# ThreatQuotient

# Maltego TRX for ThreatQ User Guide

## Version 2.0.0

July 11, 2023

**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** | 2.0.0 |
| **Compatible with ThreatQ Versions** | >= 5.6.0 |
| **Python Version** | 3.6 |
| **Third-Party Application** | Maltego Desktop Application |
| **Support Tier** | ThreatQ Supported |

# Introduction

The Maltego TRX for ThreatQ is a transforms library enabling bi-directional communication between ThreatQ and Maltego and enables analysts to have more visibility into their threat intelligence knowledgebase, via ThreatQ. The included transforms allow an analyst to perform contextual lookups for IOCs and other object types. This includes relationships, tags, attributes, and more.

The library comes with over 500 transforms allowing you to interact with all sorts of IOC types within the Maltego, as well as custom entity types representing custom objects within ThreatQ. In addition, analysts will be able to interact with certain entities from the official STIX2 plugin.

> The Maltego TRX for ThreatQ integration replaces the Maltego Transforms for ThreatQ (mac and windows) integrations.

# Prerequisites

The following is required by the integration:

- Maltego Desktop Application (free) installed on your local machine. This application can be downloaded from https://www.maltego.com/downloads/.
- A python 3 environment installed on your local host.
- The Maltego and ThreatQ SDKs installed on your local host.

## Installing Python 3 Environment

You must first install Python 3 onto your host machine. This can be done in various ways, depending on your operating system. The following links will provide you with the steps based on your operating system:

- **Windows**: https://docs.python-guide.org/starting/install3/win/
- **Linux**: https://docs.python-guide.org/starting/install3/linux/
- **macOS**: https://docs.python-guide.org/starting/install3/osx/

Continue on to installing the required SDKs once you have installed and activated your python 3 environment.

## Installing Maltego and ThreatQ SDKs

After you have installed and activated your python 3 environment, proceed with installing the required SDKs.

1. Install the Maltego SDK:

```
pip install maltego-trx
```

2. Install the ThreatQ SDK via the ThreatQ download repository:

```
pip install -i https://<username>:<password>@extensions.threatq.com/
threatq/sdk threatqsdk
```

> Replace the <username> and <password> placeholders with your repository credentials given to you by your ThreatQ Support Team.

# 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 |
| maltego-trx | N/A | N/A |

# Installation of ThreatQ Local Transforms

The following steps will instruct you on how to install and configure the integration with ThreatQ, into Maltego.

> Confirm that all the prerequisites listed have been addressed prior to starting the installation steps below.

1. Navigate to the ThreatQ Marketplace, and download the zip file for the integration.
2. Transfer the zip file to a directory on the same host running the Maltego Desktop Application. For example:
   - **Windows**: C:\Users\username>\Documents\ThreatQ\Code
   - **Linux**: /usr/local/bin/ThreatQ/Code
   - **maxOS**: /Users/username>/Documents/ThreatQ/Code
3. Extract the integration:

   ```
   unzip threatq-maltego-trx.zip
   ```

4. Navigate into the extracted code directory.
5. Locate the **threatquotient.cfg.example** configuration file and make a copy of it, removing the `.example` suffix.

   > threatquotient.cfg

6. Update the **threatquotient.cfg** file with the following parameters:

| PARAMETER | DESCRIPTION |
|---|---|
| **host** | This is the host of the ThreatQ instance, either the IP Address or Hostname as resolvable by ThreatQ. |
| **username** | For User-based Authentication - this is the email address of the user in the ThreatQ System that will manage integrations. |
| **password** | For User-based Authentication - the password for the above ThreatQ account. |
| **clientid** | For User-based Authentication - this is the OAuth id that can be found at Settings Gear → User Management → API details within the user's details. |

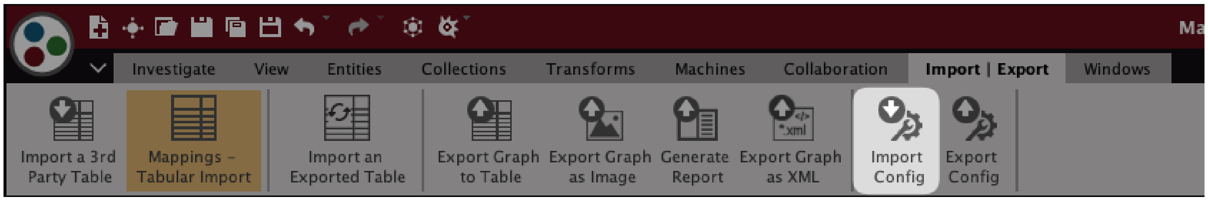
| PARAMETER | DESCRIPTION |
|---|---|
| **oauth_client_id** | For OAuth Authentication - this is the OAuth Client ID, generated via the ThreatQ CLI. |
| **oauth_client_secret** | For OAuth Authentication - the is the OAuth Client Secret, generated via the ThreatQ CLI. |

7. Run the integration once to generate the transform import files:

```
python src/project.py local runserver
```

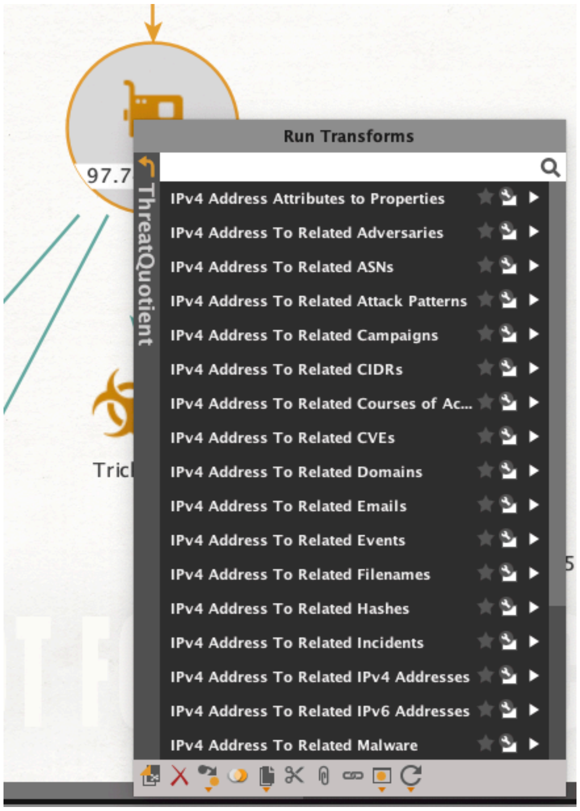
> You may see a handful of WARNING logs. These warnings can be ignored.

8. Open Maltego and navigate to the **Import | Export tab** and click on the **Import Config** button.



9. Use the file browser to locate the **.mtz files** in `./artifacts/mtz`.
10. Select the **threatq-entities.mtz package** and click **Next**.
11. Use the checkboxes to select what you want to import and then click **Next**.
12. Complete the import and repeat steps 7-10 with the threatq-transforms.mtz package.

You should now be able to run the ThreatQ transforms on your Maltego entities.


97.7
Tric
Run Transforms
ThreatQuotient
IPv4 Address Attributes to Properties
IPv4 Address To Related Adversaries
IPv4 Address To Related ASNs
IPv4 Address To Related Attack Patterns
IPv4 Address To Related Campaigns
IPv4 Address To Related CIDRs
IPv4 Address To Related Courses of Ac...
IPv4 Address To Related CVEs
IPv4 Address To Related Domains
IPv4 Address To Related Emails
IPv4 Address To Related Events
IPv4 Address To Related Filenames
IPv4 Address To Related Hashes
IPv4 Address To Related Incidents
IPv4 Address To Related IPv4 Addresses
IPv4 Address To Related IPv6 Addresses
IPv4 Address To Related Malware

# Usage

The following section provides information on integration transforms and steps for setting a python 3 executable path.

## Transforms

The integration provides over 500 transforms.  You can execute the following transforms on a variety of entity types:

- IOC -> Object Relationships
- Object -> Object Relationships
- STIX2 Object -> Object Relationships
  - Supported STIX2 Object Types: Attack Pattern, Course of Action, Threat Actor, Malware, Tool
- Fetch IOC Attributes as Properties

  > This includes attributes, tags, score, status, type, description, etc.

- Fetch Object Attributes as Properties

  > This includes attributes, tags, status, type, description, etc.

## Custom Python 3 Executable

The following steps will allow you to set a custom python 3 executable path.

> These steps assume that the transforms for ThreatQ are already installed.

1. Open Maltego.
2. From the the Transforms tab, click the **Transform Manager** button.
3. Search for **ThreatQ** in the the transforms search bar.
4. Select all the transforms by holding clicking the first entry, holding shift, and then selecting the last entry.
5. Enter your custom Python executable path for the Command field in the bottom right configuration box.

   > After hitting enter, allow the Maltego window a few minutes to aggregate and make the changes.

# Known Issues / Limitations

- The **URL Attributes to Properties** transform does not export the attributes to Maltego.
- Exporting relationships between entities and URLs from ThreatQ is not working due to an issue on Maltego.

# Change Log

- **Version 2.0.0**
    - Complete rewrite of the integration based on the new Maltego TRX SDK.
    - Added support for running transforms on ThreatQ custom objects
    - Added transform to fetch object metadata (context: Attributes, Tags, Relationships, etc.)
    - Added transform to create an entity (i.e. Indicator, Malware, etc.) in ThreatQ.
    - Added support for running transforms on more entity types
- **Version 1.0.0**
    - Initial release