ThreatQuotient

FS-Group Action

Version 1.0.0

October 29, 2024

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

Warning and Disclaimer 3
Support 4
Integration Details 5
Introduction 6
Prerequisites 7
Installation 8
Configuration 9
Actions 11
FS-Group Enrich IP Address 12
Enriched Data 16
Known Issues / Limitations 17
Change Log 18

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 5.26.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

FS-Group is a leader in the field of research and cyber threat prevention. The company's Ukraine-based experts have successfully engaged in the investigation of high-tech crimes through the use of security audits of computer systems and the implementation of integrated network solutions. Government agencies, private companies, and individual entities are among FS-Group's client base.

The integration provides the following action:

- **FS-Group Enrich IP Address** - retrieves all the info for submitted IP Addresses.

The action is compatible with the following IP Address type Indicators.

The action returns the following enriched indicator types:

- FQDN
- IP Addresses

This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing IP Address type indicators.
- A FS-Group API Key.
- The public IP address of your ThreatQ Instance must whitelisted by the FS-Group provider.

Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
   - Drag and drop the zip file into the dialog box
   - Select **Click to Browse** to locate the zip file on your local machine

   > ThreatQ will inform you if the action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

You will still need to configure the action.

Configuration

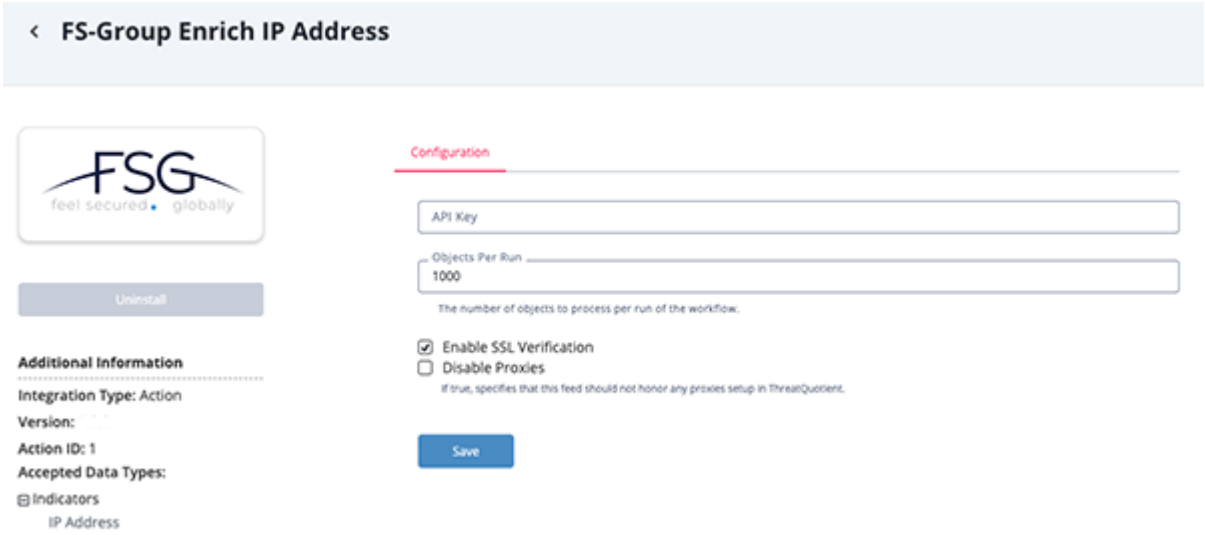
> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
API Key	Your FS-Group API Key.
Disable Proxies	Enable this parameter if the action should not honor the proxies set in ThreatQ.
Enable SSL Verification	When enabled, the action validates the host-provided SSL certificate. This option is enabled by default.



5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
FS-Group Enrich IP Address	Enrich IP Addresses	Indicators	IP Address

FS-Group Enrich IP Address

The FS-Group Enrich IP Address action enriches the submitted IP Address for relevant data.

`GET https://fslistapi.groupfs.net:44344/api/v2/ip/{{ip}}`

Sample Response:


```
[
    {
        "103.234.119.248": {
            "data": [],
            "meta": {
                "enrichment": {
                    "asn": 150306,
                    "asn_name": "dewan enterprise",
                    "city": "rangpur sadar",
                    "conn_speed": "broadband",
                    "conn_type": "wifi",
                    "count": 122,
                    "country": "Bangladesh",
                    "country_code": "bd",
                    "criminal": true,
                    "ip": "103.234.119.248",
                    "isp": "dewan enterprise",
                    "latitude": 25.75,
                    "listed_location": null,
                    "longitude": 89.23,
                    "method": "website",
                    "ns_name": "104-195-225-43.cpe.teksavvy.com",
                    "organization": "dewan enterprise",
                    "proxy": true,
                    "proxy_description": null,
                    "proxy_type": null,
                    "region": "f",
                    "source_description": "This IP address has been associated
with a proxy network providing residential and datacenter services.",
                    "source_id": "f15c917a-9d2e-4fe9-9fde-80bc0221f79f",
                    "source_name": "pyproxy",
                    "source_type": "proxy",
                    "tags": [
                        "Proxy",
                        "Criminal",
                        "Exit"
                    ],
                    "timestamps": [
                        {
                            "context": "first_seen",
                            "raw": "2024-04-23T00:00:00.000000Z",
                            "value": 1713830400
```

```
                        },
                        {
                            "context": "last_seen",
                            "raw": "2024-10-15T00:00:00.000000Z",
                            "value": 1728950400
                        }
                    ],
                    "url": "pyproxy.com"
                },
                "total": 0,
                "version": "4.33.8"
            }
        }
    },
    200
]
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.value	Indicator.Value	IP Address	.{ip}.meta.enrichment.timestamps.value	103.234.119.248	N/A
.{ip}.meta.enrichment.asn	Related Attribute	ASN	.{ip}.meta.enrichment.timestamps.value	150306	N/A
.{ip}.meta.enrichment.asn_name	Related Attribute	ASN Name	.{ip}.meta.enrichment.timestamps.value	dewan enterprise	N/A
.{ip}.meta.enrichment.city	Indicator.Attribute	City	.{ip}.meta.enrichment.timestamps.value	rangpur sadar	N/A
.{ip}.meta.enrichment.conn_speed	Indicator.Attribute	Connection Speed	.{ip}.meta.enrichment.timestamps.value	broadband	N/A
.{ip}.meta.enrichment.conn_type	Indicator.Attribute	Connection Type	.{ip}.meta.enrichment.timestamps.value	wifi	N/A
.{ip}.meta.enrichment.country	Indicator.Attribute	Country	.{ip}.meta.enrichment.timestamps.value	Bangladesh	N/A
.{ip}.meta.enrichment.country_code	Indicator.Attribute	Country Code	.{ip}.meta.enrichment.timestamps.value	bd	N/A
.{ip}.meta.enrichment.isp	Indicator.Attribute	ISP	.{ip}.meta.enrichment.timestamps.value	dewan enterprise	N/A
.{ip}.meta.enrichment.latitude	Indicator.Attribute	Latitude	.{ip}.meta.enrichment.timestamps.value	25.75	N/A
.{ip}.meta.enrichment.longitude	Indicator.Attribute	Longitude	.{ip}.meta.enrichment.timestamps.value	89.23	N/A
.{ip}.meta.enrichment.method	Indicator.Attribute	Method	.{ip}.meta.enrichment.timestamps.value	website	N/A
.{ip}.meta.enrichment.ns_name	Indicator.Attribute	NS Name	.{ip}.meta.enrichment.timestamps.value	104-195-225-43.cpe.teksavvy.com	N/A
.{ip}.meta.enrichment.organization	Indicator.Attribute	Organization	.{ip}.meta.enrichment.timestamps.value	dewan enterprise	N/A
.{ip}.meta.enrichment.region	Indicator.Attribute	Region	.{ip}.meta.enrichment.timestamps.value	f	N/A
.{ip}.meta.enrichment.source_name	Indicator.Attribute	Source Name	.{ip}.meta.enrichment.timestamps.value	pyproxy	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.{ip}.meta.enrichment.source_type`	Indicator.Attribute	Source Type	`.{ip}.meta.enrichment.timestamps.value`	`proxy`	N/A
`.{ip}.meta.enrichment.source_description`	Indicator.Description	N/A	`.{ip}.meta.enrichment.timestamps.value`	`This IP address has been associated with a proxy netw...`	N/A
`.{ip}.meta.enrichment.tags`	Indicator.Tag	N/A	`.{ip}.meta.enrichment.timestamps.value`	`Criminal`	N/A
`.{ip}.meta.enrichment.url`	Related Indicator.Value	FQDN	`.{ip}.meta.enrichment.timestamps.value`	`pyproxy.com`	N/A

Enriched Data

Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

METRIC	RESULT
Run Time	1 Day
Indicators	21,677
Indicator Attributes	256,430

Known Issues / Limitations

- This provider works with an IP whitelist; to ingest data from this feed, the public IP address of the ThreatQ instance must be whitelisted by FS-Group.

Change Log

- **Version 1.0.0**
  - Initial release