ThreatQuotient

Trellix Helix Action User Guide

Version 1.0.0

June 21, 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	1.0.0
Compatible with ThreatQ Versions	>= 5.12.1
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Trellix Helix Action for ThreatQ enables the automatic dissemination of malicious IOCs to a Trellix Helix Intel Matching List.

The following action is included:

- **Trellix Helix - IOC Export** - Exports IOCs to a Trellix Helix list.

The action is compatible with the following indicator types:

- IP Address
- IPv6 Address
- FQDN
- Email Address
- MD5
- SHA-1

The action returns enriched indicator system objects.

> This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one of following indicator types:
    - IP Address
    - IPv6 Address
    - FQDN
    - Email Address
    - MD5
    - SHA-1
- ATenant and API Key for authenticating to Trellix Helix.

Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
   - Drag and drop the zip file into the dialog box
   - Select **Click to Browse** to locate the zip file on your local machine

   > ThreatQ will inform you if the action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

You will still need to configure the action.

Configuration

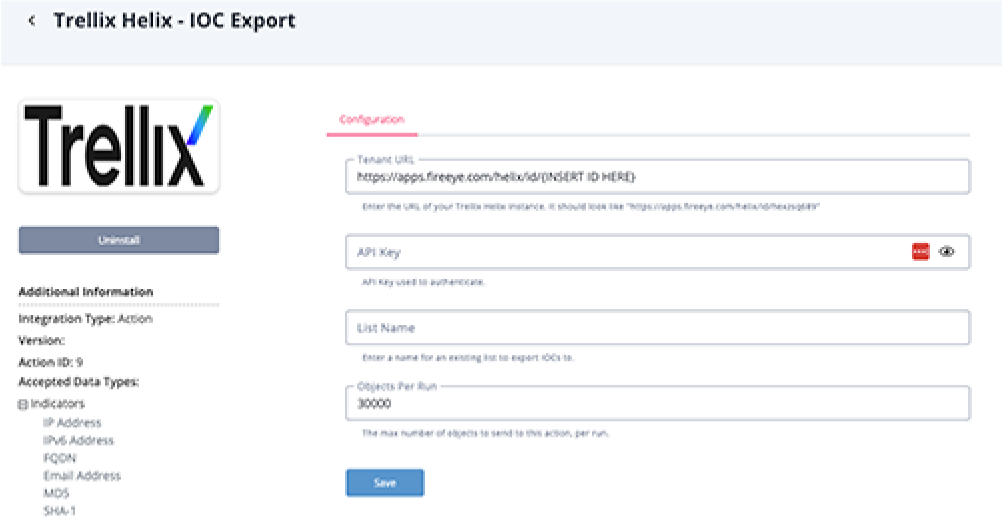
> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
Tenant URL	The URL of the Trellix Helix Instance. **Example:** https://apps.fireeye.com/helix/id/hexzsq689
API Key	Your Trellix API Key.
List Name	The name of the existing list to export IOCs to.
Objects Per Run	The max number of objects per run to send with this action.



‹ Trellix Helix - IOC Export

Additional Information

Integration Type: Action

Version:

Action ID: 9

Accepted Data Types:

⊟ Indicators
- IP Address
- IPv6 Address
- FQDN
- Email Address
- MD5
- SHA-1

Tenant URL: https://apps.fireeye.com/helix/id/{INSERT ID HERE}

Enter the URL of your Trellix Helix instance. It should look like "https://apps.fireeye.com/helix/id/hexzsg689"

API Key

API Key used to authenticate.

List Name

Enter a name for an existing list to export IOCs to.

Objects Per Run: 30000

The max number of objects to send to this action, per run.

5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Trellix Helix - IOC Export	Exports IOCs to a Trellix Helix list.	Indicator	IP Address, IPv6 Address, FQDN, Email Address, MD5, SHA-1

Trellix Helix - IOC Export

This action exports IOCs to a Trellix Helix matching list. It first searches in Trellix Helix for a list with the name configured by the user. If it finds it, it will remove all IOCs from that list and then adds the IOCs from the Data Collection.

- `GET {TENANT URL}/api/v3/lists/search`
- `DELETE {TENANT URL}/api/v3/lists/{LIST ID}/items`
- `POST {TENANT URL}/api/v3/lists/{LIST ID}/items/import`

When uploading IOCs to Trellix Helix, an optional Notes field is provided. This integration will utilize the ThreatQ sources to populate it. For example, if an IOC was reported by abuse.ch and US-CERT, the Notes field will look like: `Reported by: abuse.ch, US-CERT`

ThreatQ Score to Trellix Helix Risk

ThreatQ scores will be converted into a Trellix Helix Risk value.

THREATQ SCORE	TRELLIX HELIX RISK
0 - 3	Low
4 - 6	Medium
7 - 9	High
>= 10	Critical

Known Issues / Limitations

- Trellix Helix allows a maximum of 28,000 IOCs per list.

Change Log

- **Version 1.0.0**
  - Initial release