ThreatQuotient

McAfee TIE Connector

Version 1.3.3

May 20, 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

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	1.3.3
Compatible with ThreatQ Versions	>= 4.19.0
Python Version	3.6
Support Tier	ThreatQ Supported

Introduction

The McAfee TIE Connector interacts with the McAfee TIE server. The TIE server is a database of malicious files and their reputations. The integration pulls the indicator hashes from the ThreatQ Threat Library, performs a potentially custom mapping of indicator attributes to the McAfee file reputations, and then pushes these indicators to the TIE server.

Key features of this integration include:

- User configurable rate limiting: ThreatQ will not push more than the configured indicators per day in the TIE server. **100,000 indicators per day** is the hard limit. The rate limit is honored regardless of how often the connector runs.
- ThreatQ indicator scores are mapped to McAfee reputation scores via user configuration. A user can export only indicators of interest out of the ThreatQ platform via configuration.
- Ability to use McAfee ePO's provisioning capability to get a signed certificate for communication with the TIE server.
- Ability to enrich any hash indicators in ThreatQ sent to McAfee TIE with additional information from the McAfee ecosystem.
- Ability to publish to multiple DXL fabrics, which are the communication layers for given segments of an enterprise. The communication occurs over one or multiple DXL servers, providing near seamless functionality. Publishing across multiple fabrics is a powerful mechanism.
- Ability to track the share status of indicators and re-push reputations, if desired by an analyst.

Prerequisites

Review the following requirements before attempting to install the connector.

Time Zone

You should ensure all ThreatQ devices are set to the correct time, time zone, and date (UTC is recommended), and using a clock source available to all.

To identify which time zone is closest to your present location, use the `timedatectl` command with the list-`timezones` command line option.

For example, enter the following command to list all available time zones in Europe:

```
timedatectl list-timezones | grep Europe
Europe/Amsterdam
Europe/Athens
Europe/Belgrade
Europe/Berlin
```

Enter the following command, as root, to change the time zone to UTC:

```
timedatectl set-timezone UTC
```

Provisioning McAfee ePolicy Orchestrator (ePO)

To communicate with the McAfee TIE server, you must have a certificate and the equivalent Certificate Authority (CA) must be imported in the McAfee ePO.

ThreatQuotient recommends using the a McAfee command line provisioning tool included with the integration. The integration wraps the McAfee command line provisioning tool and provides a command line utility that can be invoked as follows:

```
tq-mcafee-tie-prov --epo-ip <epo_ip> --epo-login <epo_login> --epo-pass
<epo_pass>
```

You can also pass a nonstandard EPO port and other optional arguments to the program above. To find additional options, simply invoke the program with `-h`.

If it is undesirable to supply the password on the command line, you can omit it and instead invoke the utility as:

```
tq-mcafee-tie-prov --epo-ip <epo_ip> --epo-login <epo_login>
```

The program will then prompt you for the password.

If this connector is being used to connect to multiple DXL brokers, the `-cn` or `--conn-name` option will be used to differentiate among those connectors. This option should be passed to the provisioning script (and the exact same `--conn-name` should be used in the actual connector as described below).

If you do not wish to use the command line provisioning tools option, you can follow the steps in the link provided below regarding external certificate authority provisioning:

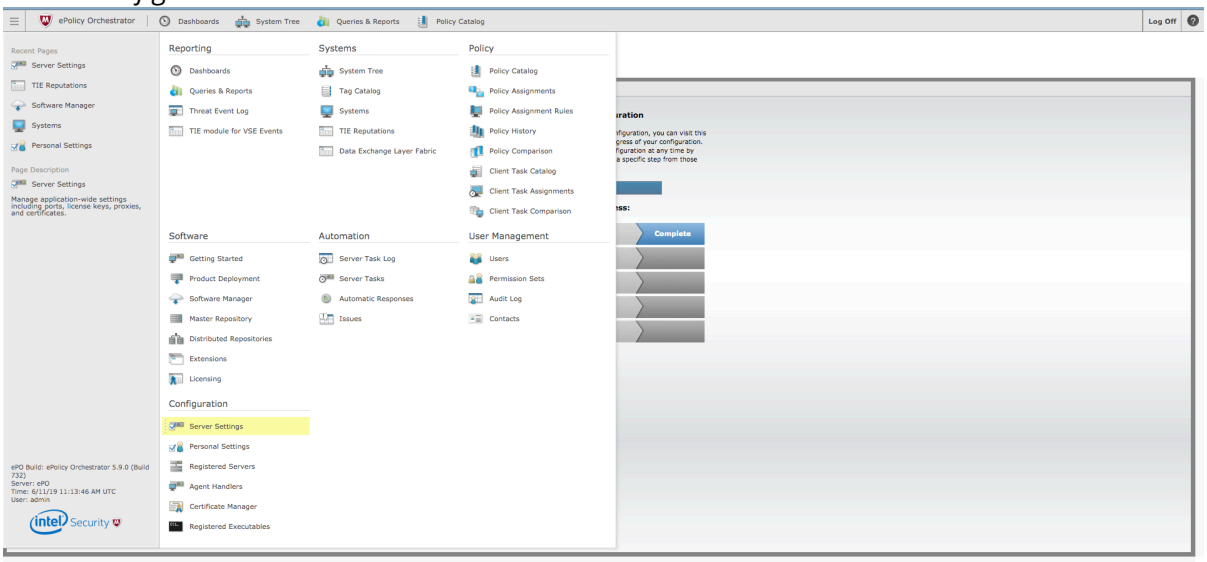
https://opendxl.github.io/opendxl-client-python/pydoc/epoexternalcertissuance.html

You will still need to configure and then enable the connector.

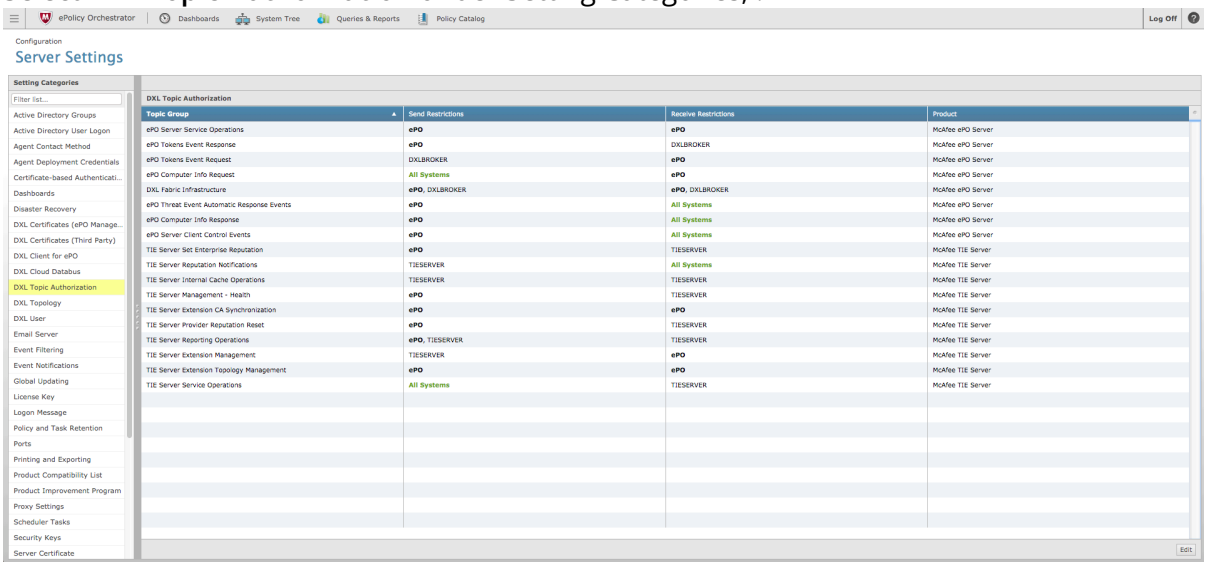
Enabling DXL Authorization

ThreatQ's integration with the Threat Intelligence Exchange relies on the Set Enterprise Reputation topic over DXL (/mcafee/service/tie/file/reputation/set). As a result, ThreatQ's certificate will need to be authorized to publish on this topic. After completing the steps in Provisioning the McAfee ePolicy Orchestrator (ePO), complete the following steps:

1. Log into the ePO user interface.
2. Click the menu button, located at the upper left portion of the page, and select **Server Settings** under *Configuration*.

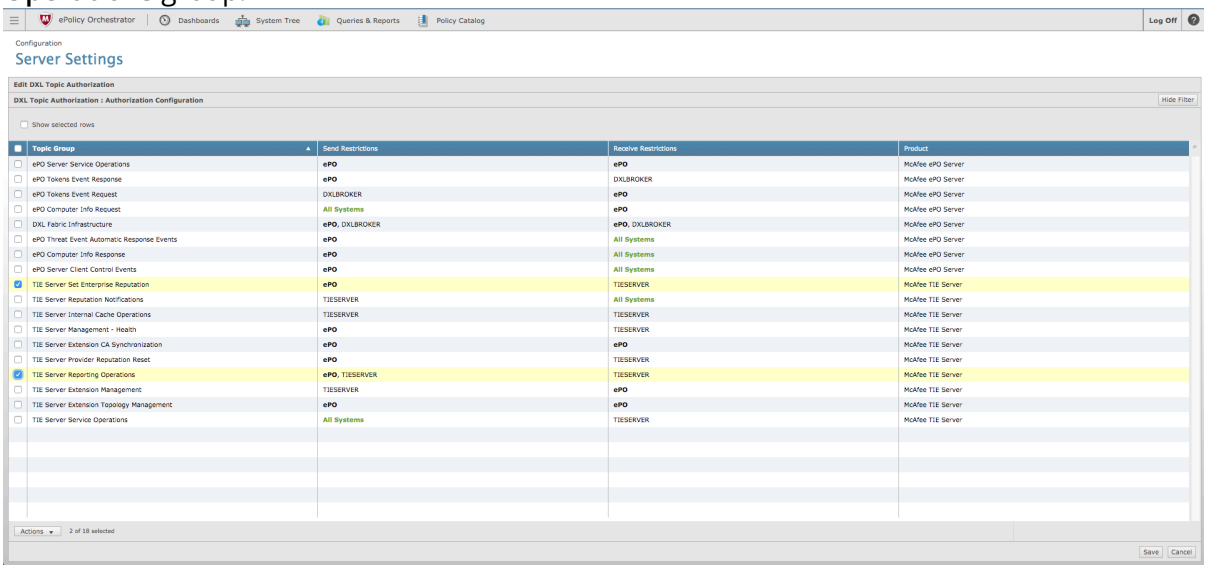


3. Select **DXL Topic Authorization** under Setting Categories, .

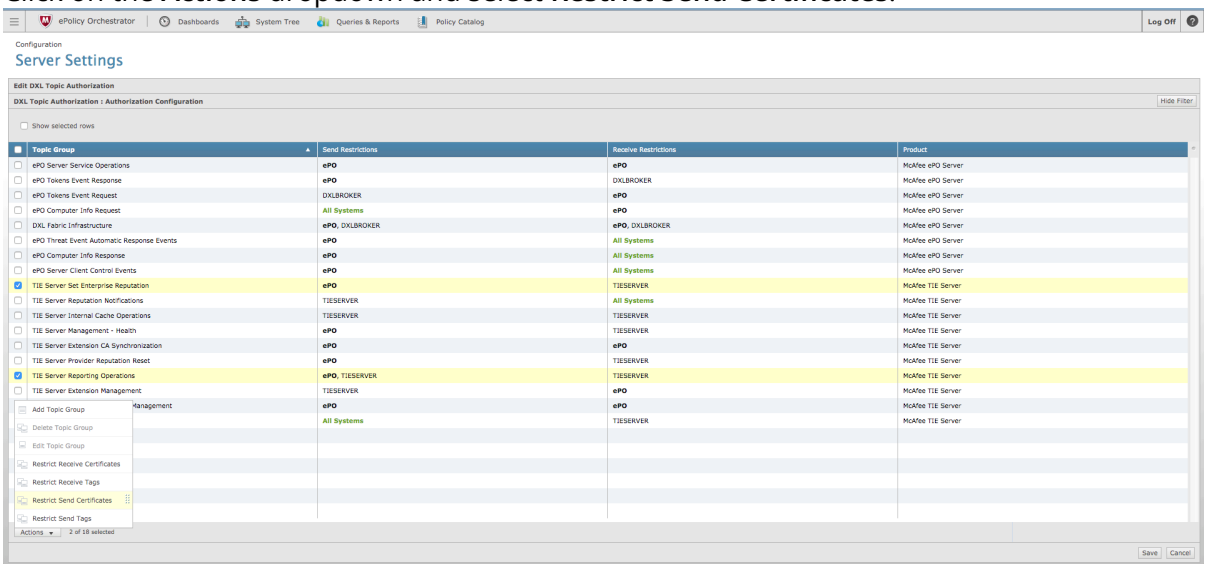


4. Click **Edit**, located in lower right portion of the page, and then select the check boxes associated with the **TIE Server Set Enterprise Reputation** topic group and the **TIE Server Reporting**

Operations group.

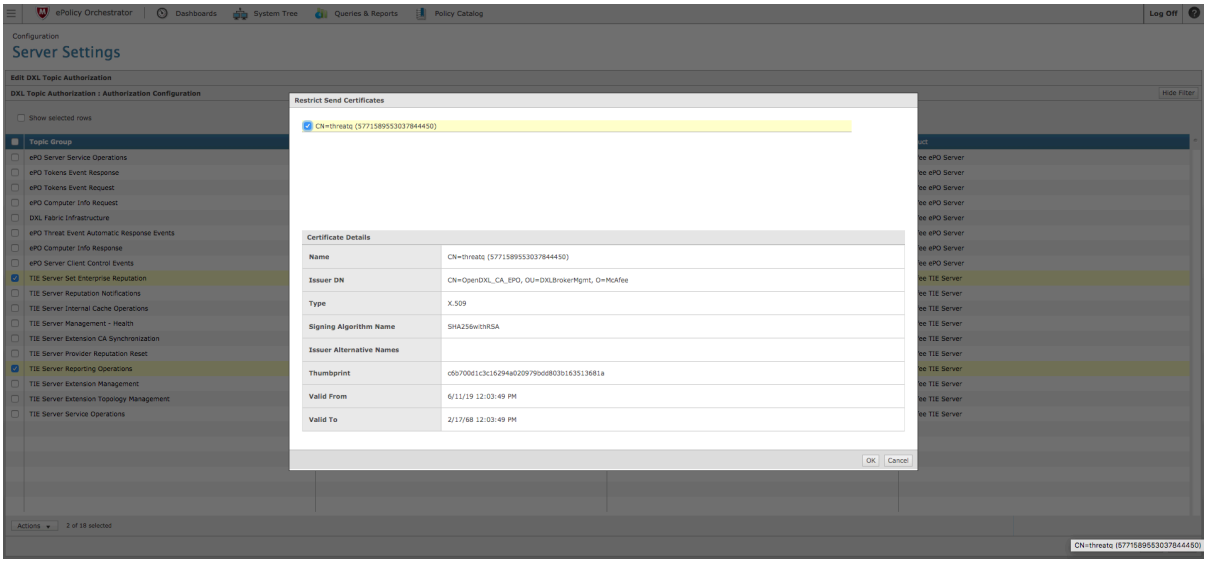


5. Click on the **Actions** dropdown and select **Restrict Send Certificates**.

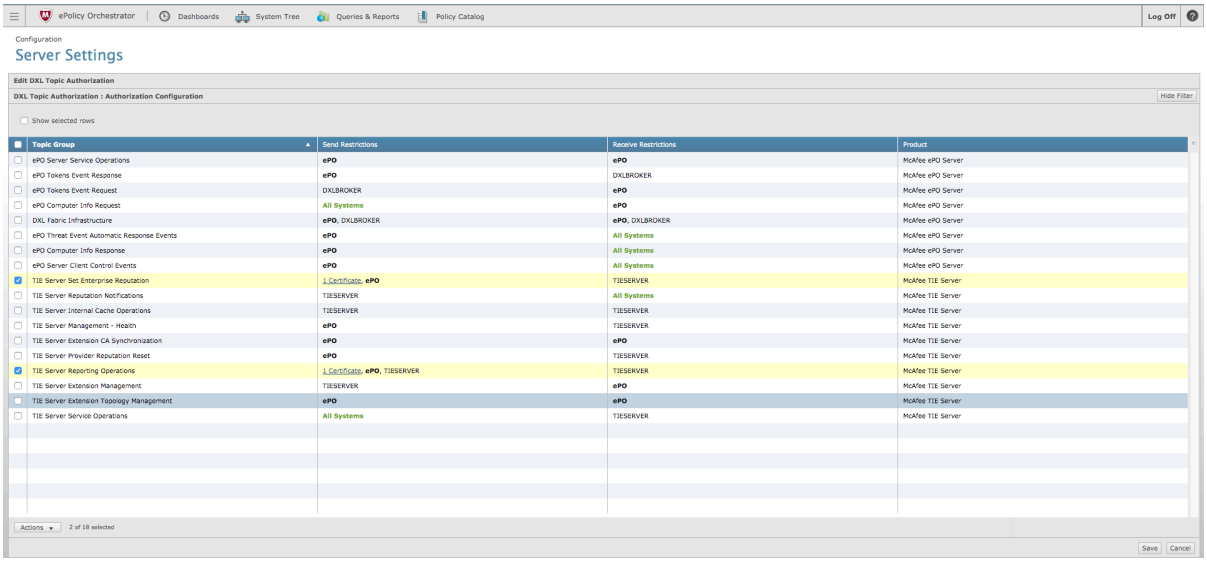


6. Identify the **threatq certificate** that was created during the provisioning step.

The value will start with CN=threatq.



7. Click **OK**.
8. Verify that the **TIE Server Set Enterprise Reputation** and **TIE Server Reporting Operations** now each have one certificate listed within the *Send Restrictions* column.



9. Click **Save** located in the lower left portion of the page.

It may take several minutes or a few hours for the topic authorizations to take effect. Running the ThreatQ-TIE connector during this time will cause it to hang and eventually time out.

Integration Dependencies

The integration must be installed in a python 3.6 environment.

The following is a list of required dependencies for the integration. These dependencies are downloaded and installed during the installation process. If you are an Air Gapped Data Sync (AGDS) user, or run an instance that cannot connect to network services outside of your infrastructure, you will need to download and install these dependencies separately as the integration will not be able to download them during the install process.

Items listed in bold are pinned to a specific version. In these cases, you should download the version specified to ensure proper function of the integration.

DEPENDENCY	VERSION	NOTES
asn1crypto	**1.0.0**	**Pinned Version**
distlib	N/A	N/A
threatqsdk	>= 1.3.6	N/A
threatqcc	>= 1.3.1	N/A
dxltieclient	**0.1.0**	**Pinned Version**
dxlclient	**4.0.0.418**	**Pinned Version**

Installation

The following provides you with steps on installing a Python 3 Virtual Environment and installing the connector.

Creating a Python 3.6 Virtual Environment

Run the following commands to create the virtual environment:

```
mkdir /opt/tqvenv/
sudo yum install -y python36 python36-libs python36-devel python36-pip
python3.6 -m venv /opt/tqvenv/<environment_name>
source /opt/tqvenv/<environment_name>/bin/activate
pip install --upgrade pip
pip install threatqsdk threatqcc setuptools==59.6.0
```

Proceed to Installing the Connector.

Installing the Connector

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. Navigate to the ThreatQ Marketplace and download the .whl file for the integration.
2. Activate the virtual environment if you haven't already:

```
source /opt/tqvenv/<environment_name>/bin/activate
```

3. Transfer the whl file to the `/tmp` directory on your ThreatQ instance.
4. Install the connector on your ThreatQ instance:

```
pip install /tmp/tq_conn_<wheel_name>-<version>-py3-none-any.whl
```

A driver called `tq-conn-mcafee-tie` will be installed. After installing, a script stub will appear in `/opt/tqvenv/<environment_name>/bin/tq-conn-mcafee-tie`.

5. 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/
mkdir -p /etc/pki/tls/certs/mcafee_dxl_certs/
```

6. Perform an initial run using the following command:

```
/opt/tqvenv/<environment_name>/bin/tq-conn-mcafee-tie -ll /var/log/
tq_labs/ -c /etc/tq_labs/ -v3
```

7. Enter the following parameters when prompted:

PARAMETER	DESCRIPTION
ThreatQ Host	This is the host of the ThreatQ instance, either the IP Address or Hostname as resolvable by ThreatQ.
ThreatQ Client ID	This is the OAuth id that can be found at Settings Gear → User Management → API details within the user's details.

PARAMETER	DESCRIPTION
ThreatQ Username	This is the Email Address of the user in the ThreatQ System for integrations.
ThreatQ Password	The password for the above ThreatQ account.
Status	This is the default status for objects that are created by this Integration.

Example Output

```
/opt/tqvenv/<environment_name>/bin/tq-conn-mcafee-tie -ll /var/log/
tq_labs/ -c /etc/tq_labs/ -v3
ThreatQ Host: <ThreatQ Host IP or Hostname>
ThreatQ Client ID: <ClientID>
ThreatQ Username: <EMAIL ADDRESS>
ThreatQ Password: <PASSWORD>
Status: Review
Connector configured. Set information in UI
```

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

PARAMETER	DESCRIPTION
Daily Rate Limiting	Enter a daily limit, 1-100000, for the number of DXL set reputation requests made. The default limit setting is 1000. The daily rate limit helps to prevent overloading the McAfee TIE infrastructure. Data pertaining to the daily rate limiting is persisted in the file `mcafee_tie_cache.json` (or `mcafee_tie_cache-<connector-name>.json`). This file can be modified or removed to reset the daily rate limit for the specific connector in question.
Known Malicious Reputation Mapping	Select the appropriate . Options include: ◦ Very High ◦ High ◦ Medium ◦ Low ◦ Very Low See the ThreatQ Scoring to McAfee TIE Reputation Mapping section for more information regarding this parameter.
Most Likely Malicious Reputation Mapping	Select the appropriate . Options include: ◦ Very High ◦ High ◦ Medium ◦ Low ◦ Very Low See the ThreatQ Scoring to McAfee TIE Reputation Mapping section for more information regarding this parameter.

PARAMETER	DESCRIPTION
Might Be Malicious Reputation Mapping	Select the appropriate . Options include: ◦ Very High ◦ High ◦ Medium ◦ Low ◦ Very Low See the ThreatQ Scoring to McAfee TIE Reputation Mapping section for more information regarding this parameter.
Number of Days	Enter the number of days back the integration should go for indicators added to the ThreatQ platform. Accepted values range from 1 - 365.
Filter by Indicator Status	Enter a ThreatQ Status to filter indicators by. This parameter only accepts single-word statuses. **Example:** Active
Filter by Indicator Score	Enter an indicator score to filter indicators by. The value provided will be calculated as a greater than or equal to equation. **Example:** Enter 5 will filter indicators with a score of 5 or greater. Entering a value of 0 will include all scores.
Filter by Indicator Attributes	Enter a comma-separated list of key-value pairs in which the key corresponds to the Attribute Name and the value corresponds to the Attribute Value. The key and value are separated by a colon. You can filter on multiple Attribute Values for the same Attribute Name by having individual key-value pairs where the key is the same for both pairs. **Example:** `Attribute1:Value1, Attribute2:Value2, Attribute1:Value2`
Intelligence Data Enrichment	This parameter allows you to specify if file hashes in ThreatQ should be enriched by the McAfee ecosystem. Enabling this feature will result in The following attributes are created for each

PARAMETER	DESCRIPTION
	of McAfee ATD, McAfee GTI and the Enterprise (which in this case is ThreatQ): ◦ *** Enterprise Trust Level** - Reputation of this hash as known by Enterprise. ◦ *** GTI Trust Level** - Reputation of this hash as known by GTI. ◦ **Prevalence** - True when the file was referenced by more than a configurable amount of end- points. ◦ **Detection Count** ◦ **Enterprise Count** ***** See the **Trust Level** entry found in the McAfee Cache File chapter of this guide for further details.

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Scoring to McAfee TIE Reputation Mapping

Use the following information to assist in setting the reputation mapping parameters under the Configuration tab for the integration.

ThreatQ supports the following scoring bands:

THREATQ SCORING BAND	RANGE
very low	0-4
low	5-6
medium	7-8
high	9
very high	10+

One or more ThreatQ scoring bands can be mapped to a McAfee reputation score with the following conditions:

- The same ThreatQ scoring band cannot be mapped to multiple McAfee TIE reputation scores.
- A higher ThreatQ scoring band cannot be mapped to a less malicious McAfee TIE reputation score. For example, the following configuration is **invalid**:

MCAFEE TIE REPUTATION	THREATQ SCORING BANDS
Known Malicious	low
Most Likely Malicious	medium
Might Be Malicious	high

- Multiple scoring bands can be assigned to the same Reputation as long as the above two conditions are satisfied. An example of a **valid** configuration is as follows:

MCAFEE TIE REPUTATION	THREATQ SCORING BANDS
Known Malicious	very high, high
Most Likely Malicious	medium
Might Be Malicious	low, very low

McAfee Cache File

A cache file, `mcafee_tie_cache.json`, is utilized by the connector. The following key values pairs are recorded in the cache file:

VALUE PAIRS	DESCRIPTION
`indicators_sent`	The total number of indicators sent to McAfee TIE over a 24 hour period.
`start_time`	The epoch time from when the connector was initially ran. This value is set to the current time whenever the connector runs 24 hours after the recorded start time.
`Trust Level`	Trust levels are as follows: • Reputation 0 = Not Set • Reputation 1 = Known Malicious • Reputation 15 = Most Likely Malicious • Reputation 30 = Might be Malicious

VALUE PAIRS	DESCRIPTION
	• Reputation 50 = Unknown • Reputation 70 = Might be Trusted • Reputation 85 = Most Likely Trusted • Reputation 99 = Known Trusted
`Share Status - <connector_name>`	This attribute is created for each indicator after the indicator is pushed to a particular fabric. Possible values are: • `Pushed` - If indicator is not in the fabric • `Locally set` - If indicator was already in the fabric before pushing
`Reputation Override - <connector_name>`	This attribute can be added manually from the ThreatQ user interface if a user wants to re-push an already pushed indicator to the DXL fabric with a different reputation. At maximum, there can be one Reputation Override attribute per indicator.

Usage

Use the following command to execute the driver:

```
/opt/tqvenv/<environment_name>/bin/tq-conn-mcafee-tie -v3 -ll /var/log/
tq_labs/ -c /etc/tq_labs/ -x /etc/tq_labs/ -dc /etc/pki/tls/certs/
mcafee_dxl_certs/
```

Command Line Arguments

This connector supports the following custom command line arguments:

ARGUMENT	DESCRIPTION
`-h`, `--help`	Review all additional options and their descriptions.
`-ll LOGLOCATION`, `--loglocation LOGLOCATION`	Sets the logging location for the connector. The location should exist and be writable by the current. A special value of 'stdout' means to log to the console (this happens by default).
`-c CONFIG`, `--config CONFIG`	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.)
`-v {1,2,3}`, `--verbosity {1,2,3}`	This is the logging verbosity level where **3** means everything.
`-cn, --con-name`	Name of the connector (Option used in order to allow users to configure multiple McAfee TIE connector instances on the same TQ box)
`-x, --cache` (Optional)	This sets the location of the cache file that marks the last file hash indicator that was received in this connector's previous run. The default is cwd.

ARGUMENT	DESCRIPTION
`dc, --dxl-config-dir` (Optional)	This sets the location of where the connector will look for the directory containing the McAfee DXL certificate files. The default is cwd.

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 * * * /opt/tqvenv/<environment_name>/bin/tq-conn-mcafee-tie -v3
   -ll /var/log/tq_labs/ -c /etc/tq_labs/ -x /etc/tq_labs/ -dc /etc/pki/
   tls/certs/mcafee_dxl_certs/
   ```
4. Save and exit CRON.

Change Log

- **Version 1.3.3**
  - Updated integration to improve overall performance. The improvements will resolve a 500 server error that some users experienced when running the connector.
- **Version 1.3.2:**
  - Fixed a bug for conflicting dependencies regarding asn1crypto-1.3.0.
- **Version 1.3.1:**
  - Reputations that were labeled *Possible Malicious* have been relabeled as *Might Be Malicious*.
- **Version 1.3.0:**
  - The maximum number of DXL set reputation requests allowed per day increased from 1000 to 100000.
  - Indicators sent to the DXL communication fabric are prioritized as follows:
    1. Indicators with Reputation Overwrite set (ordered descending by score)
    2. Indicators with a higher score (ordered descending by score)
  - All ThreatQ indicators, regardless of score, are now mapped to McAfee reputation Most Likely Malicious, by default.
  - Selection fields now provide multi-select and Boolean features.
  - Querying indicators in the TIE server does not increase the sighting count.