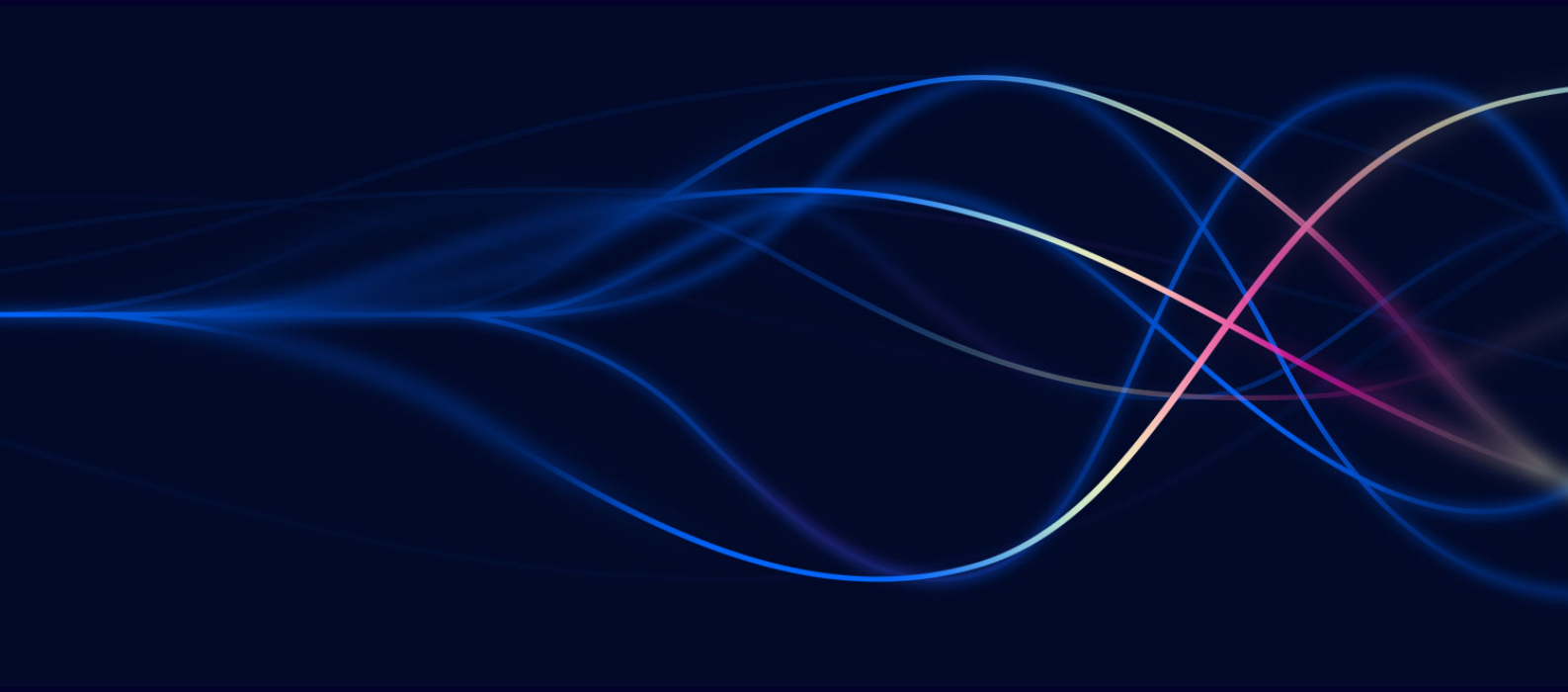
Q-FEEDS

Setup Guide
Sophos Xstream NGFW

Public



Version 1.1 - 21 November 2024

Introduction

In today's world, keeping your network secure is super important. Next Generation Firewalls (NGFWs) are essential tools for protecting your network. They can filter DNS and web traffic 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 NGFWs. By integrating Q-Feeds into your Sophos firewall, you can improve your network's protection against new and emerging threats. This means your firewall 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 Sophos firewall, so you can get the best security possible. You'll learn how to configure the firewall, 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.

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 IP	IP address	List of dangerous IP addresses	https://api.qfeeds.com/api?feed_type=malware_ip&api_token=XXXXXX&limit= XXXXXX
Malware Domains	Domain	List of malicious domains	https://api.qfeeds.com/api?feed_type=malware_domains&api_token=XXXXXX&limit= XXXXXX
Phishing URLs	URL	List of phishing URLs	https://api.qfeeds.com/api?feed_type=phishing_urls&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 visiting our website at https://qfeeds.com/start-trial-license/.

With the trial token, you will receive 30 days of free and full access to all our indicators of compromise. If you need assistance, please contact your account manager or email us at sales@qfeeds.com.

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=XXXX&limit=XXXXX
```

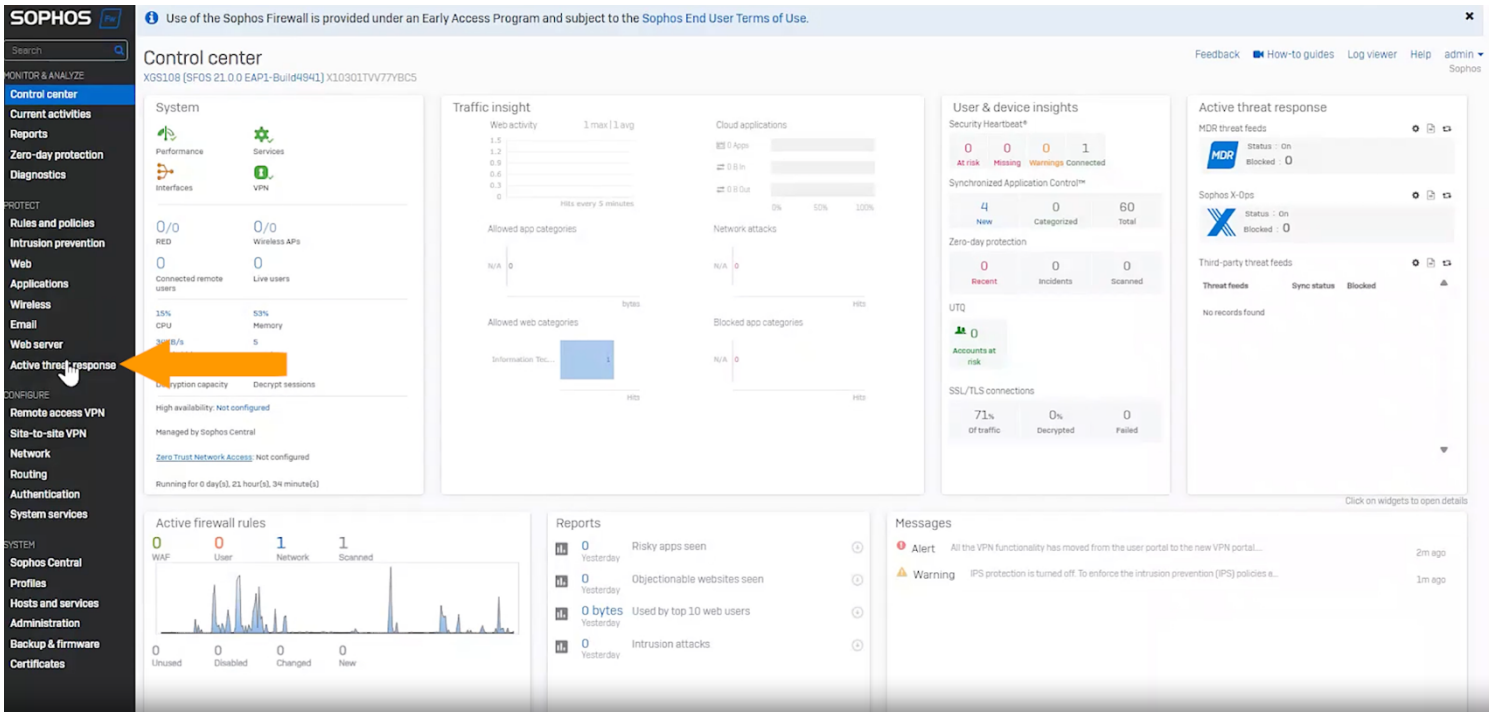
Setup Q-Feeds

Sophos's Next-Generation Firewall operates on the SFOS platform. Starting with SFOS version 21.0, the system supports the integration of external dynamic lists containing Indicators of Compromise (IoCs). These IoCs are managed as updatable text files hosted on a web server and accessible via HTTP or HTTPS. Make sure you have the Sophos Firewall: Xstream Protection Bundle.

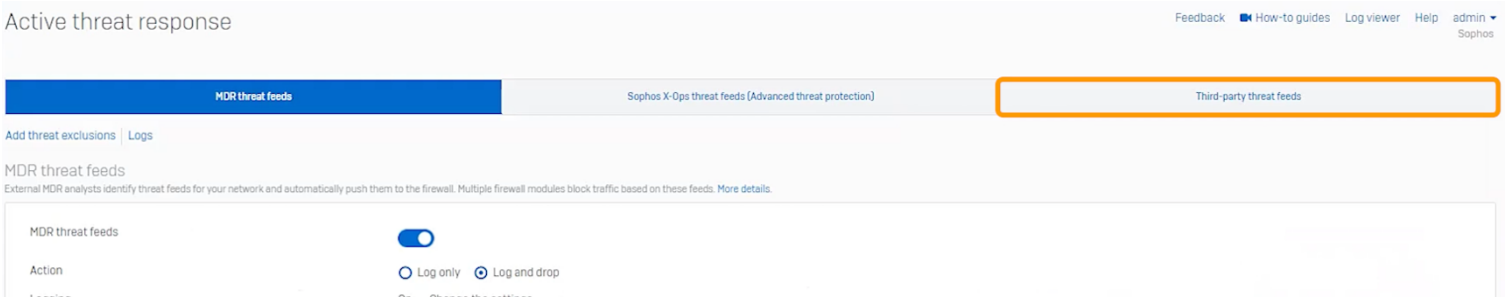
After importing IoCs into your Sophos device, you can apply them across various policy types based on their specific categories. For extra comprehensive information and illustrative examples, please consult the official Sophos documentation.

To add a new source of dynamic lists into Sophos, follow these steps:

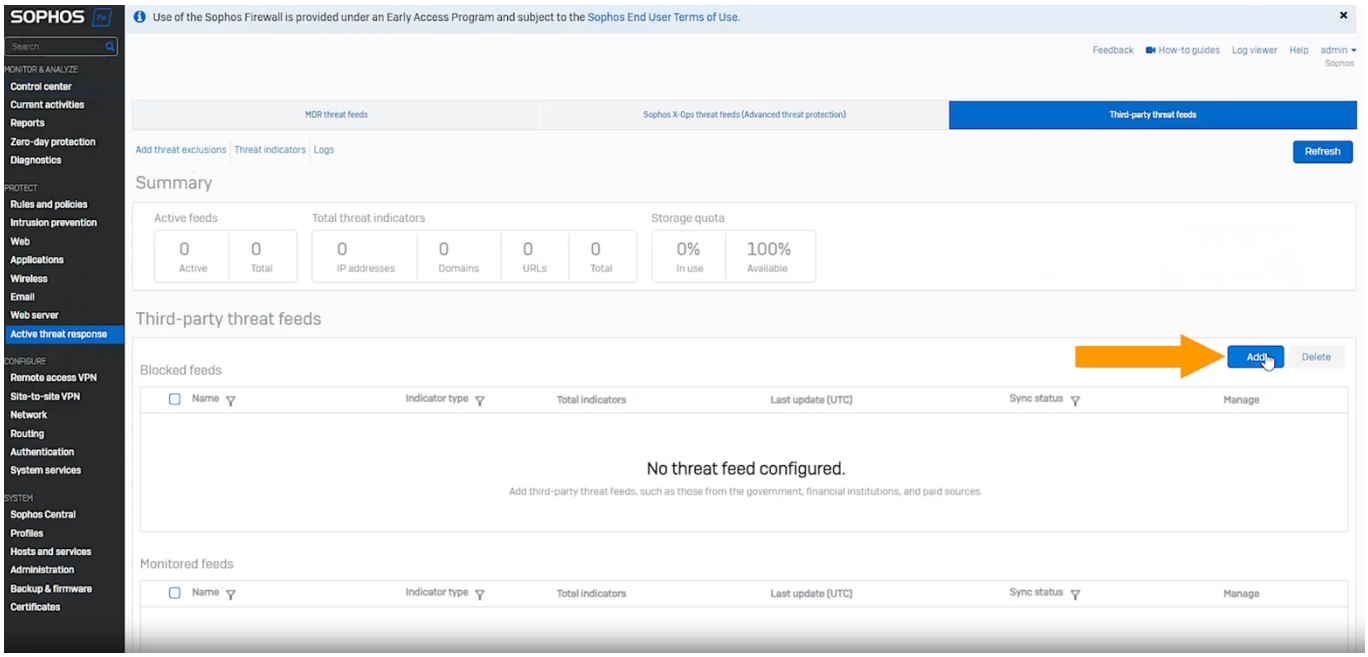
1. Navigate to Active threat response:



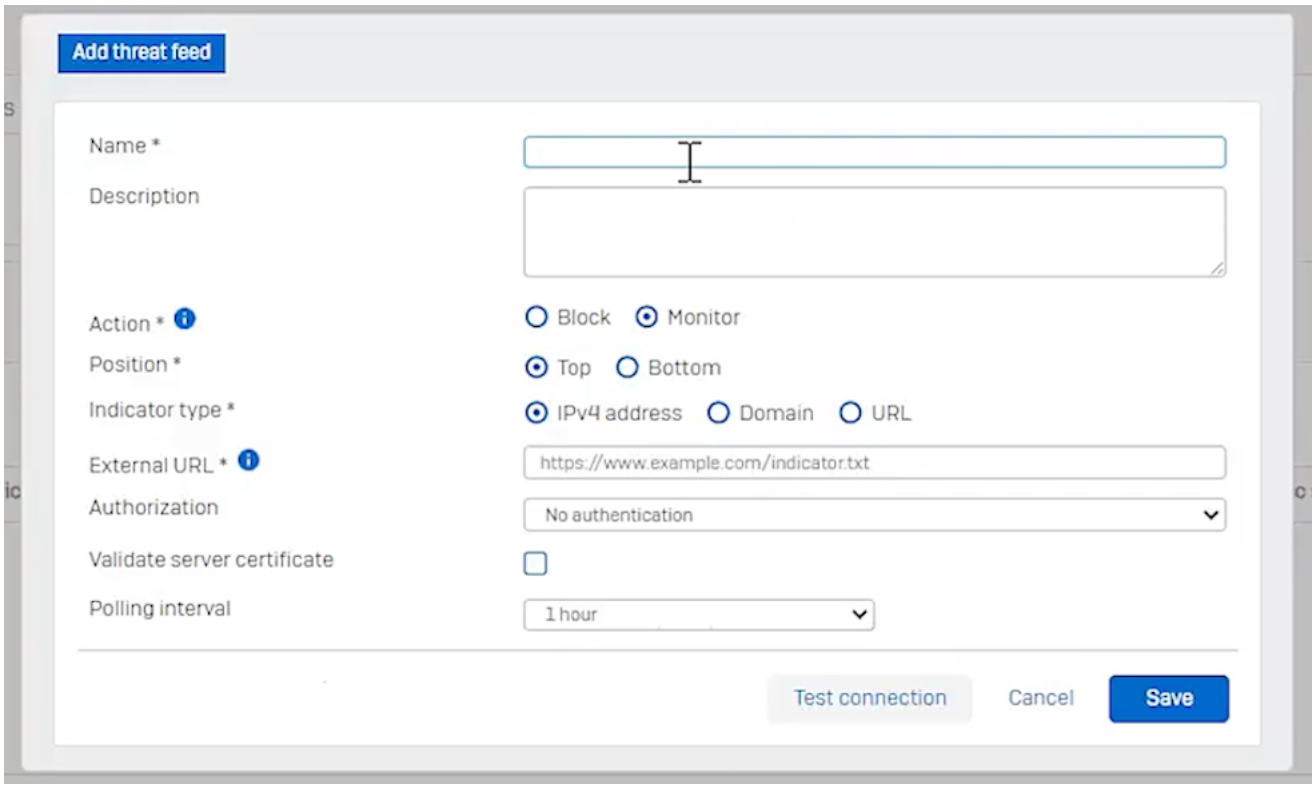
2. Select the 'Third-party threat feeds' tab



3. Click ‘Add’ under the third party threat feeds heading just below the summary on the top.



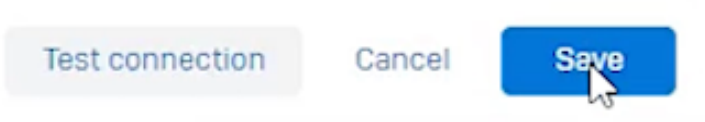
4. Setting Parameter for the threat feed.



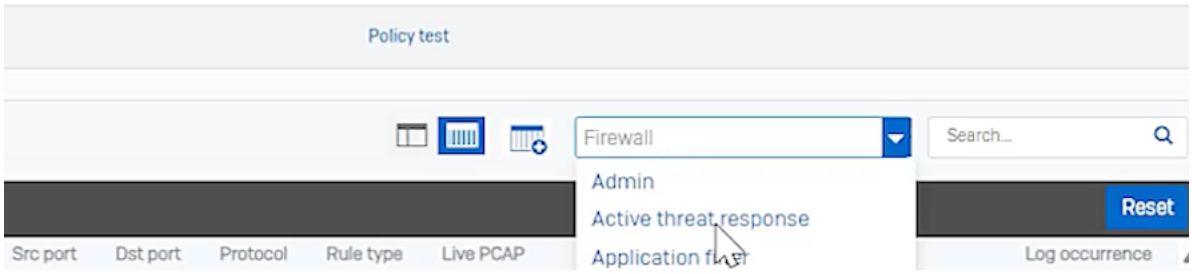
Set the values for the following parameters:

- **Name:** Enter a name for the list, e.g., "Dangerous IPs List".
- **Description:** fill a description, this is just for administrative purposes. e.g., “Q-Feeds threat intelligence feeds”
- **Action**: Block or Monitor; for you to decide. This option gives you the possibility to either block threats or just to monitor in order to evaluate our intelligence manually.
- **Position**: Top or Bottom; for you to decide. This option gives you the ability to set an order in case you have multiple threat feeds loaded in your Sophos Firewall.
- **Indicator type:** Depending on the type of source you’re trying to add as described on page 2.
- **External URL**: Enter the link to the list on Q-Feeds Threat Intelligence Portal, e.g., https://api.qfeeds.com/api?feed_type=XXXXX.
    - **Limit:** Set the threshold on the number of IoCs being downloaded. This parameter is optional but recommended to fit the allowed list capacity. Without this, all available IoCs will be downloaded, which may exceed the appliance's capacity. The limit can be set by adding “&limit=130000” to the URL.
- **HTTP Basic authentication**: Please enable. The **username** is “api_token” and the password is the token provided per mail.
    - If you encounter issues with HTTP basic authentication you can also add the api_token as a variable in the URL.
- **Polling interval:** Set the list update frequency in minutes (see recommended values in the table above).

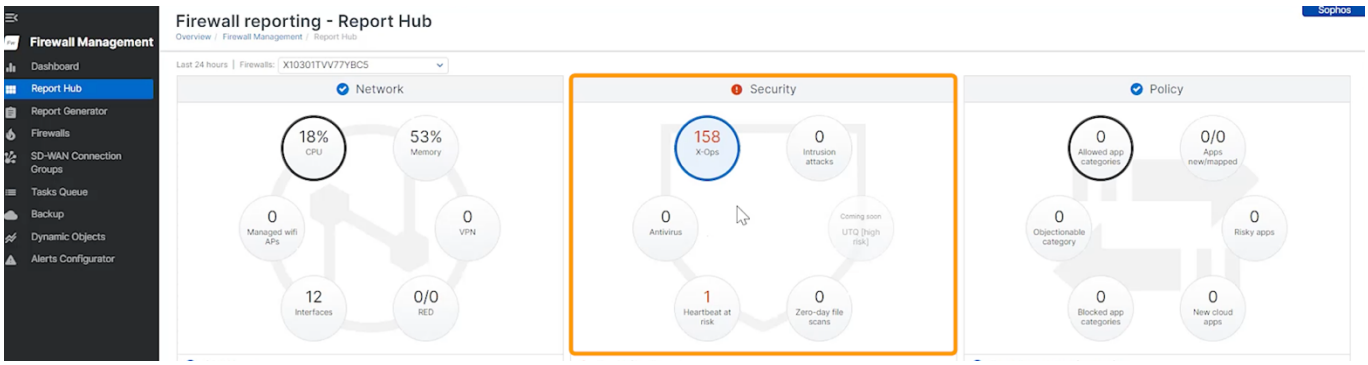
After filling in all the required settings, press "Test connection". If the test succeeded you can continue by pressing “Save” to create the connector:



Once you've imported the list, the threat intelligence will be used firewall wide in the **modules IPS, DNS, web & DPI**. Using the log viewer, you can view the number of hits on our Threat Intelligence. In order to do so select Active Threat Response in the log viewer as shown below.



Hits can also be observed using the Sophos Central Firewall Management Report hub:



Sophos Synchronized Security

In case you've implemented the Sophos Endpoint software with Synchronized Security the threat data feeds will be implemented on the endpoints as well. This helps you to protect against lateral movement.