ThreatQuotient

ThreatQuotient for Investigation Actions Operation User Guide

Version 1.0.0

October 28, 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	>= 4.20.0
Support Tier	ThreatQ Supported

Introduction

The Investigation Actions Operation for ThreatQuotient allows a ThreatQ user to execute additional actions on their investigations. This is to enhance the user's interaction with the creation and use of investigations within ThreatQ.

The operation provides the following actions:

- **Start** - allows a ThreatQ user to start an investigation from any base ThreatQ object (indicator, adversary, event, attachment).
- **Add** - allows a ThreatQ user to add any base ThreatQ object to an investigation (indicator, adversary, event, attachment).
- **Clone** - allows a ThreatQ user to clone an investigation from any base ThreatQ object (indicator, adversary, event, attachment).
- **Merge** - allows a ThreatQ user to merge related investigations to any base ThreatQ object (indicator, adversary, event, attachment).

The operation is compatible with the following object types:

- Attachment
- Adversary
- Indicator
- Event

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 integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
    - Drag and drop the file into the dialog box
    - Select **Click to Browse** to locate the integration file on your local machine

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

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to configure and then enable the operation.

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 **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Review any additional settings, make any changes if needed, and click on **Save**.
5. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Actions

The operation provides the following actions:

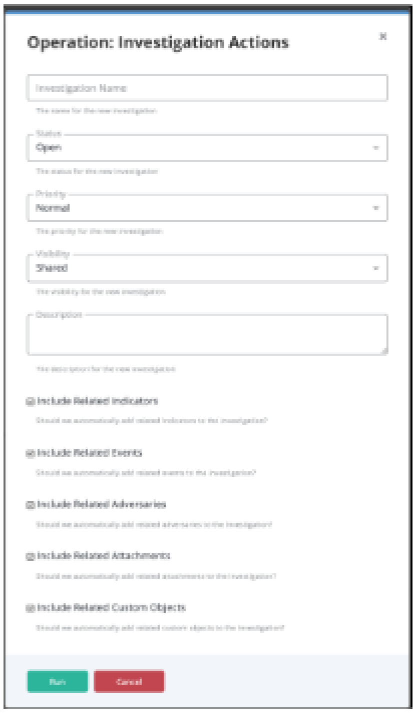
ACTION	DESCRIPTION	OBJECT TYPE
Start	Allows a ThreatQ user to start an investigation from any base ThreatQ object.	Indicator, Adversary, Event, Attachment
Add	Allows a ThreatQ user to add any base ThreatQ object to an investigation.	Indicator, Adversary, Event, Attachment
Clone	Allows a ThreatQ user to clone an investigation from any base ThreatQ object.	Indicator, Adversary, Event, Attachment
Merge	Allows a ThreatQ user to merge related investigations to any base ThreatQ object.	Indicator, Adversary, Event, Attachment

Start

The Start action allows a ThreatQ user to start an investigation from any base ThreatQ object.

The action provides the following parameters:

PARAMETER	DESCRIPTION
Investigation Name	The name for the new investigation.
Status	The status for the new investigation.
Priority	The priority for the new investigation.
Visibility	The visibility for the new investigation. This parameter can only be set to Shared at this time.
Description	The description for the new investigation.
Include Related Indicators	Whether or not to include related indicators in the new investigation.
Include Related Events	Whether or not to include related events in the new investigation.
Include Related Adversaries	Whether or not to include related adversaries in the new investigation.
Include Related Attachments	Whether or not to include related attachments in the new investigation.
Include Related Custom Objects	Whether or not to include related custom objects in the new investigation.



Operation: Investigation Actions

Investigation Name
The name for the new investigation

Status: Open
The status for the new investigation

Priority: Normal
The priority for the new investigation

Visibility: Shared
The visibility for the new investigation

Description
The description for the new investigation

☑ Include Related Indicators
Should we automatically add related indicators to the investigation?

☑ Include Related Events
Should we automatically add related events to the investigation?

☑ Include Related Adversaries
Should we automatically add related adversaries to the investigation?

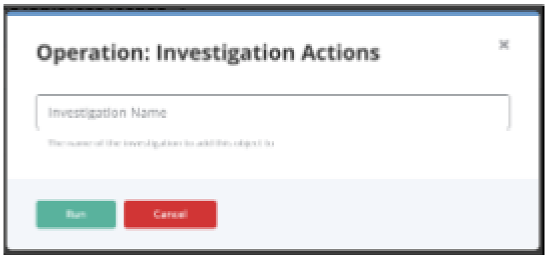
☑ Include Related Attachments
Should we automatically add related attachments to the investigation?

☑ Include Related Custom Objects
Should we automatically add related custom objects to the investigation?

Add

The Add action allows a ThreatQ user to add any base ThreatQ object to an investigation. The action provides the following parameters:

PARAMETER	DESCRIPTION
Investigation Name	The name of the investigation.



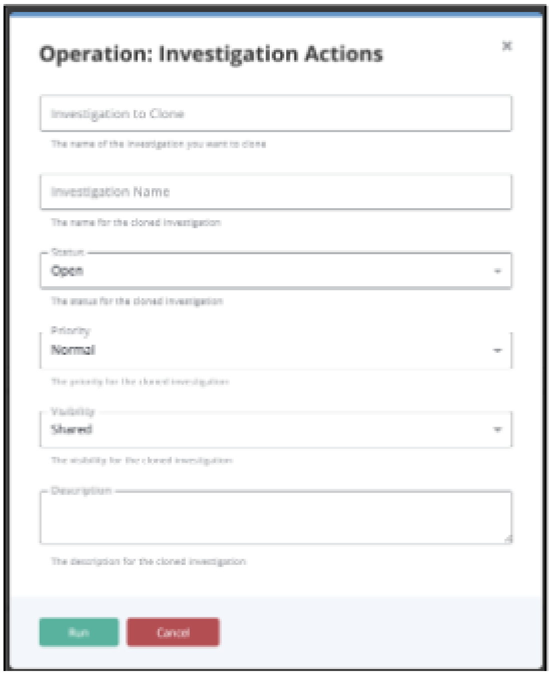
Operation: Investigation Actions

Investigation Name
The name of the investigation to add this object to

Clone

The Clone allows a ThreatQ user to clone an investigation from any base ThreatQ object. The action provides the following parameters:

PARAMETER	DESCRIPTION
Investigation to Clone	The name of the investigation to clone.
Investigation Name	The name of the new investigation.
Status	The status of the new investigation.
Priority	The priority of the new investigation.
Visibility	The visibility for the new investigation. This parameter can only be set to Shared at this time.
Description	The description of the new investigation.



Operation: Investigation Actions

Investigation to Clone
The name of the investigation you want to clone

Investigation Name
The name for the cloned investigation

Status: Open
The status for the cloned investigation

Priority: Normal
The priority for the cloned investigation

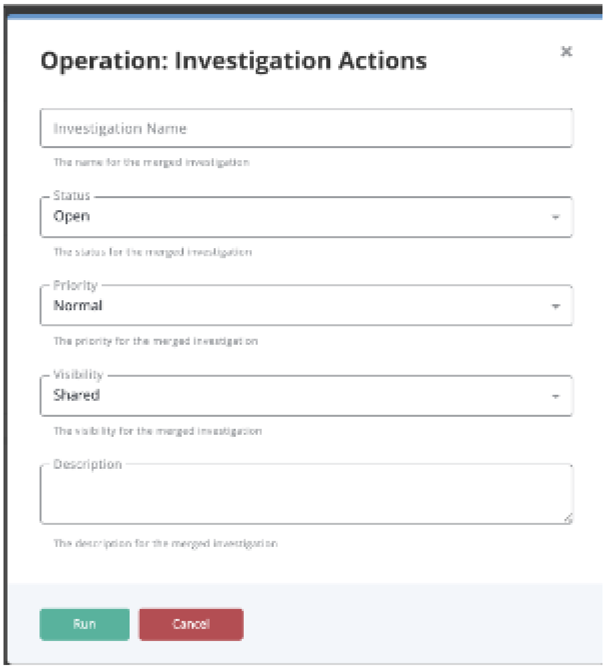
Visibility: Shared
The visibility for the cloned investigation

Description
The description for the cloned investigation

Merge

The Merge action allows a ThreatQ user to add any base ThreatQ object to an investigation. The action provides the following parameters:

PARAMETER	DESCRIPTION
Investigation Name	The name for the merged investigation.
Status	The status for the merged investigation.
Priority	The priority for the merged investigation.
Visibility	The visibility for the merged investigation. This parameter can only be set to Shared at this time.
Description	The description for the merged investigation.



Operation: Investigation Actions

Investigation Name

The name for the merged investigation

Status: Open

The status for the merged investigation

Priority: Normal

The priority for the merged investigation

Visibility: Shared

The visibility for the merged investigation

Description

The description for the merged investigation

Known Issues / Limitations

- All created investigations will be created as **Shared**. To change this, it will need to be changed manually to **Private** if needed. To **merge** or **clone** investigations, the investigations will need to be **Shared**.

Change Log

- **Version 1.0.0**
    - Initial release