McAfee TIE Connector Implementation Guide

Version 1.3.1

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.

Last Updated: Thursday, July 25, 2019

Contents

Introduction

This connector (integration) 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.

Versioning

- Current integration version: `1.3.1`
- Supported on ThreatQ versions `4.19.0` or higher

Installation

The following command installs this integration via `pip`.

```
pip install tq_conn_mcafee_tie
```

Current Features

- User configurable rate limiting: ThreatQ will not push more than the configured indicators per day in the TIE server. *100000 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.

Usage

Provisioning the 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. The steps are documented here: https://opendxl.github.io/opendxl-client-python/pydoc/epoexternalcertissuance.html.

However, there is an easier alternate way that uses a McAfee command line provisioning tool. **For simplicity of use, this approach is recommended**. This 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 you wish not 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 prompt you for the password.

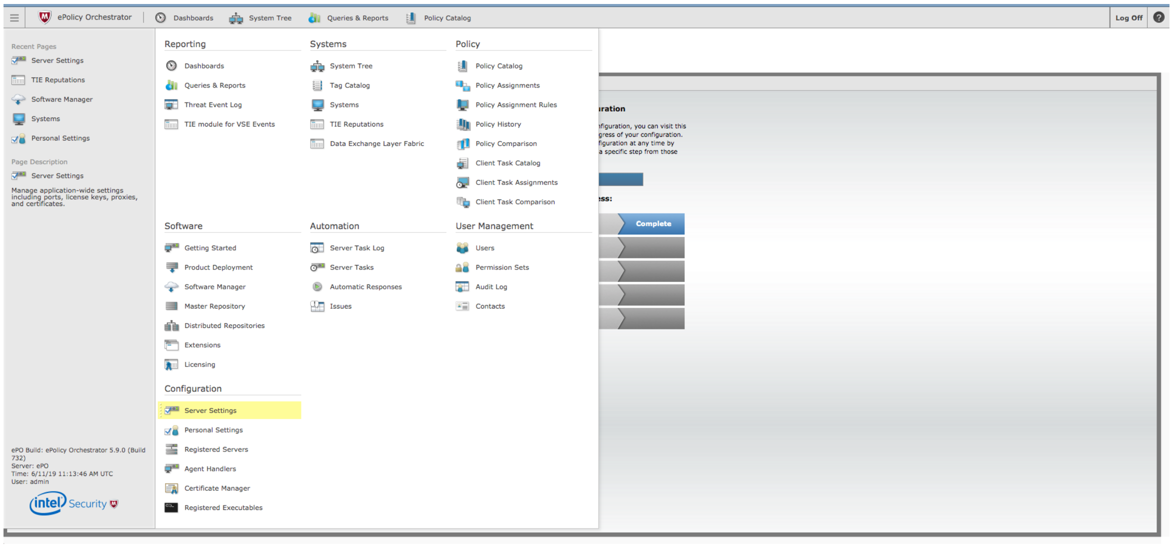
If this connector is being used to connect to multiple DXL brokers, the `-cn` or `--conn-name` option will be used to differentiate among those connectors. This option should be passed to the provisioning script (and the exact same `--conn-name` should be used in the actual connector as described later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

> On MAC High Sierra, an existing bug that doesn't support libressl can cause the ePO provisioning tool `tq-mcafee-tie-prov` to fail with a message like: `Error initializing ctypes`. You can manually apply a patch as documented here: https://github.com/wbond/oscrypto/commit/83e2a06085b5b09ee5cd6c28a2ae1c52352c9e53

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:

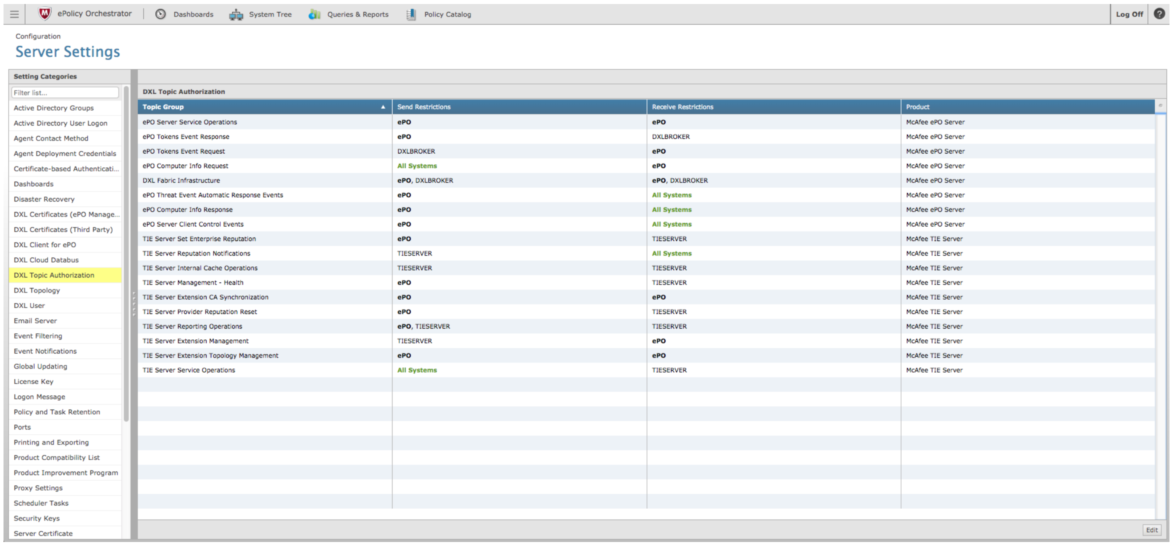
1. Log into the ePO user interface.
2. Click the menu button at the upper left portion of the page and then select **Server Settings** under **Configuration**.



Manage application-wide settings including ports, license keys, proxies, and certificates.

ePO Build: ePolicy Orchestrator 5.9.0 (Build 732)
Server: ePO
Time: 6/11/19 11:13:46 AM UTC
User: admin

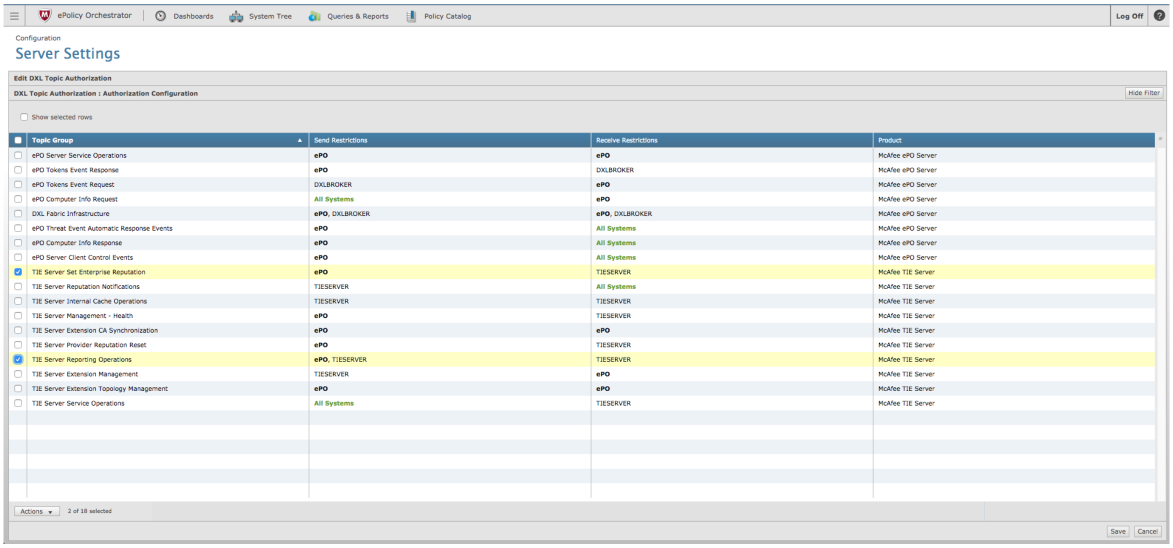
3. Under **Setting Categories**, select **DXL Topic Authorization**.



DXL Topic Authorization

Topic Group	Send Restrictions	Receive Restrictions	Product
ePO Server Service Operations	ePO	ePO	McAfee ePO Server
ePO Tokens Event Response	ePO	DXLBROKER	McAfee ePO Server
ePO Tokens Event Request	DXLBROKER	ePO	McAfee ePO Server
ePO Computer Info Request	All Systems	ePO	McAfee ePO Server
DXL Fabric Infrastructure	ePO, DXLBROKER	ePO, DXLBROKER	McAfee ePO Server
ePO Threat Event Automatic Response Events	ePO	All Systems	McAfee ePO Server
ePO Computer Info Response	ePO	All Systems	McAfee ePO Server
ePO Server Client Control Events	ePO	All Systems	McAfee ePO Server
TIE Server Set Enterprise Reputation	ePO	TIESERVER	McAfee TIE Server
TIE Server Reputation Notifications	TIESERVER	All Systems	McAfee TIE Server
TIE Server Internal Cache Operations	TIESERVER	TIESERVER	McAfee TIE Server
TIE Server Management - Health	ePO	TIESERVER	McAfee TIE Server
TIE Server Extension CA Synchronization	ePO	ePO	McAfee TIE Server
TIE Server Provider Reputation Reset	ePO	TIESERVER	McAfee TIE Server
TIE Server Reporting Operations	ePO, TIESERVER	TIESERVER	McAfee TIE Server
TIE Server Extension Management	TIESERVER	ePO	McAfee TIE Server
TIE Server Extension Topology Management	ePO	ePO	McAfee TIE Server
TIE Server Service Operations	All Systems	TIESERVER	McAfee TIE Server

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



Configuration

Server Settings

Edit DXL Topic Authorization

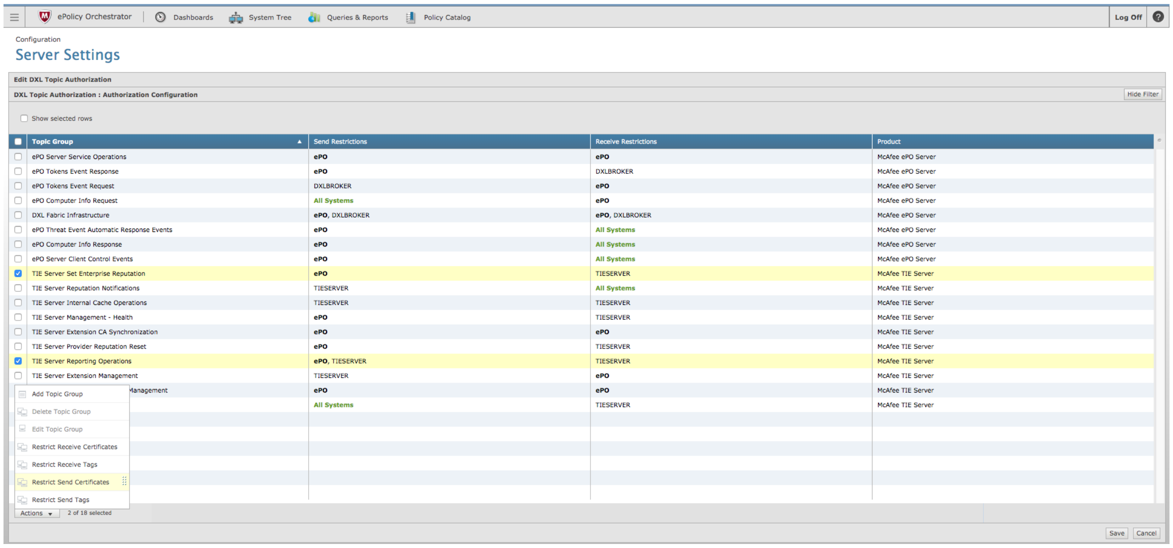
DXL Topic Authorization : Authorization Configuration

□ Show selected rows

□	Topic Group	Send Restrictions	Receive Restrictions	Product
□	ePO Server Service Operations	ePO	ePO	McAfee ePO Server
□	ePO Tokens Event Response	ePO	DXLBROKER	McAfee ePO Server
□	ePO Tokens Event Request	DXLBROKER	ePO	McAfee ePO Server
□	ePO Computer Info Request	All Systems	ePO	McAfee ePO Server
□	DXL Fabric Infrastructure	ePO, DXLBROKER	ePO, DXLBROKER	McAfee ePO Server
□	ePO Threat Event Automatic Response Events	ePO	All Systems	McAfee ePO Server
□	ePO Computer Info Response	ePO	All Systems	McAfee ePO Server
□	ePO Server Client Control Events	ePO	All Systems	McAfee ePO Server
☑	TIE Server Set Enterprise Reputation	ePO	TIESERVER	McAfee TIE Server
□	TIE Server Reputation Notifications	TIESERVER	All Systems	McAfee TIE Server
□	TIE Server Internal Cache Operations	TIESERVER	TIESERVER	McAfee TIE Server
□	TIE Server Management - Health	ePO	TIESERVER	McAfee TIE Server
□	TIE Server Extension CA Synchronization	ePO	ePO	McAfee TIE Server
□	TIE Server Provider Reputation Reset	ePO	TIESERVER	McAfee TIE Server
☑	TIE Server Reporting Operations	ePO, TIESERVER	TIESERVER	McAfee TIE Server
□	TIE Server Extension Management	TIESERVER	ePO	McAfee TIE Server
□	TIE Server Extension Topology Management	ePO	ePO	McAfee TIE Server
□	TIE Server Service Operations	All Systems	TIESERVER	McAfee TIE Server

2 of 18 selected

5. In the lower left portion of the page , select the **Actions** dropdown and then select **Restrict Send Certificates**.



Configuration

Server Settings

Edit DXL Topic Authorization

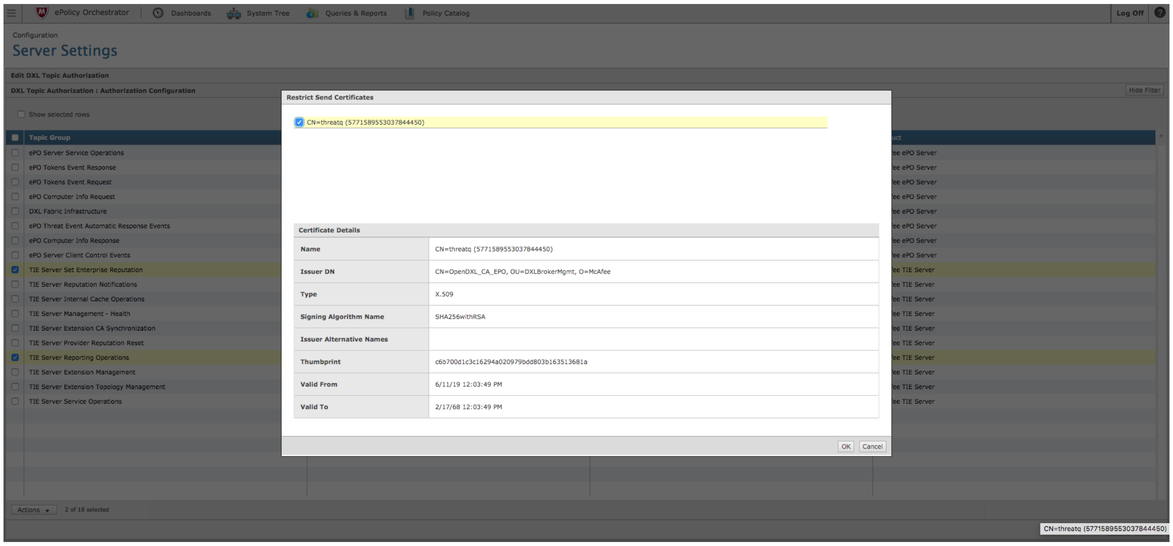
DXL Topic Authorization : Authorization Configuration

□ Show selected rows

□	Topic Group	Send Restrictions	Receive Restrictions	Product
□	ePO Server Service Operations	ePO	ePO	McAfee ePO Server
□	ePO Tokens Event Response	ePO	DXLBROKER	McAfee ePO Server
□	ePO Tokens Event Request	DXLBROKER	ePO	McAfee ePO Server
□	ePO Computer Info Request	All Systems	ePO	McAfee ePO Server
□	DXL Fabric Infrastructure	ePO, DXLBROKER	ePO, DXLBROKER	McAfee ePO Server
□	ePO Threat Event Automatic Response Events	ePO	All Systems	McAfee ePO Server
□	ePO Computer Info Response	ePO	All Systems	McAfee ePO Server
□	ePO Server Client Control Events	ePO	All Systems	McAfee ePO Server
☑	TIE Server Set Enterprise Reputation	ePO	TIESERVER	McAfee TIE Server
□	TIE Server Reputation Notifications	TIESERVER	All Systems	McAfee TIE Server
□	TIE Server Internal Cache Operations	TIESERVER	TIESERVER	McAfee TIE Server
□	TIE Server Management - Health	ePO	TIESERVER	McAfee TIE Server
□	TIE Server Extension CA Synchronization	ePO	ePO	McAfee TIE Server
□	TIE Server Provider Reputation Reset	ePO	TIESERVER	McAfee TIE Server
☑	TIE Server Reporting Operations	ePO, TIESERVER	TIESERVER	McAfee TIE Server
□	TIE Server Extension Management	TIESERVER	ePO	McAfee TIE Server
	Management	ePO	ePO	McAfee TIE Server
		All Systems	TIESERVER	McAfee TIE Server

2 of 18 selected

6. Identify the `threatq` certificate that was created during the provisioning step. The value will start with CN=threatq.



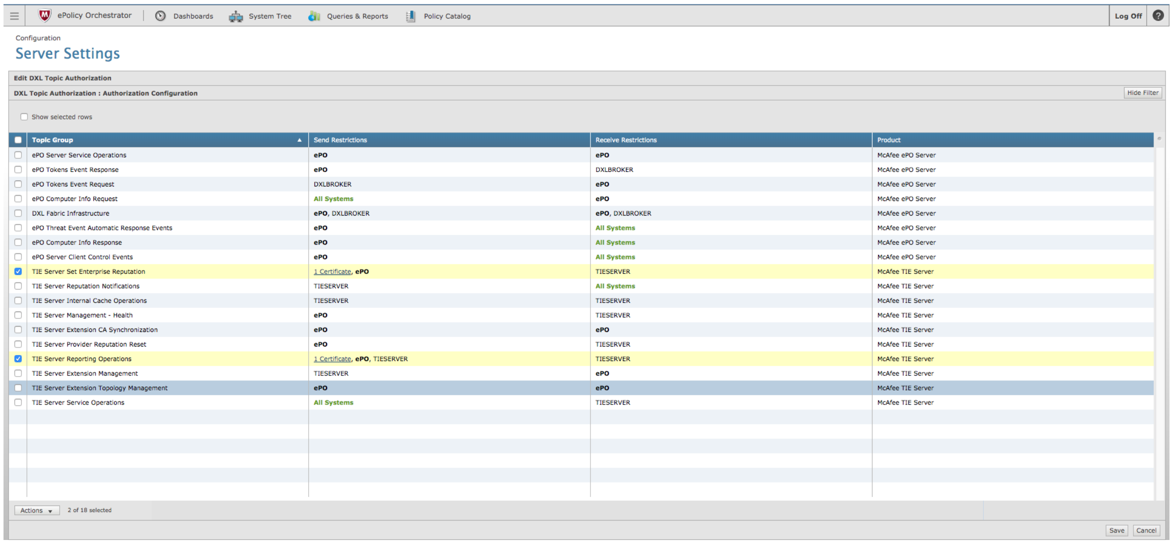
Restrict Send Certificates

☑ CN=threatq (5771589553037844450)

Certificate Details	
Name	CN=threatq (5771589553037844450)
Issuer DN	CN=OpenDXL_CA_EPO, OU=DXLBrokerMgmt, O=McAfee
Type	X.509
Signing Algorithm Name	SHA256withRSA
Issuer Alternative Names	
Thumbprint	c6b700d1c3c16294a020979bdd803b163513681a
Valid From	6/11/19 12:03:49 PM
Valid To	2/17/68 12:03:49 PM

7. Click **OK**.

8. Verify that the TIE Server Set Enterprise Reputation and TIE Server Reporting Operations now each have **1 certificate** listed within the **Send Restrictions** column.



Configuration

Server Settings

Edit DXL Topic Authorization

DXL Topic Authorization : Authorization Configuration

□ Show selected rows

□	Topic Group	Send Restrictions	Receive Restrictions	Product
□	ePO Server Service Operations	ePO	ePO	McAfee ePO Server
□	ePO Tokens Event Response	ePO	DXLBROKER	McAfee ePO Server
□	ePO Tokens Event Request	DXLBROKER	ePO	McAfee ePO Server
□	ePO Computer Info Request	All Systems	ePO	McAfee ePO Server
□	DXL Fabric Infrastructure	ePO, DXLBROKER	ePO, DXLBROKER	McAfee ePO Server
□	ePO Threat Event Automatic Response Events	ePO	All Systems	McAfee ePO Server
□	ePO Computer Info Response	ePO	All Systems	McAfee ePO Server
□	ePO Server Client Control Events	ePO	All Systems	McAfee ePO Server
☑	TIE Server Set Enterprise Reputation	1 Certificate, ePO	TIESERVER	McAfee TIE Server
□	TIE Server Reputation Notifications	TIESERVER	All Systems	McAfee TIE Server
□	TIE Server Internal Cache Operations	TIESERVER	TIESERVER	McAfee TIE Server
□	TIE Server Management - Health	ePO	TIESERVER	McAfee TIE Server
□	TIE Server Extension CA Synchronization	ePO	ePO	McAfee TIE Server
□	TIE Server Provider Reputation Reset	ePO	TIESERVER	McAfee TIE Server
☑	TIE Server Reporting Operations	1 Certificate, ePO, TIESERVER	TIESERVER	McAfee TIE Server
□	TIE Server Extension Management	TIESERVER	ePO	McAfee TIE Server
□	TIE Server Extension Topology Management	ePO	ePO	McAfee TIE Server
□	TIE Server Service Operations	All Systems	TIESERVER	McAfee TIE Server

2 of 18 selected

9. Click **Save** 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.

Invoking the Connector

The connector cannot be invoked until a directory containing the DXL configuration file is created by Provisioning the McAfee ePolicy Orchestrator (ePO)or by manually following the steps provided by the OpenDXL documentation.

You can invoke the connector command line utility as follows (all command line options are optional):

```
tq-mcafee-tie -ll <log_location_or_stdout> -c <tq_config_location> -x <mcafee_tie_cache_file_location> -dc <dxl_cert_dir_location> -cn <connector-name>
```

All location-based options default to the current working directory if they are not provided. To find additional options and option descriptions, simply invoke the program with `-h`.

The connector requires some setup before it can start communicating with ThreatQ and the McAfee DXL server:

1. Run the `tq-mcafee-tie` command line utility in order for it to create a ThreatQ configuration file and register itself to the ThreatQ server for you.
2. Login to the ThreatQ user interface.
3. Navigate to **Incoming Feeds > Labs**.
4. Click **Feed Settings** for the McAfee TIE connector.
5. Click the toggle button to the left of the McAfee TIE connector name. The connector name in the user interface will be `McAfee TIE-<connector-name>` if you passed a `-cn` option on the command line.

After the above is setup correctly, the next invocation of the `tq-mcafee-tie` (or `tq-mcafee-tie --cn <connector-name>`) command line utility will grab file hash indicators from ThreatQ based on the Daily Rate Limiting value in order to set their reputation level in the configured McAfee TIE server.

> If you have registered multiple connectors, you must ensure you are passing the appropriate connector name suffix via the `-cn` option when invoking the CLI command.

Connector Configuration

1. This connector provides the ability to specify a daily limit for the number of DXL set reputation requests made. By default, this limit is 1000. Valid values for the Daily Rate Limiting are 1-100000. 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.

2. ThreatQ scoring to McAfee TIE reputation mapping: This connector provides the ability to map ThreatQ scoring bands to specific McAfee TIE reputation values.

   ThreatQ supports the following scoring bands:

ThreatQ Scoring Band	Range
very low	0-4
low	5-6

ThreatQ Scoring Band	Range
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

By default, no options are selected for Known Malicious Reputation Mapping and Might Be Malicious Reputation Mapping. However, for Most Likely Malicious Reputation Mapping, all options are selected by default. To clear an item in a multi-select box, with the item under the cursor, press cmd + click or press ctrl + space.

3. This connector provides the ability to filter on which indicators to send to the McAfee TIE server.

   The following McAfee TIE connector user fields can be used for indicator filtering. All fields are optional.

Field	Description	Valid Values	Default Value
Number of Days	Filters by indicators added in the last N days	1-365	N/A
Filter by Indicator Status	Filter by indicators that have the provided indicator status name. Accepts only a single status name.	Indicator status names returned by GET /api/indicator/statuses	Active

Field	Description	Valid Values	Default Value
Filter by Indicator Score	Filters by indicators that have a score ≥ the provided score. An indicator's manual score has greater precedence than its generated score. A provided score of 0 is effectively the same as if this filter weren't applied at all.	0-10	N/A
Filter by Indicator Attributes	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. The user 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`	N/A	N/A

4. You can specify whether to automatically enrich indicators sent to McAfee with additional information from the McAfee ecosystem.

   The following attributes are created for each of McAfee ATD, McAfee GTI and the Enterprise (which in this case is ThreatQ).

Attribute	Possible Values	Description
ENTERPRISE Trust Level	See item three (3) in the Appendix.	Reputation of this hash as known by Enterprise
GTI Trust Level	See item three (3) in the Appendix.	Reputation of this hash as known by GTI
Prevalence	Boolean	True when the file was referenced by more than a configurable amount of end-points
Detection Count	Integer	N/A
Enterprise Count	Integer	N/A

*Only if the Intelligence Data Enrichment field is enabled in the ThreatQ feed settings.

Appendix

- `mcafee_tie_cache.json` - Cache utilized by the connector. The following key value pairs are recorded in the cache file:
  1. `indicators_sent`: The total number of indicators sent to McAfee TIE over a 24 hour period.
  2. `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.
  3. The values for `Trust Level` attribute can be as follows:
     - Reputation 1 -->Known Malicious
     - Reputation 15 --> Most Likely Malicious
     - Reputation 30 --> Might be Malicious
     - Reputation 50 --> Unknown
     - Reputation 70 --> Might be Trusted
     - Reputation 85 --> Most Likely Trusted
     - Reputation 99 --> Known Trusted
     - Reputation 0 --> Not Set
- `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.

Known Issues

- On MAC High Sierra, an existing bug that doesn't support libressl can cause the EPO provisioning tool `tq-mcafee-tie-prov` to fail with a message like: `Error initializing ctypes`. You can manually apply a patch as documented here: https://github.com/wbond/oscrypto/commit/83e2a06085b5b09ee5cd6c28a2ae1c52352c9e53
- By default, all options are selected for **Most Likely Malicious Reputation Mapping**. To clear an item in a multi-select box, with the item under the cursor, press cmd + click or press ctrl + space.

Change Log

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 multiselect and Boolean features.
- Querying indicators in the TIE server does not increase the sighting count.