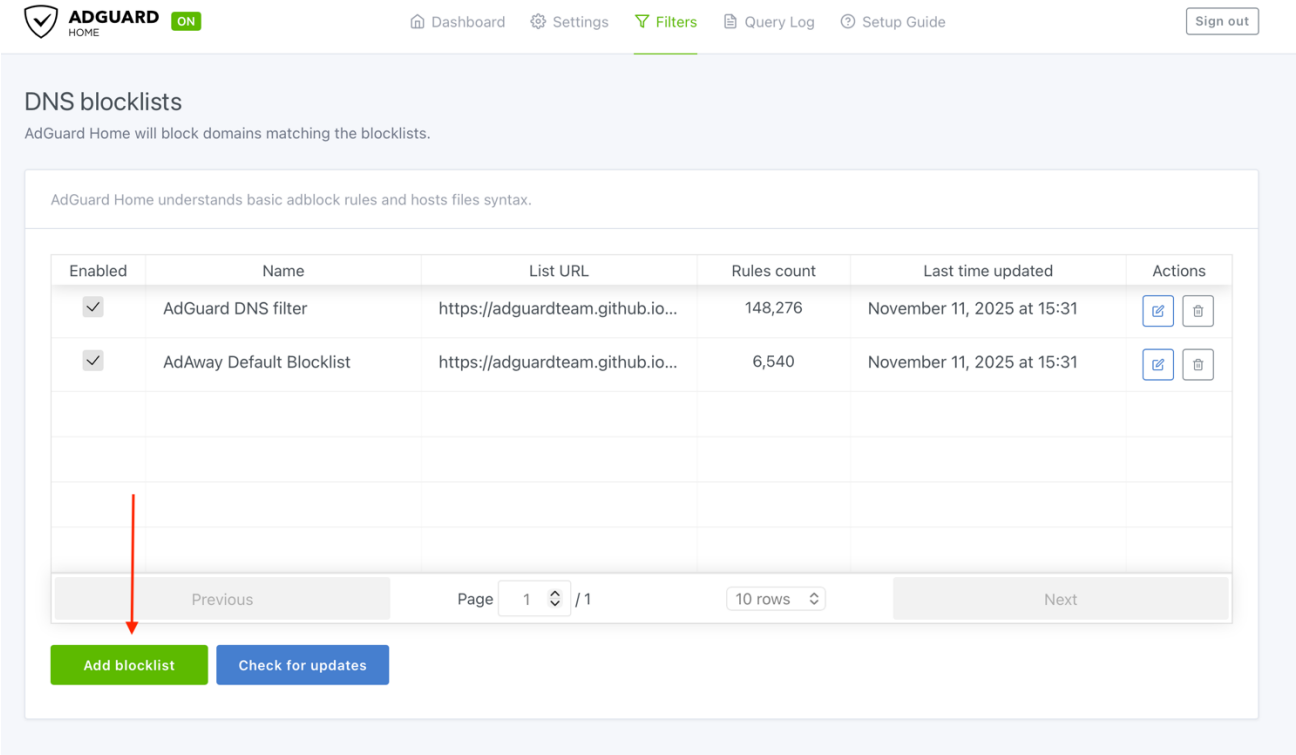
We have multiple types of keys available from Free (community edition) to Plus and Premium. You can find more information on **https://qfeeds.com/licenses**

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

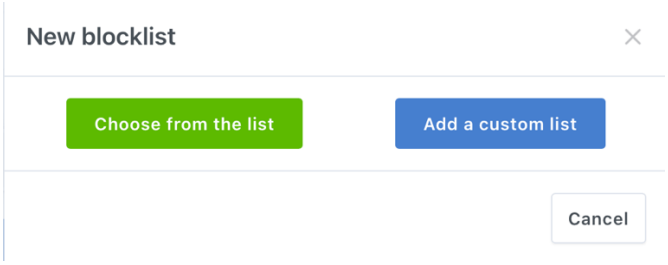
curl -v -u api_token:XXXXX https://api.qfeeds.com/api?feed_type=malware_domains&limit=XXXXX

Setup Q-Feeds on AdGuard

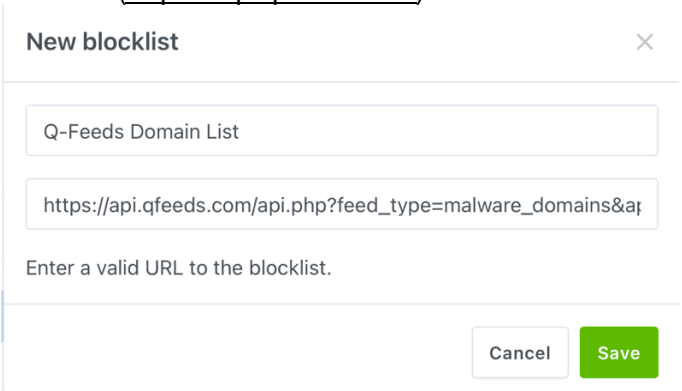
In your AdGuard management console head to **Filter → DNS Blocklists:**



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

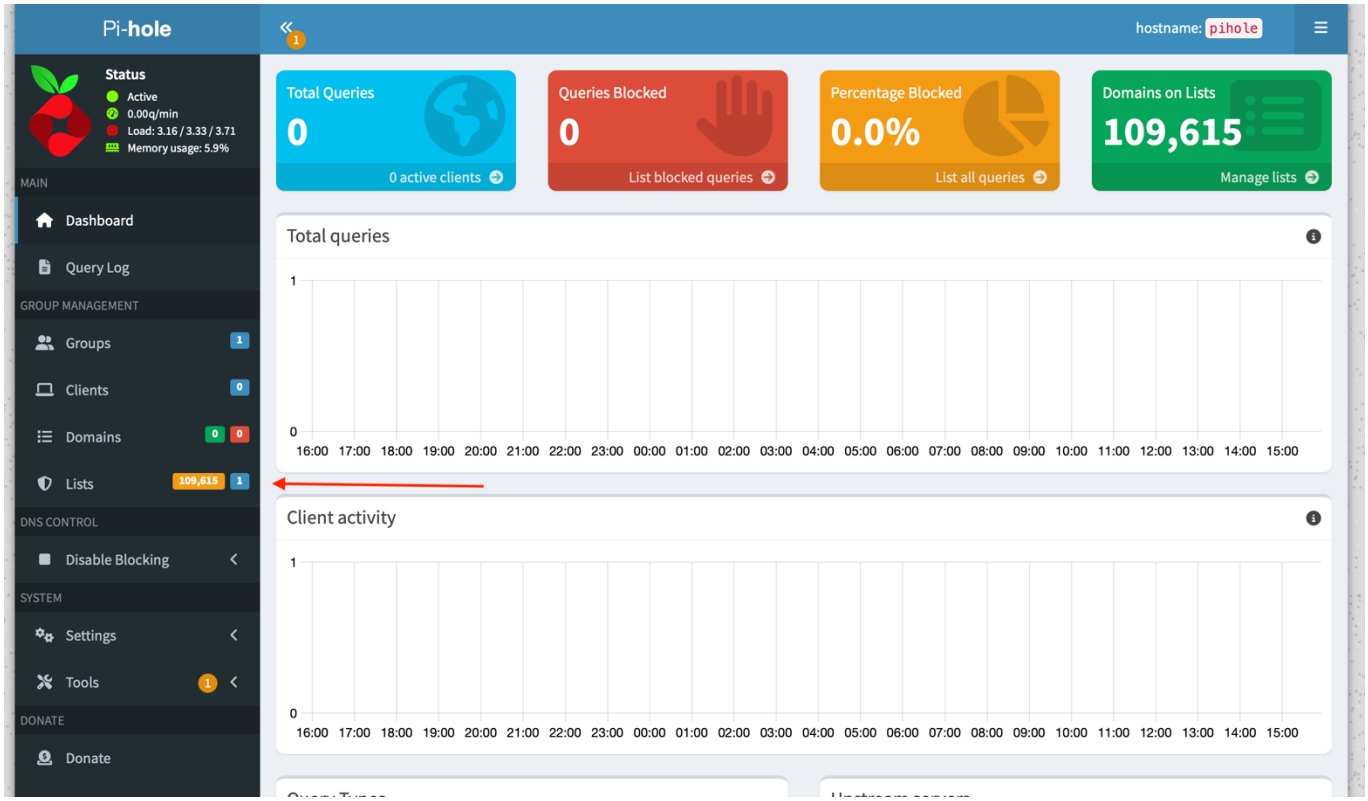


Give your list a recognaisable name and copy the link as described on page 2 of this manual. Don't forget to **replace the API token with your token** which you can obtain on our Threat Intelligence Console (https://tip.qfeeds.com).

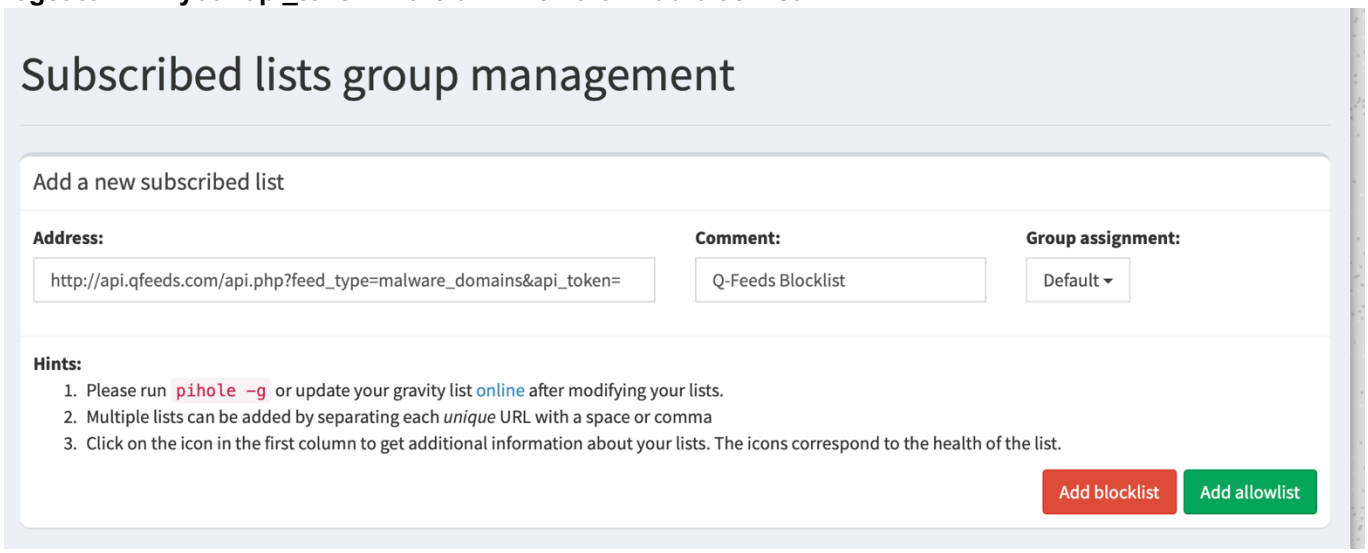


Setup Q-Feeds on Pi-Hole

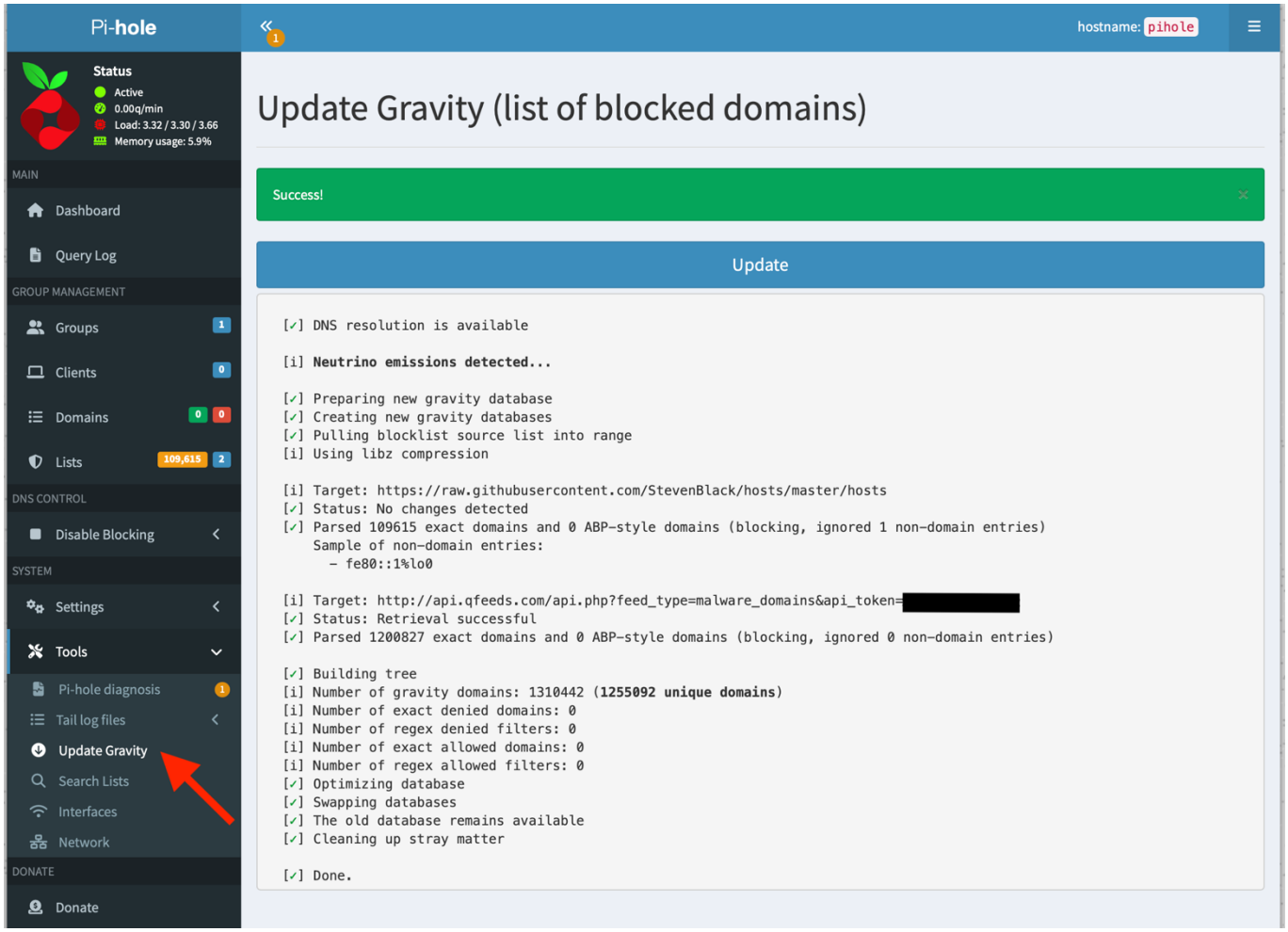
Head to your Pi-Hole instance and click on **Lists**



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

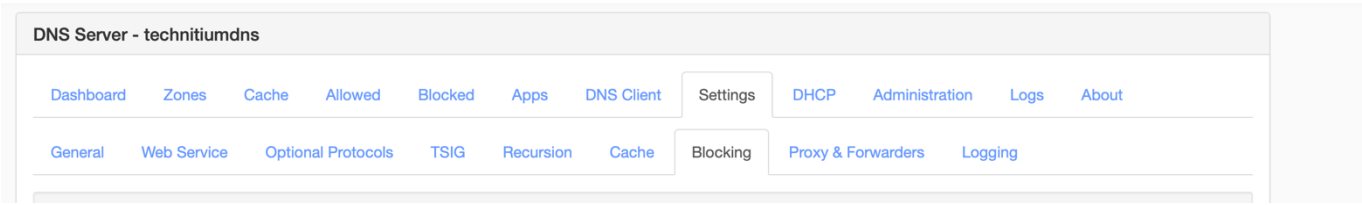


To force upate the blocklist you need to go to **Tools → Update Gravity** and click on **Update:**

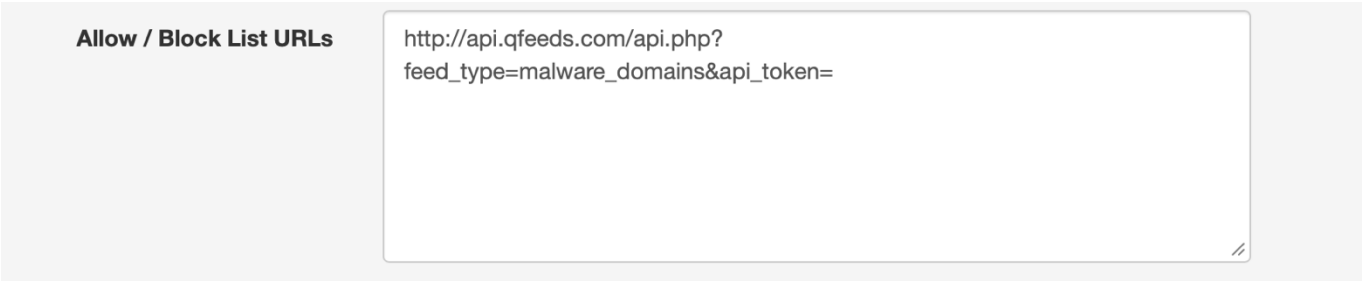


Setup Q-Feeds on Technitium DNS

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



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



Depending on you 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.