

ThreatQuotient



McAfee TIE Reputation Change for ThreatQuotient

Version 1.0.0

Wednesday, May 6, 2020

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 © 2020 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.

Last Updated: Wednesday, May 6, 2020

Contents

McAfee TIE Reputation Change for ThreatQuotient	1
Warning and Disclaimer	2
Contents	3
Introduction	5
Preface	5
Audience	5
Scope	5
Versioning	5
Implementation Overview	7
Prerequisites	7
Security and Privacy	8
Installation	9
From The ThreatQuotient Repository	9
Offline From the .whl File	10
Creating Integration Directories	12
Configuring for Reboot	14
Usage	15
Configuration	17

Example ThreatQ Results	21
Trademarks and Disclaimers	22

Introduction

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

Preface

This guide is to provide the information necessary to implement the McAfee TIE Reputation Change for ThreatQuotient. This document is not specifically intended to form a site reference guide. It is assumed that the implementation engineer has experience installing and commissioning ThreatQuotient Apps and integrations covered within the document, as well as experience necessary to troubleshoot at a basic level.

Audience

This document is intended for use by the following parties:

1. ThreatQ and Security engineers.
2. ThreatQuotient Professional Services Project Team & Engineers.

Scope

This document covers the implementation of the McAfee TIE Reputation Change for ThreatQuotient only.

Versioning

Software/App	Version
ThreatQ	v3.6 or greater

Software/App	Version
McAfee TIE Reputation Change for ThreatQuotient	v1.0.0

Implementation Overview

This document will direct a ThreatQ administrator on how to install the McAfee TIE Reputation Change for ThreatQuotient.

Prerequisites

Throughout this implementation document, there will be referrals to several files and directories, some of which will be symbolic, and others may change depend on specifics of the environmental setup.

Ensure all ThreatQ devices are set to the correct time (UTC is recommended), time zone and date, 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, to list all available time zones in Europe, type:

Time Zone List Example

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

To change the time zone to UTC, type as root:

Time Zone Change Example

```
timedatectl set-timezone UTC
```

Security and Privacy

For ThreatQuotient Professional Services engineers to configure the system, local network access is required to connect to the managed estate. Therefore, the implementation must occur at an office or data center location.

Passwords have not been provided in this document. Please contact your project team for this information, if required or applicable.

All engineers are reminded that all data belonging and pertaining to the business is confidential and should not be disclosed to any unauthorized parties.

The data held within this document is classed as confidential due to its nature.

Installation

Follow the steps below to install the McAfee TIE Reputation Change for ThreatQuotient connector. You have two options for installing the connector:

- [Install from the ThreatQuotient Repository](#)
- [Install Offline from the .whl File](#)

After installing the connector, you will then need to [create integration directories](#) and [set up a service](#) so that the connector is always listening.

From The ThreatQuotient Repository

To install this McAfee TIE Reputation Change for ThreatQuotient from the ThreatQuotient repository with YUM credentials:

1. Install the McAfee TIE Reputation Change for ThreatQuotient by issuing the following command:

```
pip install tq-conn-mcafee-tie-reputation-  
change
```

Example Output

```
pip install tq-conn-mcafee-tie-reputation-  
change Collecting tq-conn-mcafee-tie-  
reputation-change  
  Downloading  
https://extensions.threatq.com/threatq/integrat  
ions-dev/+f/e7b/7112897638161/tq-conn-mcafee-
```

```
tie-reputation-change-1.0.0-py2-none-any.whl
Requirement already satisfied: jinja2==2.8 in
/usr/lib/python2.7/site-packages (from
threatqcc>=1.3.0-> tq-conn-mcafee-tie-
reputation-change) (2.8) Collecting
pyasn1>=0.3.7 (from python-ldap==3.2.0-> tq-
conn-mcafee-tie-reputation-change)
  Downloading
https://extensions.threatq.com/root/pypi/+f/da6
/b43a8c9ae93bc/pyasn1-0.4.5-py2.py3-none-
any.whl (73kB)
  100% |████████████████████████████████████████| 81kB
1.0MB/s
Collecting pyasn1_modules>=0.1.5 (from python-
ldap==3.2.0-> tq-conn-mcafee-tie-reputation-
change)
  Downloading
  Running setup.py install for python-ldap ...
done
Successfully installed pyasn1-0.4.5 pyasn1-
modules-0.2.5 python-ldap-3.2.0 tq-conn-mcafee-
tie-reputation-change 1.0.0
```

Offline From the .whl File

To install this McAfee TIE Reputation Change for ThreatQuotient from a wheel file, the wheel file (.whl) file **tq_conn_mcafee_tie_reputation_change-<version>-py2-none-any.whl** will need to be copied via SCP into your ThreatQ instance.

1. Install the .whl file issuing the following command:

```
sudo pip install tq_conn_mcafee_tie_reputation_
change-<version>-py2-none-any.whl
```

Output Example:

```
sudo pip install tq_conn_mcafee_tie_reputation_
change-<version>-py2-none-any.whl
Requirement already satisfied (use --upgrade to
upgrade): urllib3<1.25,>=1.21.1 in
/usr/lib/python2.7/site-packages (from
requests>=2.9.1->threatqsdk>=1.6.7-> tq-conn-
mcafee-tie-reputation-change)
Requirement already satisfied (use --upgrade to
upgrade): chardet<3.1.0,>=3.0.2 in
/usr/lib/python2.7/site-packages (from
requests>=2.9.1->threatqsdk>=1.6.7-> tq-conn-
mcafee-tie-reputation-change)
Requirement already satisfied (use --upgrade to
upgrade): idna<2.9,>=2.5 in
/usr/lib/python2.7/site-packages (from
requests>=2.9.1->threatqsdk>=1.6.7->tq-conn-
mcafee-tie-reputation-change)
Installing collected packages: tq-conn-mcafee-
tie-reputation-change
Successfully installed tq-conn-mcafee-tie-
reputation-change-1.0.0
```

Creating Integration Directories



If you are using multiple DXL fabrics and want to listen on all of them, you can setup multiple instances of this integration by specifying a suffix for the integration. To specify a suffix for the integration, run the previously described command with the “-s” or “--suffix” CLI parameter. See the example provided below.

```
tq-conn-mcafee-tie-reputation-change -v 3 -ll  
/opt/tq-integrations/mcafee-tie-reputation-change/  
-c /opt/tq-integrations/mcafee-tie-reputation-  
change/ --suffix siteA
```

Once the application has been installed, A directory structure must be created.



If the integration is to be installed more than once, each installation should have its own directory.

1. Run the following command:

```
mkdir -p /opt/tq-integrations/mcafee-tie-  
reputation-change
```

A driver which will be called **tq-conn-mcafee-tie-reputation-change** is installed.

2. Issue the following command to initialize the integration:

```
tq-conn-mcafee-tie-reputation-change -v 3 -ll  
/opt/tq-integrations/mcafee-tie-reputation-  
change/ -c /opt/tq-integrations/mcafee-tie-  
reputation-change/
```

You will asked the following questions:

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

Output Example:

```
tq-conn-mcafee-tie-reputation-change -v 3 -ll
/opt/tq-integrations/mcafee-tie-reputation-
change/ -c /opt/tq-integrations/mcafee-tie-
reputation-change/
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
```

The driver will run once, where it will connect to the TQ instance and install the UI component of the Connector.

Configuring for Reboot

Once the integration is installed (via pip), you will 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 /opt/tq-integrations/tie-  
site-a/ -ll /opt/tq-integrations/tie-site-a/ -  
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
```

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 tq-conn-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 will "follow" the logs and update with any new logs coming in.

```
journalctl -u mcafee-tie-reputation-change-<suffix>  
-f
```

Configuration



ThreatQuotient does not issue credentials for third-party vendors. Contact the specific vendor to obtain connector-related credentials.

To configure the connector:

1. Click on the **Settings** icon and select **Incoming Feeds**.
2. Locate the feed under the **Labs** tab.
3. Click on the **Feed Settings** link for the feed.
4. Under the **Connection** tab, enter the following configuration parameters:

Parameter	Description
ePO Host-name or IP Address	Enter the hostname or IP address for your McAfee ePO instance. This can be left blank if you are using a pre-generated (custom) certificate.
DXL Registration Port	Enter the DXL fabric port you want to register this service on. This field defaults to 8443. Do not change this unless you have changed the default DXL port.
ePO User-name	Enter your username to authenticate with McAfee ePO. This can be left blank if you are using a pre-generated (custom) certificate.
ePO Password	Enter your password to authenticate with McAfee ePO. This can be left blank if you are using a pre-generated (custom) certificate.
Enterprise Reputations:	Listen for these Enterprise reputations. By default, we only listen for malicious reputations Choices: <ul style="list-style-type: none">• Note Set• Known Malicious (Default)

Parameter	Description
	<ul style="list-style-type: none">• Most Likely Malicious (Default)• Might be Malicious (Default)• Unknown• Might be Trusted• Most Likely Trusted• Known Trusted• Known Trusted Installer
GTI Repu- tations:	<p>Listens for these Global Threat Intelligence reputations. By default, we listen for all identified reputations Choices:</p> <ul style="list-style-type: none">• Note Set• Known Malicious (Default)• Most Likely Malicious (Default)• Might be Malicious (Default)• Unknown• Might be Trusted• Most Likely Trusted• Known Trusted• Known Trusted Installer
Advanced Threat Defense Reputations	<p>Listens for these Advanced Threat Defense Reputations Choices:</p> <ul style="list-style-type: none">• Note Set• Known Malicious (Default)• Most Likely Malicious (Default)• Might be Malicious (Default)

Parameter	Description
	<ul style="list-style-type: none">• Unknown• Might be Trusted• Most Likely Trusted• Known Trusted• Known Trusted Installer
Use TIE 2.1.1+ mapping:	Choose whether or not to use the TIE 2.1.1+ ATD mapping. Please refer to: https://kc.mcafee.com/corporate/index?page=content&id=KB84600 for more details.
Custom Certificate Directory (Optional)	If you have pre-generated a certificate, or want to use a certificate directory that you've already created, enter the absolute path here. A new certificate will not be generated. This field is optional. If you do not enter a path, a new certificate will be generated using your ePO credentials.

McAfee TIE Reputation Change Feed Settings

Connection Settings

vPO Hostname or IP Address
ego.flolan
Enter the hostname or IP address for your McAfee vPO instance. If you are using pre-generated certificates, this is optional.

DRL Registration Port
8443
Enter the port used to register with DRL. If you are using pre-generated certificates, this is optional. Default: 8443.

vPO Username
admin
Enter your username to authenticate with the McAfee vPO instance. If you are using pre-generated certificates, this is optional.

Password
xxxxxxxx
Enter your password to authenticate with the McAfee vPO instance. If you are using pre-generated certificates, this is optional.

Enterprise Reputation
Not Set
Known Malicious
Most Likely Malicious
Might be Malicious
Listen for these Enterprise Reputation. By default, we only listen for malicious reputations.

GTI Reputation
Not Set
Known Malicious
Most Likely Malicious
Might be Malicious
Listen for these Global Threat Intelligence Reputation. By default, we listen for all identified reputations.

Advanced Threat Defense Reputation
Not Set
Known Malicious
Most Likely Malicious
Might be Malicious
Listen for these Advanced Threat Defense Reputation.

☒ Use TIE 2.1.1+ mapping
Choose whether or not to use the TIE 2.1.1+ ATD mapping. Please see <https://mc.mcafee.com/corporate/index?page=content&id=688400> for more details.

Custom Certificate Directory (Optional)
If you would like to install certificates into a specific directory or pre-generated certificates you want to use, enter the absolute path to the directory here.

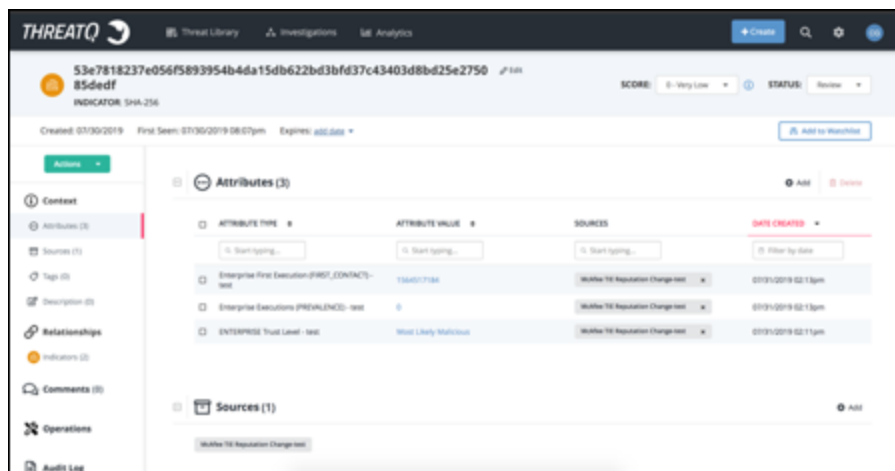
Save Changes

5. Click on **Save Changes**.
6. Click on the toggle switch to the left of the connector name to enable the connector.

Example ThreatQ Results

The screenshots below are examples of ThreatQ results. See the [ThreatQuotient Help Center](#) for further reference.

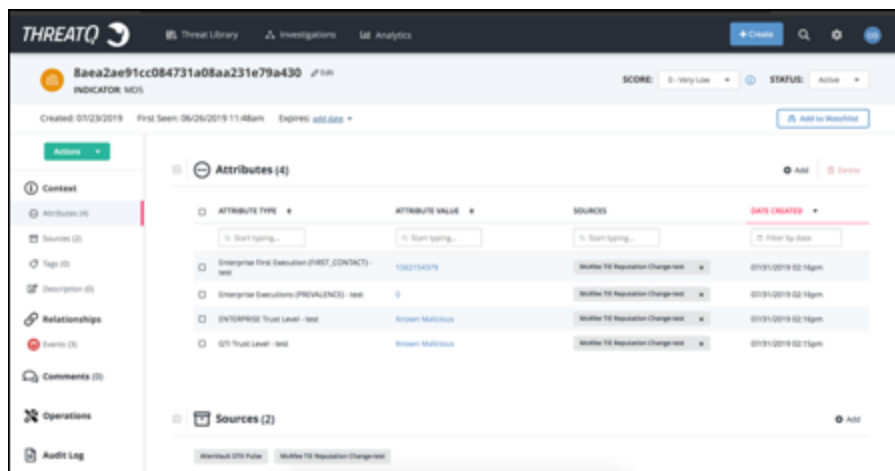
Example 1



The screenshot shows the ThreatQ interface for an indicator with SHA-256 hash 53e7818237e056f5893954b46a15db622bd3bfd37c43403d8bd25e2750. The indicator is labeled "INDICATOR: SHA-256" and has a score of "0 - Very Low" and a status of "Review". It was created on 07/30/2019 and expires on 08/07/2019. The interface displays a list of attributes and sources.

ATTRIBUTE TYPE	ATTRIBUTE VALUE	SOURCES	DATE CREATED
Enterprise First Execution (FIRST_CONTACT)-test	1564077186	McAfee TIE Reputation Change test	01/31/2019 02:13pm
Enterprise Executions (PREVALENCE)-test	0	McAfee TIE Reputation Change test	01/31/2019 02:13pm
ENTERPRISE Trust Level -test	Most Likely Malicious	McAfee TIE Reputation Change test	01/31/2019 02:13pm

Example 2



The screenshot shows the ThreatQ interface for an indicator with MD5 hash 8aea2ae91cc084731a08aa231e79a430. The indicator is labeled "INDICATOR: MD5" and has a score of "0 - Very Low" and a status of "Active". It was created on 07/23/2019 and expires on 08/26/2019. The interface displays a list of attributes and sources.

ATTRIBUTE TYPE	ATTRIBUTE VALUE	SOURCES	DATE CREATED
Enterprise First Execution (FIRST_CONTACT)-test	1562154079	McAfee TIE Reputation Change test	01/31/2019 02:16pm
Enterprise Executions (PREVALENCE)-test	0	McAfee TIE Reputation Change test	01/31/2019 02:16pm
ENTERPRISE Trust Level -test	Known Malicious	McAfee TIE Reputation Change test	01/31/2019 02:16pm
QTY Trust Level -test	Known Malicious	McAfee TIE Reputation Change test	01/31/2019 02:16pm

Trademarks and Disclaimers

THE SUBJECT AND SPECIFICATIONS INCLUDING ALL INFORMATION REGARDING THE PRODUCTS IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE AT THE TIME OF WRITING BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE TERMS AND CONDITIONS WHEN PURCHASED. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR THREATQUOTIENT REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THIRD PARTY SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. THREATQUOTIENT AND THIRD-PARTY SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL THREATQUOTIENT OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF THREATQUOTIENT OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

It is wholly the customers responsibility for any design requirements and the utilization of any recommendations provided by ThreatQuotient. ThreatQuotient recommendations are based upon customer information provided to ThreatQuotient at the time of the services. ThreatQuotient shall not be liable for the accuracy or completeness of the customer information contained in the ThreatQuotient recommendations.

All documentation and deliverables shall be provided in the English language, unless specifically stated otherwise. or agreed before the commencement of any services in writing. Any costs incurred by ThreatQuotient as a result of translations requested by Customer shall be Customer’s responsibility.

In the event of any conflict between this English version and the translation(s), the English version will prevail.

ThreatQuotient and the ThreatQuotient Rhino Logo are trademarks of ThreatQuotient, Inc.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

©2020 ThreatQuotient, Inc. All rights reserved.