

# ThreatQuotient



## McAfee TIE Reputation Change Connector Guide

Version 1.1.0

April 16, 2021

**ThreatQuotient**

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

### **Support**

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [support.threatq.com](http://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

    Configuring for Reboot ..... 8

Configuration..... 9

Usage..... 12

    Example ThreatQ Results ..... 13

Change Log..... 15

# Versioning

- Current integration version: 1.1.0
- Supported on ThreatQ versions  $\geq$  3.6.0

# Introduction


The McAfee TIE Reputation Change Connector for ThreatQ listens on the DXL fabric for changes in indicator reputation. Those new reputations will be updated in ThreatQ.

## Notes

- There are several additional steps to the installation process for this connector including DXL and reboot configurations. Review all steps in the [Installation](#) section.
- This connector runs as a service and does not require the use of a CRON job. You will be able to stop and start service using the commands found in the [Usage](#) section.

# 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-mcafee-tie-reputation-change
```

## Offline via tar.gz

To install the integration offline, the tar.gz will need to be copied via SCP into your ThreatQ instance.

- a. Run the following command:

```
sudo pip install tq-conn-mcafee-tie-reputation-change-1.1.0.tar.gz
```

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. DXL will now need to be configured so that you can read messages from topics. Run the following command



You can listen on multiple DXL fabrics by installing the connector with a suffix. Use the `-s` or `--suffix` CLI flags to specify a name to use for the integration. This suffix will be appended to the integration name (and attribute names).

```
tq-conn-mcafee-tie-reputation-change -v3 -c /etc/tq_labs/ -ll /var/log/tq_labs/ [--suffix NAME]
```



If you already have a DXL fabric configuration saved (from a different integration), you can re-use that directory by entering the directory path when prompted.

Running this command will install the integration for you by doing the following. You will need to fill out information on your ePO and ThreatQ instance:

- Creates a DXL configuration file and certificates.
- Installing the connector into the ThreatQ UI.
- Creates a service for the integration so the integration starts on reboot.

4. Enter the following parameters when prompted:

PARAMETER	DESCRIPTION
<b>ThreatQ Host</b>	This is the host of the ThreatQ instance, either the IP Address or Hostname as resolvable by ThreatQ.
<b>Client ID</b>	This is the OAuth id that can be found at Settings Gear → User Management → API details within the user's details.
<b>Email Address</b>	This is the User in the ThreatQ System for integrations.
<b>Password</b>	The password for the above ThreatQ account.
<b>Status</b>	This is the default status for objects that are created by this Integration. It is common to set this to "Review", but Organization SOPs should be respected when setting this.

### Example Output

```
tq-conn-mcafee-tie-reputation-change -v3 -ll /var/log/tq_labs/ -c /etc/tq_labs/  
ThreatQ Host: <ThreatQ Host IP or Hostname>  
Client ID: <ClientID>  
E-Mail Address: <EMAIL ADDRESS>  
Password: <PASSWORD>  
Status: Review  
Connector configured. Set information in UI
```

# Configuring for Reboot

You will now need to setup a service so that the integration is always-on and listening for changes.

1. Create the service file (replacing <suffix> if you are using one):

```
sudo vi /etc/systemd/system/mcafee_tie_reputation_change_<suffix>.service
```

2. Paste the following configuration into the service file (replacing suffix> if you are using one)

```
[Unit]
Description=ThreatQ integration listening for changes on the DXL fabric
After=httpd.service
Requires=httpd.service
[Service] Type=simple
RemainAfterExit=yes
KillMode=none
ExecStart=/usr/bin/tq-conn-mcafee-tie-reputation-change
-c /etc/tq_labs/ -ll /var/log/tq_labs/ -v3 --suffix <suffix>
Restart=always
RestartSec=60
[Install]
WantedBy=multi-user.target
```

3. Give the service file execution privileges (replacing suffix> if you are using one):

```
sudo chmod 664 /etc/systemd/system/mcafee_tie_reputation_change_<suffix>.service
```

4. Reload the system daemons and enable the service (replacing suffix> if you are using one):

```
sudo systemctl daemon-reload
```

```
sudo systemctl enable mcafee_tie_reputation_change_<suffix>.service
```

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
Enterprise Reputations	<p>Select the Enterprise reputations to listen for with the connector. By default, the connector only listens for malicious reputations.</p> <p>Options include:</p> <ul style="list-style-type: none"><li>◦ Not Set</li><li>◦ Known Malicious (Default)</li><li>◦ Most Likely Malicious (Default)</li><li>◦ Might be Malicious (Default)</li><li>◦ Unknown</li><li>◦ Might be Trusted</li><li>◦ Most Likely Trusted</li><li>◦ Known Trusted</li><li>◦ Known Trusted Installer</li></ul>

PARAMETER	DESCRIPTION
<b>GTI Reputations</b>	<p>Select the Global Threat Intelligence reputations to listen for with the connector. By default, the connector only listens for all identified reputations.</p> <p>Options include:</p> <ul style="list-style-type: none"><li>◦ Not Set</li><li>◦ Known Malicious (Default)</li><li>◦ Most Likely Malicious (Default)</li><li>◦ Might be Malicious (Default)</li><li>◦ Unknown</li><li>◦ Might be Trusted</li><li>◦ Most Likely Trusted</li><li>◦ Known Trusted</li><li>◦ Known Trusted Installer</li></ul>
<b>Advanced Threat Defense Reputations</b>	<p>Select the Advanced Threat Defense reputations to listen for with the connector. By default, the connector only listens for malicious reputations.</p> <p>Options include:</p> <ul style="list-style-type: none"><li>◦ Not Set</li><li>◦ Known Malicious (Default)</li><li>◦ Most Likely Malicious (Default)</li><li>◦ Might be Malicious (Default)</li><li>◦ Unknown</li><li>◦ Might be Trusted</li><li>◦ Most Likely Trusted</li><li>◦ Known Trusted</li><li>◦ Known Trusted Installer</li></ul>
<b>Use TIE 2.1.1+ Mapping</b>	<p>Use the checkbox to select to use TIE 2.1.1+ ATD mapping. See <a href="https://kc.mcafee.com/corporate/index?page=content&amp;id=KB84600">https://kc.mcafee.com/corporate/index?page=content&amp;id=KB84600</a> for more details.</p>

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

# Usage

After running through the installation, the connector will be running as a service. It will not need to have a CRON-job configured. You will be able to start/stop/restart the service just like any other service on CentOS/Red Hat.

## Start Service

```
systemctl start mcafee_tie_reputation_change_<suffix>
```

## Restart Service

```
systemctl restart mcafee_tie_reputation_change_<suffix>
```

## Stop Service

```
systemctl stop mcafee_tie_reputation_change_<suffix>
```

You will also be able to view the logs using Journal CTL.



This command will "follow" the logs and update with any new incoming logs.

```
journalctl -u mcafee_tie_reputation_change_<suffix> -f
```

# Example ThreatQ Results

The following are examples that show how the data will be presented, when reputations have changed, in the ThreatQ platform.

## Example 1

The screenshot displays the ThreatQ interface for an indicator. The top navigation bar includes 'Threat Library', 'Investigations', and 'Analytics'. The indicator's ID is '53e7818237e056f5893954b4da15db622bd3bfd37c43403d8bd25e2750' with a sub-ID '85dedf'. The indicator type is 'INDICATOR: SHA-256'. The score is '0 - Very Low' and the status is 'Review'. The indicator was created on 07/30/2019, first seen on 07/30/2019 at 08:07pm, and expires on an addable date. A sidebar on the left shows 'Context' with 'Attributes (3)', 'Sources (1)', 'Tags (0)', 'Description (0)', 'Relationships', 'Indicators (2)', 'Comments (0)', 'Operations', and 'Audit Log'. The main content area shows 'Attributes (3)' with a table of attributes and their values, and 'Sources (1)' with a single source.

ATTRIBUTE TYPE	ATTRIBUTE VALUE	SOURCES	DATE CREATED
Enterprise First Execution (FIRST_CONTACT) - test	1564517184	McAfee TIE Reputation Change-test	07/31/2019 02:13pm
Enterprise Executions (PREVALENCE) - test	0	McAfee TIE Reputation Change-test	07/31/2019 02:13pm
ENTERPRISE Trust Level - test	Most Likely Malicious	McAfee TIE Reputation Change-test	07/31/2019 02:11pm

Sources (1)
McAfee TIE Reputation Change-test


## Example 2

THREATQ

Threat LibraryInvestigationsAnalytics

+ Create

CG

 **8aea2ae91cc084731a08aa231e79a430** [Edit](#)

INDICATOR: MD5

SCORE: 0 - Very Low [?](#) STATUS: Active

Created: 07/23/2019 First Seen: 06/26/2019 11:48am Expires: [add date](#) [Add to Watchlist](#)

Actions

Context

Attributes (4)

Sources (2)

Tags (0)

Description (0)

Relationships

Events (3)

Comments (0)

Operations

Audit Log

Attributes (4)

AddDelete

ATTRIBUTE TYPE	ATTRIBUTE VALUE	SOURCES	DATE CREATED
<input type="checkbox"/> Enterprise First Execution (FIRST_CONTACT) - test	1562154379	McAfee TIE Reputation Change-test x	07/31/2019 02:16pm
<input type="checkbox"/> Enterprise Executions (PREVALENCE) - test	0	McAfee TIE Reputation Change-test x	07/31/2019 02:16pm
<input type="checkbox"/> ENTERPRISE Trust Level - test	Known Malicious	McAfee TIE Reputation Change-test x	07/31/2019 02:16pm
<input type="checkbox"/> GTI Trust Level - test	Known Malicious	McAfee TIE Reputation Change-test x	07/31/2019 02:15pm

Sources (2)

Add

AllenVault OTX PulseMcAfee TIE Reputation Change-test

# Change Log

- **Version 1.1.0**
  - Fixed an issue where the ATD Verdict was extracted in the wrong format.
- **Version 1.0.0**
  - Initial Release