ThreatQuotient

Trellix TIE Reputation Change Connector

Version 1.2.0 rev-b

January 06, 2025

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	1.2.0
Compatible with ThreatQ Versions	>= 4.56.0
Python Version	3.6
Support Tier	ThreatQ Supported

Introduction

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

Prerequisites

Review the following requirements before attempting to install the connector.

Time Zone

> ⚠ The time zone steps are for ThreatQ v5 only. ThreatQ v6 users should skip these steps.

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
```

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
threatqsdk	>= 1.8.7	N/A
threatqcc	>= 1.4.2	N/A
requests	>= 2.25.1	N/A
asn1crypto	>= 1.5.1	N/A
dxlclient	>= 5.6.0.4	N/A
dxltieclient	>= 0.3.0	N/A

Installation

> **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.

ThreatQ v6 Process

1. Download the connector integration file from the ThreatQ Marketplace.
2. Transfer the connector whl file to the `/tmp/` directory on your instance.
3. SSH into your instance.
4. Move the connector whl file from its `/tmp/` location to the following directory: `/opt/tqvenv`
5. Navigate to the custom connector container:

```
kubectl exec -n threatq -it deployments/custom-connectors -- /bin/bash
```

6. Create your python 3 virtual environment:

```
python3.6 -m venv /opt/tqvenv/<environment_name>
```

7. Active the new environment:

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

8. Run the pip upgrade command:

```
pip install --upgrade pip
```

9. Install the required dependencies:

```
pip install threatqsdk threatqcc setuptools==59.6.0
```

10. Install the connector:

```
pip install /opt/tqvenv/tq_conn_trellix_tie_reputation_change-
<version>-py3-none-any.whl
```

11. Perform an initial run of the connector:

```
/opt/tqvenv/<environment_name>/bin/
tq_conn_trellix_tie_reputation_change
```

12. Enter the following parameters when prompted:

PARAMETER	DESCRIPTION
ThreatQ Host	**Leave this field blank as it will be set dynamically.**
ThreatQ Client ID	This is the OAuth id that can be found at Settings Gear → User Management → API details within the user's details.
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-trellix-tie-reputation-change
ThreatQ Host:
ThreatQ Client ID: <ClientID>
ThreatQ Username: <EMAIL ADDRESS>
ThreatQ Password: <PASSWORD>
Status: Review
Connector configured. Set information in UI
```

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

ThreatQ v5 Process

1. Navigate to the ThreatQ Marketplace and download the .whl file for the integration.
2. Create the following directory:

   ```
   mkdir /opt/tqvenv/
   ```

3. Install python 3.6:

   ```
   sudo yum install -y python36 python36-libs python36-devel python36-pip
   ```

4. Create a virtual environment:

   ```
   python3.6 -m venv /opt/tqvenv/<environment_name>
   ```

5. Activate the virtual environment:

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

6. Run the pip upgrade command:

```
pip install --upgrade pip
```

7. Install the required dependencies:

```
pip install threatqsdk threatqcc setuptools==59.6.0
```

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

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

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

10. 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/
```

11. Perform an initial run using the following command:

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

12. 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.
ThreatQ Username	This is the Email Address of the user in the ThreatQ System for integrations.

PARAMETER	DESCRIPTION
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-trellix-tie-reputation-change
-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
```

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

PARAMETER	DESCRIPTION
ePO hostname or IP Address	Enter the Hostname or IP Address for your Trellix ePO instance.
DXL Registration Port	Enter the Port used to register with DXL. The defaults is 8443.
ePO Username	Username to authenticate with the Trellix ePO instance.
ePO Password	Password to authenticate with the Trellix ePO instance.
Enterprise Reputations	Select the Enterprise reputations to listen for with the connector. By default, the connector only listens for malicious reputations. Options include: ◦ Not Set ◦ Known Malicious (Default) ◦ Most Likely Malicious (Default) ◦ Might be Malicious (Default) ◦ Unknown ◦ Might be Trusted ◦ Most Likely Trusted ◦ Known Trusted ◦ Known Trusted Installer
GTI Reputations	Select the Global Threat Intelligence reputations to listen for with the connector. By default, the connector only listens for all identified reputations.

PARAMETER	DESCRIPTION
	Options include: ◦ Not 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	Select the Advanced Threat Defense reputations to listen for with the connector. By default, the connector only listens for malicious reputations. Options include: ◦ Not Set ◦ Known Malicious (Default) ◦ Most Likely Malicious (Default) ◦ Might be Malicious (Default) ◦ Unknown ◦ Might be Trusted ◦ Most Likely Trusted ◦ Known Trusted ◦ Known Trusted Installer
Use TIE 2.1.1+ Mapping	Use the checkbox to select to use TIE 2.1.1+ ATD mapping. See https://kcm.trellix.com/corporate/index?page=content&id=KB84600 for more details.
Custom Certificate Directory	Enter the absolute pathway for the directory where any certificates will be installed. ⚠ This parameter is **required** for ThreatQ v6 users. This must be a subdirectory of `/opt/tqvenv`. **Example**: `/opt/tqvenv/tie-reputation-certs`. This parameter is **optional** for ThreatQ v5 users.

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.

Usage

ThreatQ v6 Driver Command

```
/opt/tqvenv/<environment_name>/bin/tq-conn-trellix-tie-reputation
```

ThreatQ v5 Driver Command

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

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.
`-n, --name`	Optional - the name of the connector (Option used in order to allow users to configure multiple connector instances on the same TQ box).

ARGUMENT	DESCRIPTION
`-hist, --historical {DATE}`	Optional - allows you to set the start date for the Threat Library search.

Accessing Connector Logs

ThreatQ v6

ThreatQ version 6 aggregates the logs for all custom connectors to its output container. You can access the container's log using the following command:

```
kubectl logs -n threatq deployments/custom-connectors
```

ThreatQ v5

The connector log directory was created in 10 of the installation process and is identified using the `-ll` argument flag when executing the driver.

Accessing Connector Configuration

ThreatQ v6

The custom connector configuration file can be found in the following directory: `/etc/tq_labs/`.

ThreatQ v5

The custom connector configuration file was created in step 10 of the install process and identified using the `-c` argument flag when executing the driver.

Change Log

- **Version 1.2.0 rev-b**
  - Guide Update - added ThreatQ v6 documentation.
- **Version 1.2.0 rev-a**
  - Guide Update - removed CRON section of the guide as it does not apply to this connector.
- **Version 1.2.0**
  - Replaced python 2 version with python 3.
  - Updated minimum ThreatQ version to 4.56.0
  - Rebranded integration to Trellix TIE Reputation Change Connector.
- **Version 1.1.0**
  - Fixed an issue where the ATD Verdict was extracted in the wrong format.
- **Version 1.0.0**
  - Initial Release