

ThreatQuotient



FireEye HX Export Connector Guide

Version 1.0.0

June 24, 2021

ThreatQuotient

11400 Commerce Park Dr., Suite 200
Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

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.

Copyright © 2021 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Contents

Versioning.....	4
Introduction.....	5
Installation	6
Configuration.....	9
Usage.....	11
Command Line Arguments	11
CRON.....	12
Example Run Log	13
FireEye HX Dashboard Example	14
Average Connector Run	15
Known Issues / Limitations.....	16
Change Log.....	17

Versioning

- Current integration version: 1.0.0
- Supported on ThreatQ versions \geq 4.35.0
- Supported Python Versions: 2.7.X, 3.5.X

There are two versions of this integration:

- Python 2 version
- Python 3 version

Introduction

The FireEye HX Export Connector for ThreatQ enables the automatic export of IOCs to Indicator Rules in FireEye HX. The connector has the ability to export up to 10,000 IOCs per type (FQDNs, IPs, & MD5s).

Installation

The connector can be installed from the ThreatQuotient repository with YUM credentials or offline via a .whl file.

⚠ Upgrading Users - Review the [Change Log](#) for updates to configuration parameters before updating. If there are changes to the configuration file (new/removed parameters), you must first delete the previous version's configuration file before proceeding with the install steps listed below. Failure to delete the previous configuration file will result in the connector failing.

1. Install the connector using one of the following methods:

ThreatQ Repository

- a. Run the following command:

```
<> pip install tq_conn_fireeye_hx_export
```

Offline via .whl file

To install this connector from a wheel file, the wheel file (.whl) will need to be copied via SCP into your ThreatQ instance.

- a. Download the connector whl file with its dependencies:

```
<> mkdir /tmp/tq_conn_fireeye_hx_export  
  
pip download tq_conn_fireeye_hx_export -d  
  
/tmp/tq_conn_fireeye_hx_export/
```

- b. Archive the folder with the .whl files:

```
<> tar -czvf tq_conn_fireeye_hx_export.tgz /tmp/  
tq_conn_fireeye_hx_export/
```

- c. Transfer all the whl files, the connector and all the dependencies, to the ThreatQ instance.
- d. Open the archive on ThreatQ:

```
<> tar -xvf tq_conn_fireeye_hx_export.tgz
```

- e. Install the connector on the ThreatQ instance.



The example assumes that all the whl files are copied to /tmp/conn on the ThreatQ instance.

```
<> pip install /tmp/conn/tq_conn_fireeye_hx_export-<version>-<python version>-none-any.whl --no-index --find-links /tmp/conn/
```



```
pip install /tmp/conn/tq_conn_fireeye_hx_export-1.0.0-py2-none-any.whl --no-index --find-links /tmp/conn/
```



A driver called `tq-conn-fireeye-hx-export` is installed. After installing with `pip` or `setup.py`, a script stub will appear in `/usr/bin/tq-conn-fireeye-hx-export`.

2. Once the application has been installed, a directory structure must be created for all configuration, logs and files, using the `mkdir -p` command. Use the commands below to create the required directories:

```
<> mkdir -p /etc/tq_labs/
    mkdir -p /var/log/tq_labs
```

3. Perform an initial run using the following command:

```
<> tq-conn-fireeye-hx-export -c /etc/tq_labs/ -ll /var/log/tq_labs/ -v3
```

4. Enter the following parameters when prompted:

PARAMETER	DESCRIPTION
ThreatQ Host	This is the hostname or IP address for the ThreatQ instance. Enter 127.0.0.1 if installing on the ThreatQ instance.
ThreatQ CID (Client ID)	This is the OAuth ID that can be found in your user profile in ThreatQ. Your account must have Administrative or Maintenance privileges
Email	The username that you use to log into ThreatQ.
Password	The password associated with the username above.

PARAMETER	DESCRIPTION
<hr/>	
Status	The default status for IoCs that are created by this integration. It is common to set this to Active but organization SOPs should be respected when setting this field.

Example Output

```
tq-conn-fireeye-hx-export -c /etc/tq_labs/ -ll /var/log/tq_labs/ -v3
ThreatQ Host: <ThreatQ Host IP or Hostname>
ThreatQ CID: <ClientID>
EMail A: <EMAIL ADDRESS>
Password: <PASSWORD>
Status: Active
Connector configured. Set information in UI
```

You will still need to [configure and then enable the connector](#).

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 **Labs** option from the *Category* dropdown (optional).




If you are installing the connector for the first time, it will be located under the **Disabled** tab.

3. Click on the integration to open its details page.
4. Enter the following parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
FireEye HX Host/ IP	Enter the hostname or IP address for your FireEye HX instance and include a port (if required).
FireEye HX API Username	<div>Enter your FireEye HX login username.</div> <div> Confirm that the user account is an API user, and not a regular user account, when configuring a username/ password. To create/view user accounts, log into FireEye HX, and navigate to Admin -> Appliance Settings -> User Accounts.</div>
FireEye HX API Password	Enter your FireEye HX login password.

PARAMETER	DESCRIPTION
Data Collection Name (Threat Library)	Enter the name of the data collection from ThreatQ that you'd like to export to FireEye HX. Each indicator type can only have a maximum of 10,000 entries.
Category Name	Enter the name of the category you want indicators added to.
Indicator Prefix	Enter a prefix for the indicator list name. Indicators will be created like so: <prefix> - <ioc type>.
Platforms	Select the platforms you want this export to apply to (Windows, OSX, or Linux).
Verify SSL	Enable or disable SSL verification for your FireEye HX host.

< FireEye HX Export



Disabled ☒ Enabled

Additional Information
Integration Type: Connector

Configuration

FireEye HX Host/IP
x.x.x.x:3000
Enter the hostname or IP address for your FireEye HX instance. Please include a port (if required)

FireEye HX Username
api_admin
Enter your FireEye HX login username

FireEye HX Password
.....
Enter your FireEye HX login password

Data Collection Name (Threat Library)
FireEye Export
Enter the name of the data collection from ThreatQ that you'd like to export to FireEye HX. Each indicator type can only have a maximum of 10,000 entries

Category Name
ThreatQ
Enter the name of the category you want indicators added to

Indicator Prefix
Malicious IOCs
Enter a prefix for the indicator list name. Indicators will be created like so: '<prefix> - <ioc type>'

Platforms
Select the platforms you want this export to apply to

☒ Windows
☒ OSX (macOS)
☒ Linux

☐ Verify SSL
Enable or disable SSL verification for your FireEye HX host

Save

- Review the **Settings** configuration, make any changes if needed, and click on **Save**.
- Click on the toggle switch, located above the *Additional Information* section, to enable it.

FireEye HX Export Connector
Version 1.0.0

10

Usage

Use the following command to execute the driver:

```
<> tq-conn-fireeye-hx-export -v3 -ll /var/log/tq_labs/ -c /etc/tq_labs/
```

Command Line Arguments

This connector supports the following custom command line arguments:

ARGUMENT	DESCRIPTION
<code>-h, --help</code>	Shows this help message and exits.
<code>-ll LOGLOCATION, --loglocation LOGLOCATION</code>	Sets the logging location for the connector. The location should exist and be writable by the current.
<code>-c CONFIG, --config CONFIG</code>	This is the location of the configuration file for the connector. This location must be readable and writable by the current user. If no config file path is given, the current directory will be used. This file is also where some information from each run of the connector may be put (last run time, private oauth, etc.)
<code>-v {1,2,3}, --verbosity {1,2,3}</code>	This is the logging verbosity level where 3 means everything.
<code>-ep, --external-proxy</code>	This allows you to use the proxy that is specified in the ThreatQ UI. This specifies an internet facing proxy, NOT a proxy to the TQ instance.

CRON

Automatic CRON configuration has been removed from this script. To run this script on a recurring basis, use CRON or some other jobs scheduler. The argument in the CRON script must specify the config and log locations.

Add an entry to your Linux crontab to execute the connector at a recurring interval. Depending on how quickly you need updates, this can be run multiple times a day (no more than once an hour) or a few times a week.

In the example below, the command will execute the connector every two hours.

1. Log into your ThreatQ host via a CLI terminal session.
2. Enter the following command:

```
<> crontab -e
```

This will enable the editing of the crontab, using vi. Depending on how often you wish the cronjob to run, you will need to adjust the time to suit the environment.

3. Enter the commands below:

Every 2 Hours Example

```
<> 0 */2 * * * tq-conn-fireeye-hx-export -c /etc/tq_labs/ -ll /  
var/log/tq_labs/ -v3
```

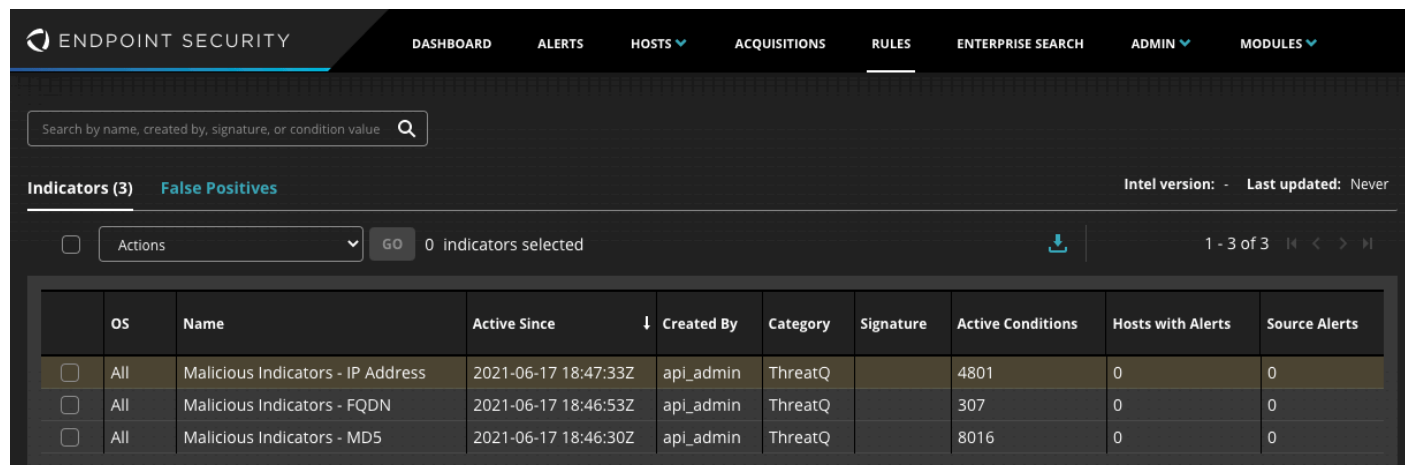
4. Save and exit CRON.

Example Run Log

```
2021-06-17 19:01:26 - threatqcc.custom_connector DEBUG: Using Current working directory for config path
2021-06-17 19:01:26 - tq_conn_fireeye_hx_export DEBUG: Private Connection Established
2021-06-17 19:01:27 - fireeye_hx_export INFO: Checking for category: ThreatQ Intelligence
2021-06-17 19:01:27 - fireeye_hx_export DEBUG: Category not found, creating...
2021-06-17 19:01:28 - fireeye_hx_export INFO: Checking for existing indicators...
2021-06-17 19:01:28 - fireeye_hx_export DEBUG: Creating indicator: Trickbot Malware - MD5
2021-06-17 19:01:28 - fireeye_hx_export DEBUG: Creating indicator: Trickbot Malware - FQDN
2021-06-17 19:01:28 - fireeye_hx_export DEBUG: Creating indicator: Trickbot Malware - IP Address
2021-06-17 19:01:29 - fireeye_hx_export INFO: Downloading data collection: FireEye Export
2021-06-17 19:01:29 - threatqsdk.threat_library DEBUG: Executing [indicators] Query: {"fields": ["value", "type"],
"filters": {"+and": [{"+or": [{"type_name": "FQDN"}, {"type_name": "IP Address"}, {"type_name": "MD5"}]}]},
"criteria": []}
2021-06-17 19:01:29 - threatqsdk.threat_library DEBUG: Threat Library search found 13124 total results
2021-06-17 19:01:29 - fireeye_hx_export DEBUG: Received batch of 1000 indicators from the data collection
2021-06-17 19:01:30 - fireeye_hx_export DEBUG: Received batch of 1000 indicators from the data collection
2021-06-17 19:01:30 - fireeye_hx_export DEBUG: Received batch of 1000 indicators from the data collection
2021-06-17 19:01:30 - fireeye_hx_export DEBUG: Received batch of 1000 indicators from the data collection
2021-06-17 19:01:30 - fireeye_hx_export DEBUG: Received batch of 1000 indicators from the data collection
2021-06-17 19:01:30 - fireeye_hx_export DEBUG: Received batch of 1000 indicators from the data collection
2021-06-17 19:01:31 - fireeye_hx_export DEBUG: Received batch of 1000 indicators from the data collection
2021-06-17 19:01:31 - fireeye_hx_export DEBUG: Received batch of 1000 indicators from the data collection
2021-06-17 19:01:31 - fireeye_hx_export DEBUG: Received batch of 1000 indicators from the data collection
2021-06-17 19:01:31 - fireeye_hx_export DEBUG: Received batch of 1000 indicators from the data collection
2021-06-17 19:01:31 - fireeye_hx_export DEBUG: Received batch of 1000 indicators from the data collection
2021-06-17 19:01:31 - fireeye_hx_export DEBUG: Received batch of 1000 indicators from the data collection
2021-06-17 19:01:32 - fireeye_hx_export DEBUG: Received batch of 1000 indicators from the data collection
2021-06-17 19:01:32 - fireeye_hx_export DEBUG: Received batch of 124 indicators from the data collection
2021-06-17 19:01:32 - fireeye_hx_export DEBUG: Uploading 4801 IP Address IOCs to Indicator, "Trickbot Malware - IP
Address"
2021-06-17 19:02:02 - fireeye_hx_export DEBUG: Uploading 307 FQDN IOCs to Indicator, "Trickbot Malware - FQDN"
2021-06-17 19:02:04 - fireeye_hx_export DEBUG: Uploading 8016 MD5 IOCs to Indicator, "Trickbot Malware - MD5"
2021-06-17 19:03:06 - tq_conn_fireeye_hx_export INFO: [::] Completed execution of the FireEye HX Export Connector in
99 seconds.
```

FireEye HX Dashboard Example

The following screenshot shows an example of exported ThreatQ data displayed in the FireEye HX Dashboard.



ENDPOINT SECURITY

DASHBOARD ALERTS HOSTS ACQUISITIONS RULES ENTERPRISE SEARCH ADMIN MODULES

Search by name, created by, signature, or condition value

Indicators (3) False Positives Intel version: - Last updated: Never

Actions GO 0 indicators selected

	OS	Name	Active Since	Created By	Category	Signature	Active Conditions	Hosts with Alerts	Source Alerts
<input type="checkbox"/>	All	Malicious Indicators - IP Address	2021-06-17 18:47:33Z	api_admin	ThreatQ		4801	0	0
<input type="checkbox"/>	All	Malicious Indicators - FQDN	2021-06-17 18:46:53Z	api_admin	ThreatQ		307	0	0
<input type="checkbox"/>	All	Malicious Indicators - MD5	2021-06-17 18:46:30Z	api_admin	ThreatQ		8016	0	0

Average Connector Run



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

EXPORTED OBJECT COUNT	FEED RUNTIME
15,000	100 seconds

Known Issues / Limitations

- The FireEye HX Indicator lists can only support up to 10,000 IOCs per type (MD5, FQDN, or IP Address)
- The FireEye HX API can only ingest MD5s, FQDNs, and IP Addresses

Change Log

- Version 1.0.0
 - Initial Release