ThreatQuotient

ThreatQ Investigations Action

Version 1.0.0

June 23, 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	1.0.0
Compatible with ThreatQ Versions	>= 5.12.1
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The ThreatQ Investigations Action integration allows managers to automatically create and assign investigations to users for incoming data.

The integration provides the following action:

- **ThreatQ - Create Investigations** - automatically creates investigations for incoming intelligence objects.

The action is compatible with the following system object types:

- Adversaries
- Assets
- Attack Patterns
- Campaigns
- Courses of Action
- Events
- Exploit Targets
- Identities
- Incidents
- Intrusion Sets
- Malware
- Reports
- Tools
- TTPs
- Vulnerabilities

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:
  - Adversaries
  - Assets
  - Attack Patterns
  - Campaigns
  - Courses of Action
  - Events
  - Exploit Targets
  - Identities
  - Incidents
  - Intrusion Sets
  - Malware
  - Reports
  - Tools
  - TTPs
  - Vulnerabilities

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.

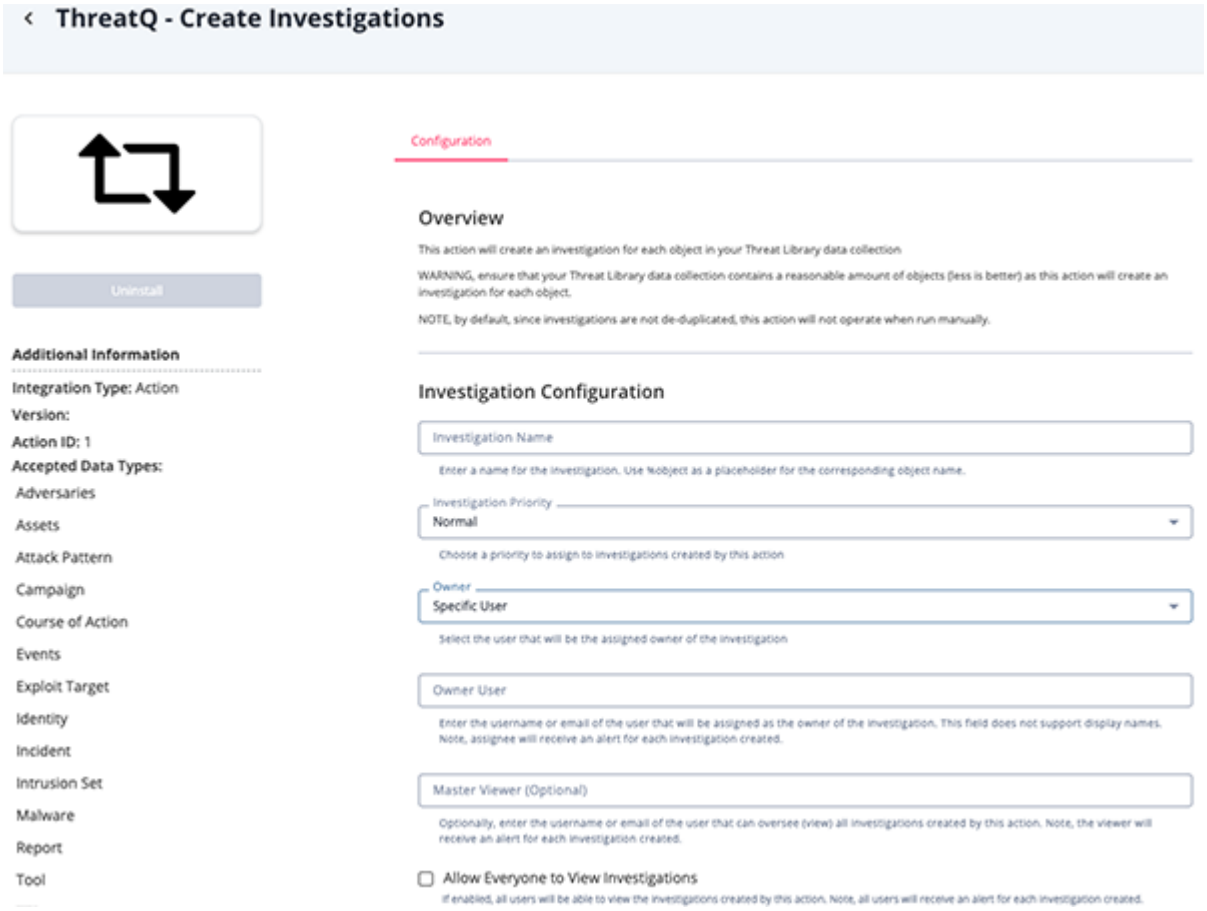
To configure the integration:

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
Investigation Name	Enter a name for the investigation. > You can use `%object` as a placeholder for the corresponding object name.
Investigation Priority	Select a priority to assign to investigations created by this action. Options include: ◦ Normal *(default)* ◦ Escalated
Owner	Select the user that will be the assigned owner of the investigation. Options include: ◦ Specific User *(default)* ◦ Least Assigned User
Owner User	Enter the username or email of the user that will be assigned as the owner of the investigation. The assignee will receive an alert for each investigation created. This parameter does not support display names.

PARAMETER	DESCRIPTION
	 This field is only accessible when the **Owner** parameter is set to `Specific User`.
Owner Pool	Enter a line-separated list of usernames or emails corresponding to users that will be considered for assignment. Assignees will receive an alert for each investigation created. This field does not support display names.  This parameter is only accessible when the `Owner` parameter is set to `Least Assigned`.
Master Viewer	Optional - Enter the username or email of the user that can oversee (view) all investigations created by this action. The viewer will receive an alert for each investigation created.
Allow Everyone to View Investigations	Enable this parameter to allow all users the ability to view the investigations created by this action. All users will receive an alert for each investigation created.
Allow Manual Execution	Enable this parameter to be able to run this action manually. When running manually, the entire data collection will be processed. This parameter is disabled by default to prevent creating duplicate investigations en masse.
Objects Per Run	Enter the number of objects to process per run. This is used to limit the number of investigations created in a single 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
ThreatQ - Create Investigations	Creates a new investigation for each object in a data collection.	Adversaries, Assets, Attack Patterns, Campaigns, Courses of Action, Events, Exploit Targets, Identities, Incidents, Intrusion Sets, Malware, Reports, Tools, TTPs, Vulnerabilities	N/A

ThreatQ - Create Investigations

The ThreatQ - Create Investigations action will take a data collection and create an investigation for each object in the collection. The investigation's owner will be set to the user specified in the configuration.

> There is no mapping for this action. The ingested data is based on inputs and user configurations.

Change Log

- **Version 1.0.0**
  - Initial release