

McAfee TIE Operation Implementation Guide

Version 1.0.0

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 © 2018 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.

ThreatQuotient and McAfee are trademarks of their respective companies.

Last Updated: Thursday, November 1, 2018

Contents

McAfee TIE Operation Implementation Guide	1
Warning and Disclaimer	2
Contents	4
Introduction	5
Actions	5
Query Reputation	6
Set Reputation	7
Operation Configuration	9
Operation Installation	9

Introduction

The McAfee TIE operation has get and set actions. The get action queries the configured TIE server for any threat information for the indicator in question. The set operation sets the Enterprise Threat Level of the indicator in question on the McAfee TIE server.

This integration requires:

- ThreatQ version 4.11 or higher

Actions

Action	Description	Object Type
Query Reputation	Query a McAfee TIE server for additional attributes relevant to certain indicators	Indicator
Set Reputation Might Be Malicious	Set the Enterprise reputation for an indicator	Indicator
Set Reputation Most Likely Malicious	Set the Enterprise reputation for an indicator	Indicator
Set Reputation Unknown	Set the Enterprise reputation for an indicator	Indicator
Set Reputation Known Malicious	Set the Enterprise reputation for an indicator	Indicator

Action	Description	Object Type
Set Reputation Known Trusted	Set the Enterprise reputation for an indicator	Indicator

Query Reputation

The following indicator types in ThreatQ can run this operation currently:

- MD5
- SHA-1
- SHA-256

This operation will create up to 12 attributes for an indicator depending upon how much information the McAfee ecosystem has about this indicator. The table below summarizes these 12 attributes. Each cell in the table represents the attribute name in ThreatQ.

McAfee Source	Reputation	Created At	Count	Prevalence
Global Threat Intelligence (GTI)	Global Threat Intelligence Trust Level	Global Threat Intelligence Created At	Global Threat Intelligence Count	Global Threat Intelligence Prevalence
Advanced Threat Defense (ATD)	Advanced Threat Defense Trust Level	Advanced Threat Defense Created At	Advanced Threat Defense Count	Advanced Threat Defense Prevalence

McAfee Source	Reputation	Created At	Count	Prevalence
Enterprise	Enterprise Reputation	Enterprise Created At	Enterprise Count	Enterprise Prevalence

The reputation attribute values are created from the mapping given in the table below.

McAfee Reputation Score	ThreatQ Trust Level Attribute Value
0	Not Set
1	Known Malicious
15	Most Likely Malicious
30	Might Be Malicious
50	Unknown
70	Might Be Trusted
85	Most Likely Trusted
100	Known Trusted

Set Reputation


This operation allows the user to set the Enterprise reputation 'trust level' in the McAfee TIE Database for the following indicator types in ThreatQ:

- MD5
- SHA-1
- SHA-256

The reputation attribute values are created from the mapping given in the table below.

McAfee Reputation Score	ThreatQ Trust Level Attribute Value
1	Known Malicious
15	Most Likely Malicious
30	Might Be Malicious
50	Unknown
100	Known Trusted

OPERATIONS



McAfee TIE: Query Reputation

McAfee TIE: Set Reputation
Might Be Malicious

McAfee TIE: Set Reputation
Most Likely Malicious

McAfee TIE: Set Reputation
Unknown

McAfee TIE: Set Reputation
Known Malicious

McAfee TIE

Output from operation: Successfully set a new Enterprise Reputation in the McAfee TIE Database.

Operation Configuration

This operation requires a signed certificate for communication with the McAfee DXL server. Currently, the operation will use the McAfee EPO to generate this certificate (meaning, the operation will not work with a signed certificate generated outside of this program). To be able to generate the certificate, the operation will require input arguments as shown below.



The screenshot shows a web-based configuration interface for the McAfee ThreatQ operation. At the top left is the McAfee logo. To its right, the text reads: "Author: ThreatQ", "Version: 1.0.0", "Required ThreatQ Version: 2.1", and "Works with: Indicator". Below this is a checkbox labeled "Bypass system proxy configuration for this operation". In the top right corner is a red button labeled "Delete Operation". The main area contains four input fields: "EPO IP", "EPO Login", "EPO Password" (with a toggle for visibility), and "EPO Port". At the bottom left is a green button labeled "Save Changes".

The parameter description is as below:

- **EPO IP:** The IP Address of the McAfee EPO server.
- **EPO Login:** EPO Login
- **EPO Password:** EPO Password
- **EPO Port:** This field is optional. If left blank, the default port, **8443**, is used.

Operation Installation

Using the `whl` file, this operation can either be installed via the user interface by navigating to **Operations Management** and clicking **Install Operation**.

Another way to install the operation is to use the `tq_plugin` command on the CLI as follows (make sure to run as `apache` user as shown):

```
sudo -u apache /opt/threatq/python/bin/tq-plugin  
install mcafee_tie-1.0.0-py3-none-any.whl
```

```
sudo -u apache php /var/www/api/artisan threatq:plu-  
gin-sync
```