ThreatQuotient

ThreatQ ACE Action User Guide

Version 1.0.0

June 27, 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	>= 5.14.1
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The ThreatQ ACE Action is an action that utilizes the ThreatQ ACE Library to automatically parse context from data within ThreatQ.

The following action is provided:

- **ThreatQ ACE - Data Collection -** automatically parse context from data within ThreatQ.

The action is compatible with the following system object types:

- Malware
- Adversary
- Event
- Campaign
- Incident
- Attachment
- Report
- Tag

The action returns the following enriched system objects:

- Indicator
- Malware
- Adversary
- Attack Pattern
- Vulnerability
- Report
- Incident
- Campaign
- Event
- Attachment

> 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 the following object types:
  - Malware
  - Adversary
  - Event
  - Campaign
  - Incident
  - Attachment
  - Report
  - Tag
- ThreatQ ACE library and ThreatQ ACE Filter installed on your ThreatQ instance. These files are included in the marketplace download zip.

ThreatQ ACE Library and ThreatQ ACE Filter

The required ThreatQ ACE library and ThreatQ ACE Filter files are included in the action's marketplace download. Use the following steps to install the library.

> ⚠ When installing the library and filter, be aware that any in-progress feed runs will be cancelled when initiating step 6.

1. Locate the **tq_ace_filter-<version>-py3-none-any.whl** and **threatq_ace-<version>-py3-none-any.whl** files bundled with the marketplace zip file.
2. SSH into your ThreatQ instance.
3. Navigate to tmp directory:
   ```
   cd /tmp/
   ```
4. Upload the library and filter files to this directory.
5. Install the library and filter:
   ```
   sudo -u apache /opt/threatq/python/bin/pip install threatq_ace-
   <version>-py3-none-any.whl

   sudo -u apache /opt/threatq/python/bin/pip install tq_ace_filter-
   <version>-py3-none-any.whl
   ```
6. Restart Dynamo:
   ```
   systemctl restart threatq-dynamo
   ```
7. Proceed with installing the action.

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.

   > ⚠ This action download contains separate ThreatQ ACE Library and ThreatQ ACE Filter files that must be installed via the command line. The ThreatQ ACE library and ThreatQ ACE Filter are required by the action and must be installed prior to attempting to use the action in a workflow.

3. Unzip the downloaded zip and extract the ThreatQ Ace Library, ThreatQ ACE Filter, and a second action zip file.
4. Navigate to the integrations management page on your ThreatQ instance.
5. Click on the **Add New Integration** button.
6. Upload the extracted zip file (from step 3) 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:

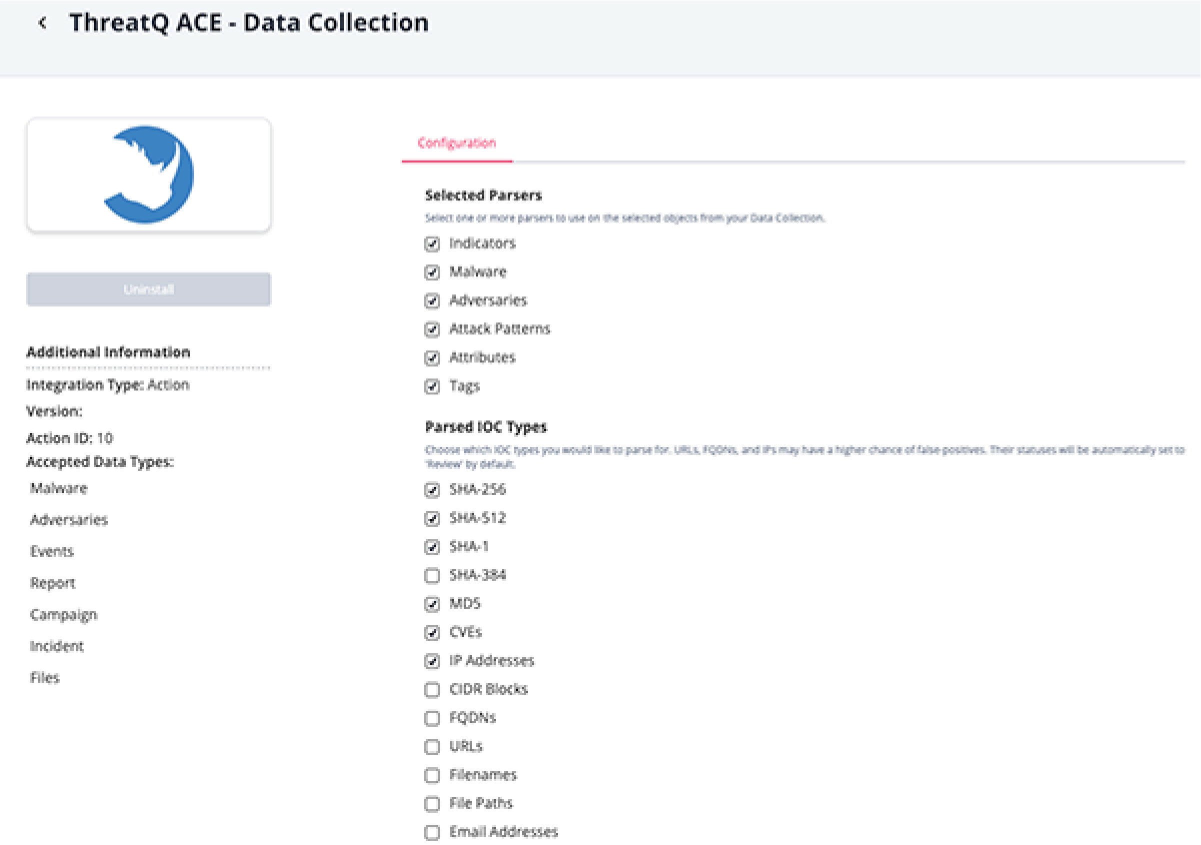
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> 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
Selected Parsers	Select the objects to parse. Options include: ◦ Indicators (default) ◦ Malware (default) ◦ Adversaries (default) ◦ Attack Patterns (default) ◦ Attributes (default) ◦ Tags (default)
Parsed IOC Types	Select the IOC types to parse. Options include: ◦ SHA-256 (default) ◦ SHA-512 (default) ◦ SHA-1 (default) ◦ SHA-384 ◦ MD5 (default) ◦ CVEs (default) ◦ IP Addresses ◦ CIDR Blocks ◦ FQDNs ◦ URLs ◦ Filenames ◦ File Paths ◦ Email Addresses
Parsed Attributes	Select the attributes to parse. Options include: ◦ Affected Operating System (default)

PARAMETER	DESCRIPTION
	◦ Target Industry (default) ◦ Threat Type (default) ◦ Tactic (default) ◦ Actor Country (default) ◦ Target Region (default) ◦ Affected Product (default) ◦ Detection
Save CVE Data as	Select which entity type you would like CVEs ingested as. Options include **Indicators** (default and **Vulnerabilities**.
Save PDF Text as Description	Enabling this will include the PDF's text in the Report's description.
List of Keywords	Enter a list of keywords to tag objects based on.
Tag Entity Type	Select the entity type you'd like the tag to be applied as. Options include **Attribute** (default) and **Tag**.
Attribute Name	Enter the name of the attribute to create if a keyword is found. The default value is **Tag**.
Adversaries NOT to match	Enter the Adversary values not to parse.
Attack Patterns NOT to match	Enter the Attack Pattern values not to parse.
Malware NOT to match	Enter the Malware values not to parse.
Indicators NOT to match	Enter the Indicators values not to parse.
Vulnerabilities NOT to match	Enter the Vulnerability values not to parse.

PARAMETER	DESCRIPTION
Objects Per Run	The max number of objects to send to this action per run. The default value is **10,000**.



‹ ThreatQ ACE - Data Collection

Additional Information

Integration Type: Action

Version:

Action ID: 10

Accepted Data Types:

Malware

Adversaries

Events

Report

Campaign

Incident

Files

Selected Parsers

Select one or more parsers to use on the selected objects from your Data Collection.

☑ Indicators

☑ Malware

☑ Adversaries

☑ Attack Patterns

☑ Attributes

☑ Tags

Parsed IOC Types

Choose which IOC types you would like to parse for. URLs, FQDNs, and IPs may have a higher chance of false-positives. Their statuses will be automatically set to 'Review' by default.

☑ SHA-256

☑ SHA-512

☑ SHA-1

□ SHA-384

☑ MD5

☑ CVEs

☑ IP Addresses

□ CIDR Blocks

□ FQDNs

□ URLs

□ Filenames

□ File Paths

□ Email Addresses

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

Action Functions

The following action is provided:

FUNCTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
ThreatQ ACE - Data Collection	Automatically parse context from data within ThreatQ	Malware, Adversary, Event, Campaign, Incident, Attachment, Report, Tag	N/A

ThreatQ ACE - Data Collection

The ThreatQ ACE - Data Collection action automatically parses context from selected data within ThreatQ.

> There is no mapping for this workflow. The ingested data depends on the selected objects & parsers.

Change Log

- **Version 1.0.0**
  - Initial release