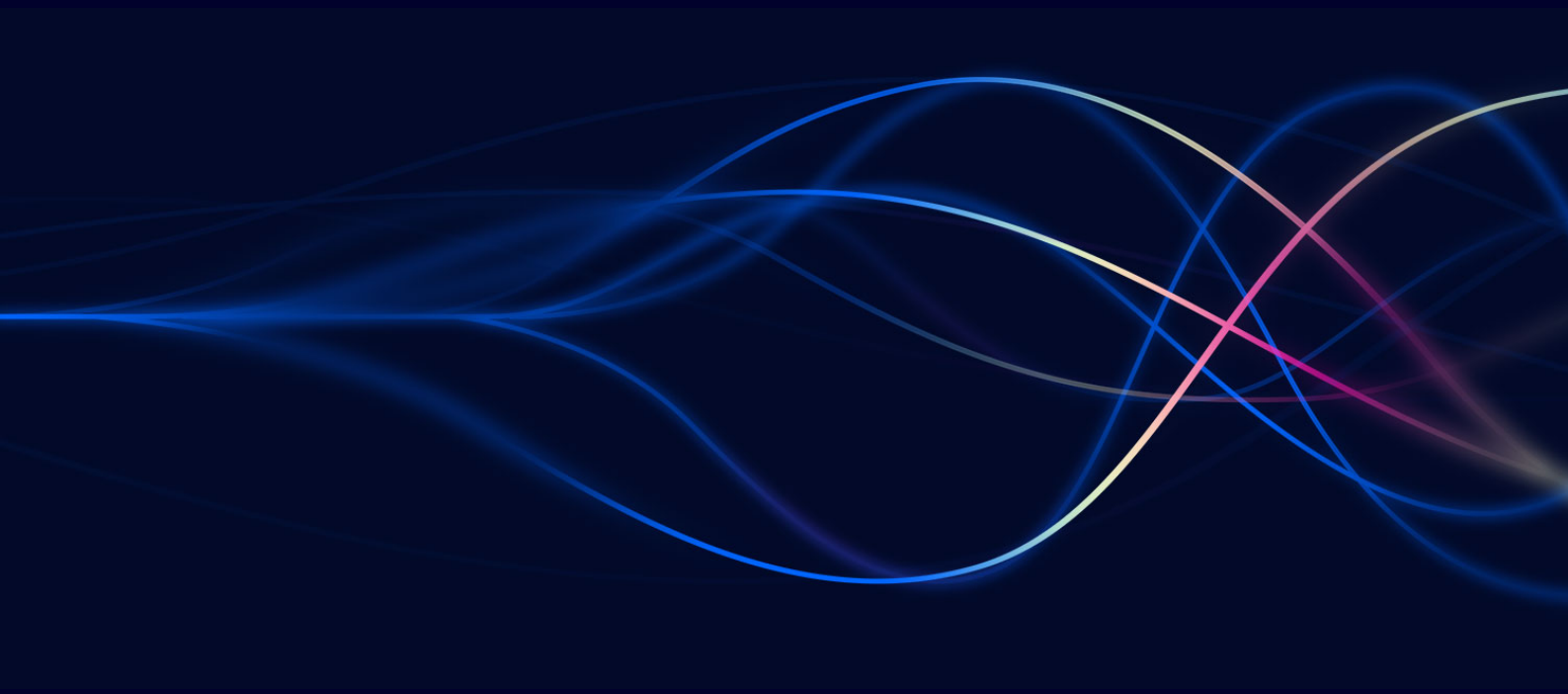
Q-FEEDS

# Setup Guide
# FortiGate NGFW

Public



Version 1.0 - 12 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 Fortigate 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 Fortigate 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 IPs** | IP | List of dangerous IP addresses | https://api.qfeeds.com/api?feed_type=malware_ips&api_token=XXXXXX&limit= XXXXXX |
| **Malware Domains** | URL | 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 and may overload the system.

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

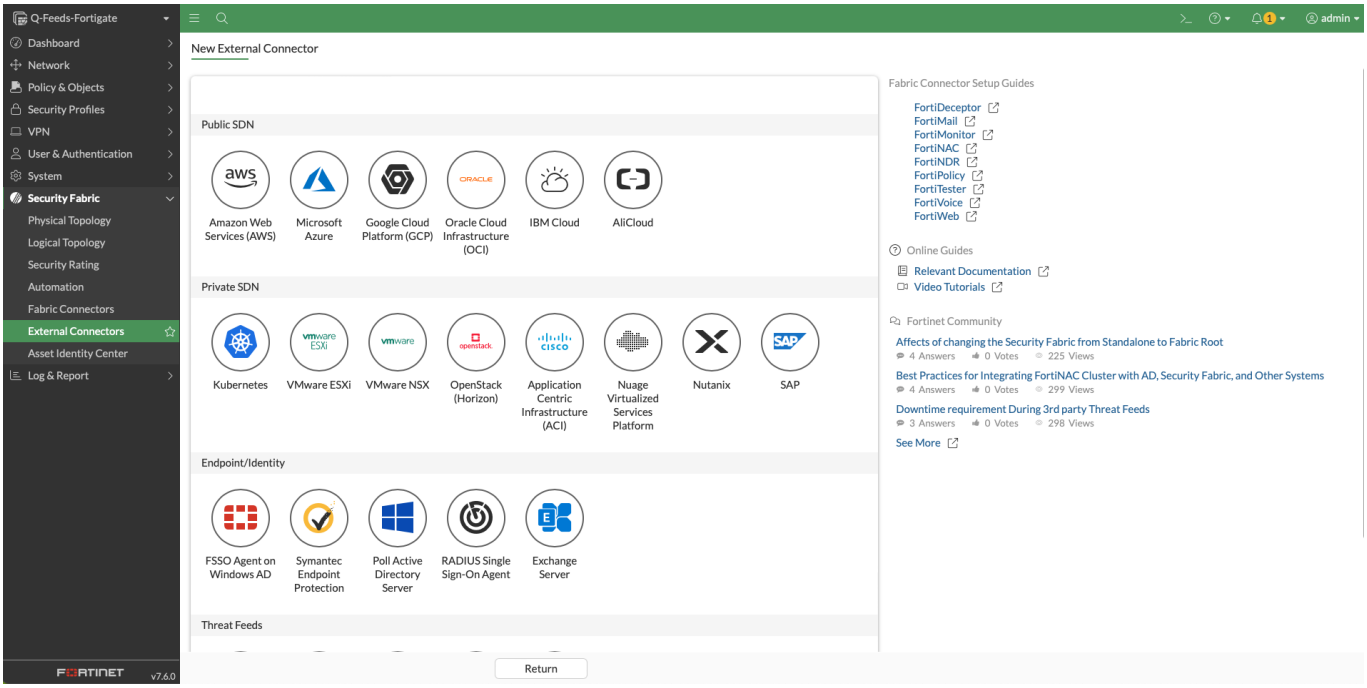
FortiGate's Next-Generation Firewall operates on the FortiOS platform. Starting with FortiOS version 6.0, the system supports the integration of external dynamic lists containing Indicators of Compromise (IoCs). These IoCs are managed as updatable text files hosted on a web server and accessible via HTTP or HTTPS.

After importing IoCs into your FortiGate device, you can apply them across various policy types based on their specific categories. These policy applications include Web Filtering, DNS Filtering, Antivirus Profiles, and can be designated as sources or destinations in both IPv4 and proxy policies. For comprehensive information and illustrative examples, please consult the official Fortinet documentation.

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

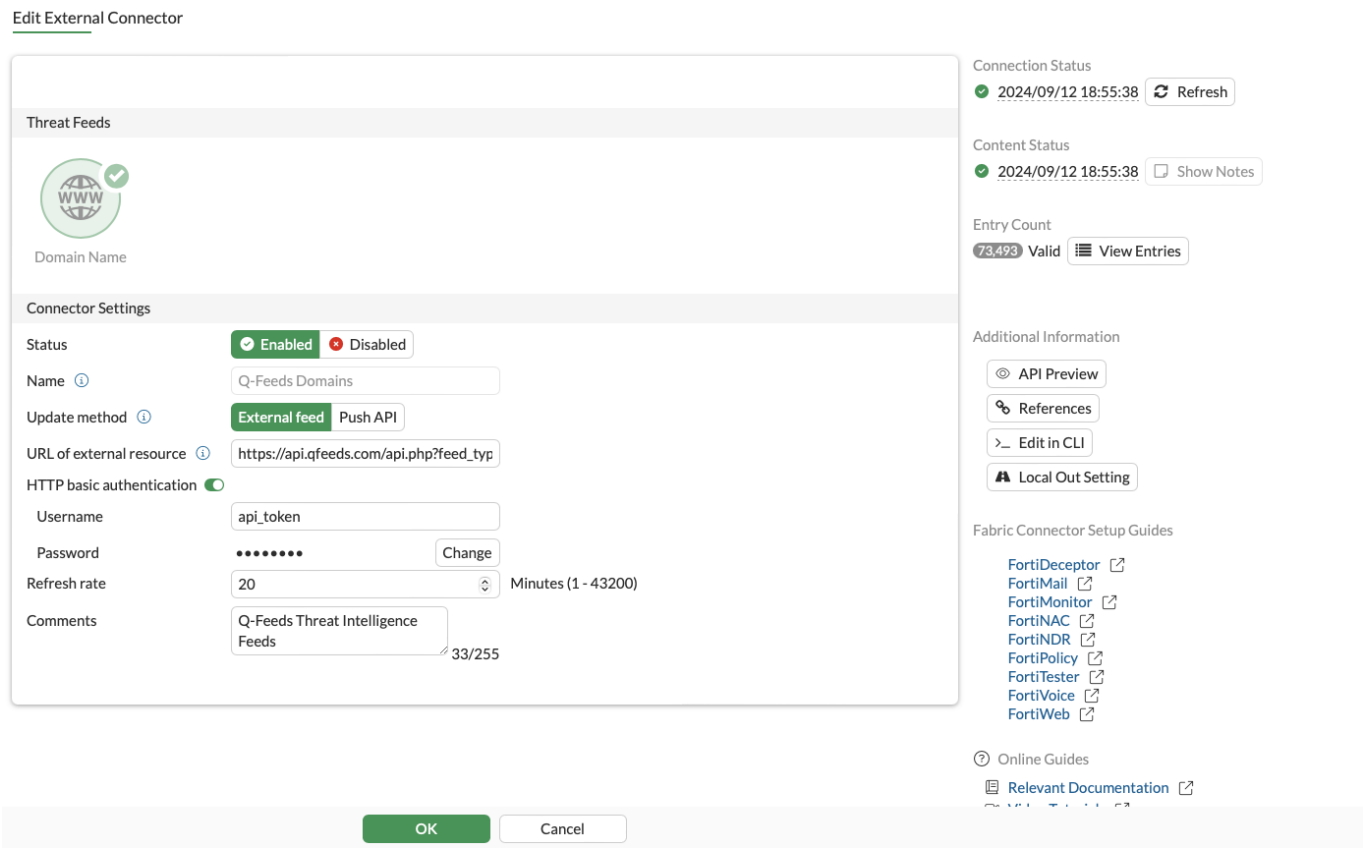
1. Navigate to Security Fabric:

    - Go to Security Fabric > External Connectors.
    - Click Create New.




2. Select Connector Type:

    - Choose the connector type based on the IoC type:
        - **IP Address** – for IP Address lists.
        - **Domain Name** – for URL lists.



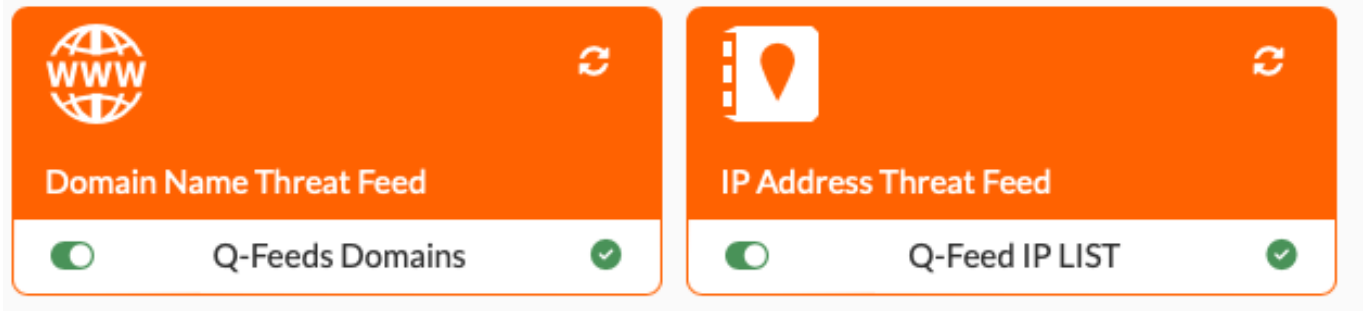

Setting Parameters for Dynamic Lists

Set the values for the following parameters:

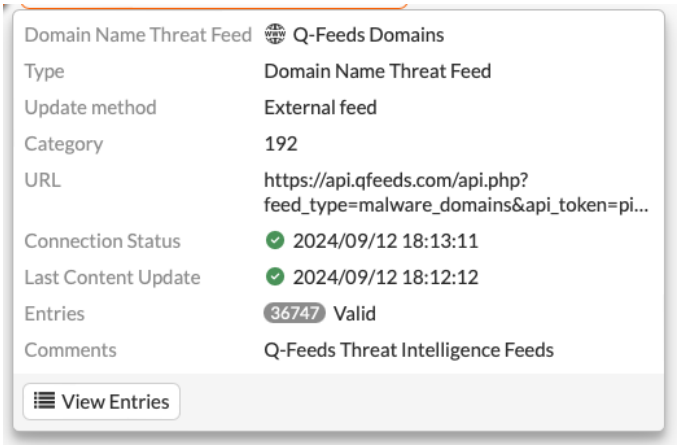
- **Name:** Enter a name for the list, e.g., "Dangerous IPs List".
- URI of External Resource: Enter the link to the list on Q-Feeds Threat Intelligence Portal, e.g., https://api.qfeeds.com/api?feed_type=XXXXX.
- **Limit:** Set the threshold on the number of IoCs being downloaded. This parameter is optional but recommended to fit the allowed list capacity. Without this, all available IoCs will be downloaded, which may exceed the appliance's capacity. See note below. The limit can be set by adding “&limit=130000” to the URL.

The maximum allowed dynamic list size for FortiGate is 10 MB or 128×1024 (131,072) IoCs. It is recommended to set limit=130000. The actual number of downloaded threat intelligence attributes can be less, depending on the number of available attributes within that specific type of feed.

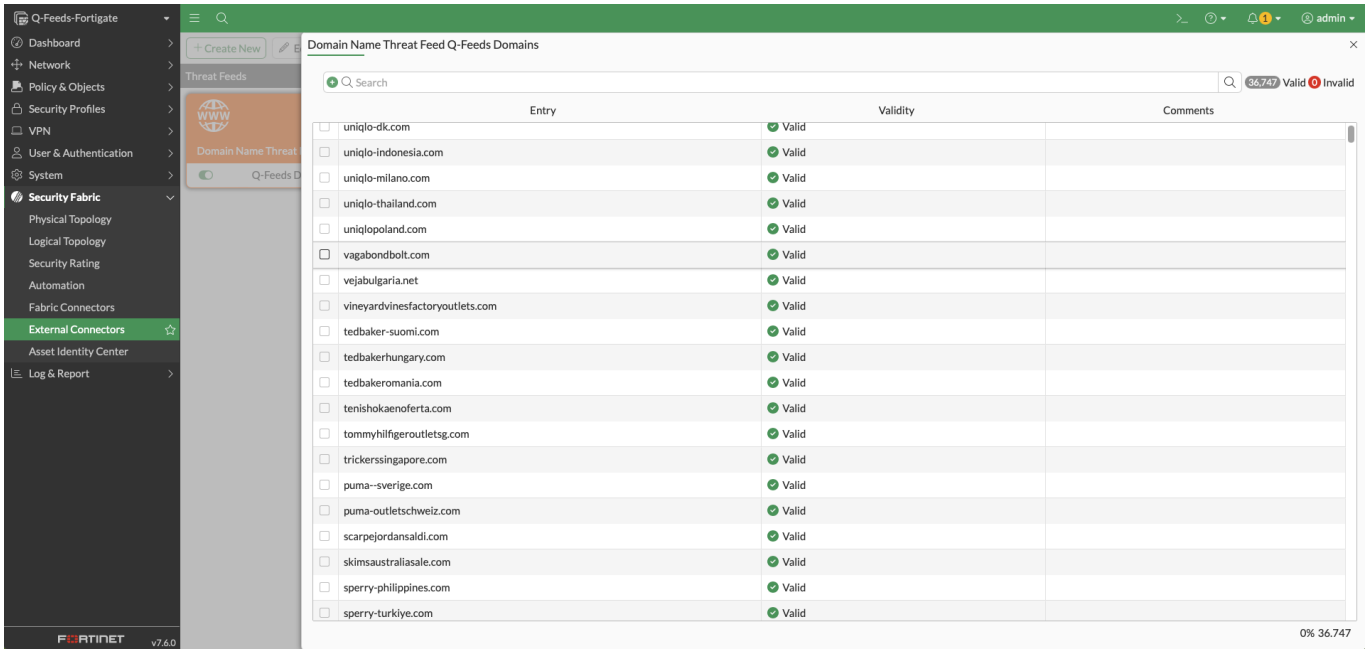
- **HTTP Basic authentication**: Please enable. The username is “api_token” and the password is the token provided per mail.
  - If you encounter issues with HTTP basic authentication you can also add the api_token as a variable in the URL.
- **Refresh Rate:** Set the list update frequency in minutes (see recommended values in the table above).
- **Comments:** Add any comments (this field is optional).
- **Status:** Switch on.




After filling in all the required settings, press "Ok" to create the connector:




You can also check the content of the feed by selecting the feed and then click “view content”.



Once you've imported the list, it can be applied to various policy types including Web Filtering, DNS Filtering, Firewall rules, Antivirus Profiles, and for specifying Source and Destination in both IPv4 and proxy policies.

**Note**: FortiGate automatically generates separate lists for IPv4 and IPv6 based on the IP addresses included in the Threat Feed.