ThreatQuotient

ThreatQ Object Action Bundle

Version 1.0.0

September 10, 2024

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	>= 5.29.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The ThreatQ Object Action for ThreatQ allows a user to interact with ThreatQ objects in complex ways to better manage the Threat Library.

The action can perform the following functions:

- **ThreatQ Object Clone** - create a new object based on the original.
- **ThreatQ Object Inherit From Children** - add relationships and other context from child relationships.

The action is compatible with the following system object types:

- Adversary
- Asset
- Attack Pattern
- Campaign
- Course Of Action
- Event
- Exploit Target
- Identity
- Incident
- Indicator
- Intrusion Set
- Malware
- Report
- Signature
- Tool
- TTP
- Vulnerability

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:
  - Adversary
  - Asset
  - Attack Pattern
  - Campaign
  - Course Of Action
  - Event
  - Exploit Target
  - Identity
  - Incident
  - Indicator
  - Intrusion Set
  - Malware
  - Report
  - Signature
  - Tool
  - TTP
  - Vulnerability

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 actions.

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:

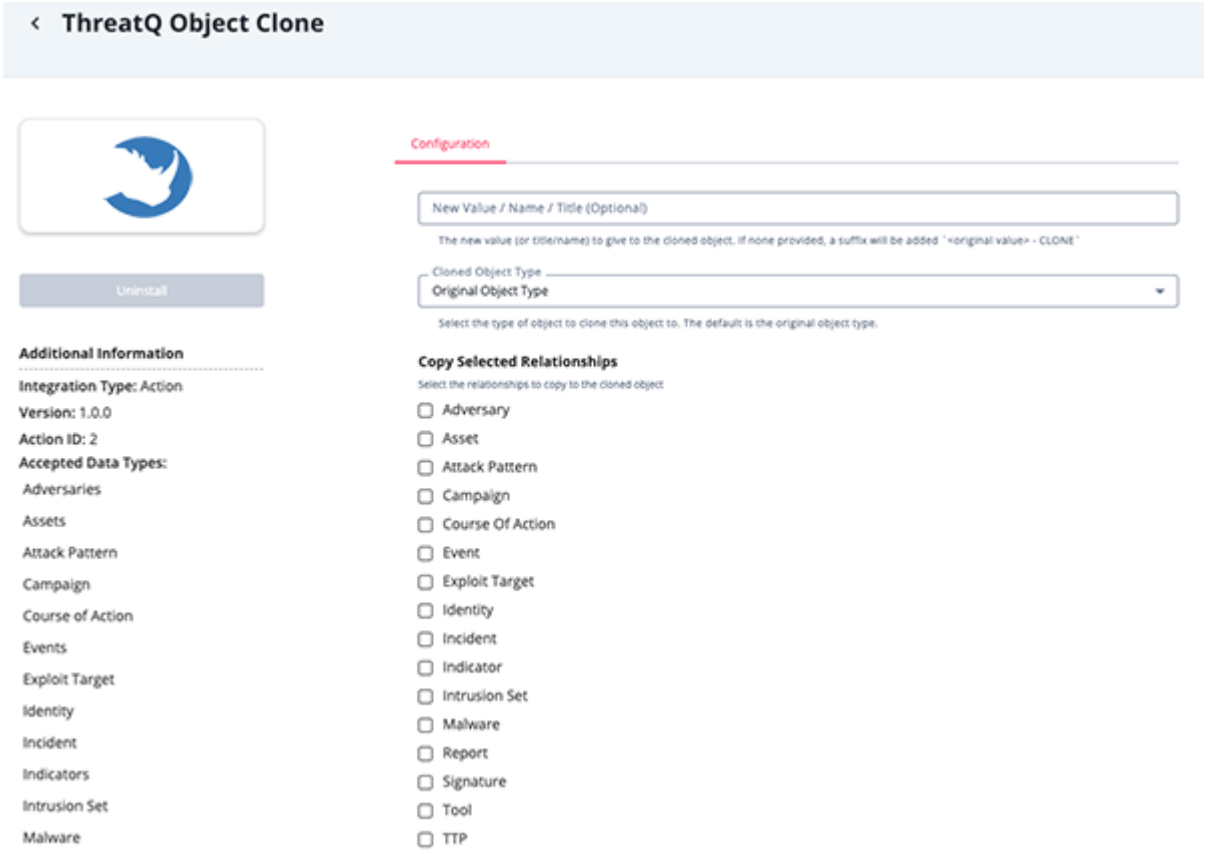
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> 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.

ThreatQ Object Clone Parameters

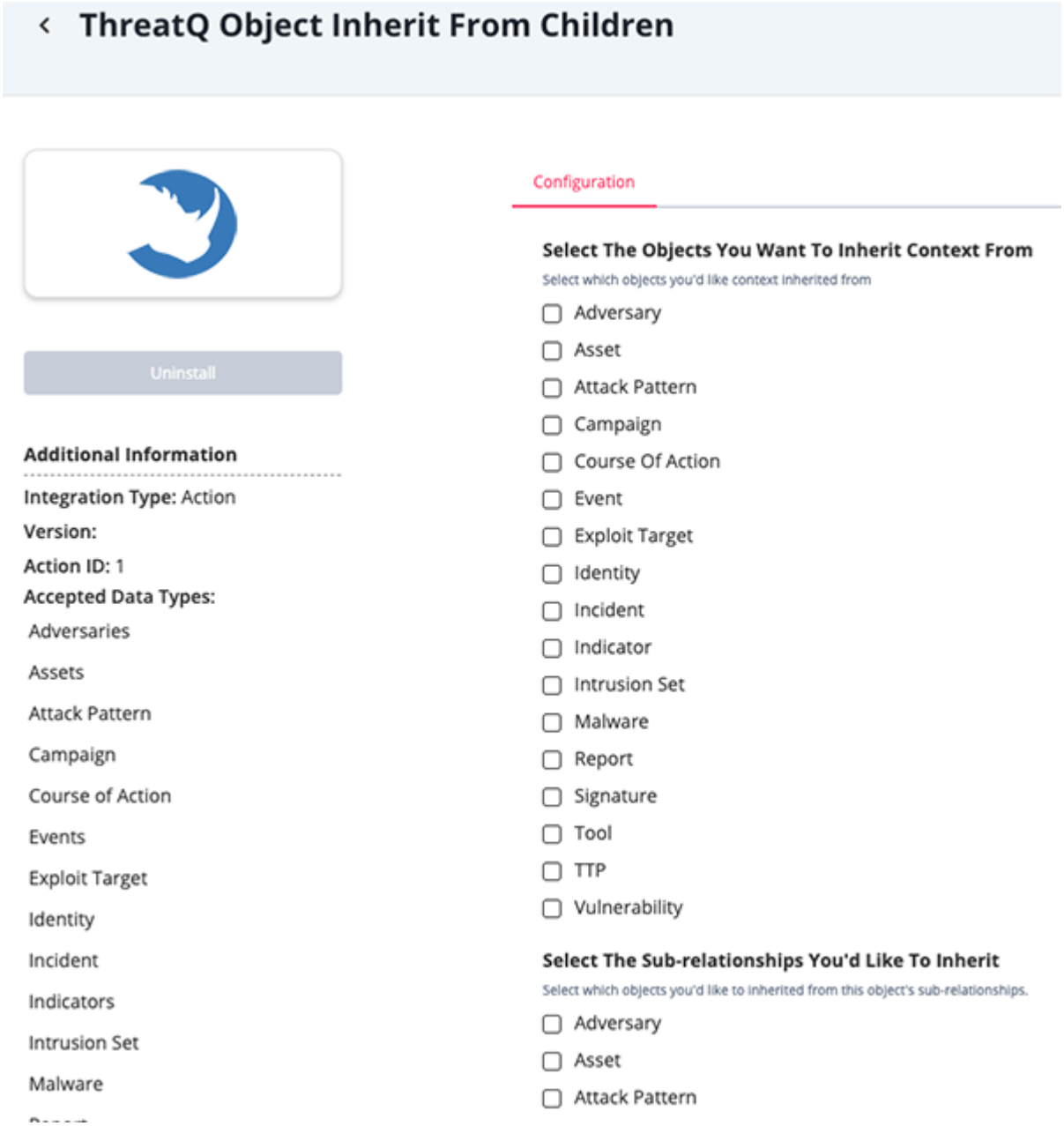
PARAMETER	DESCRIPTION
New Value / Name / Title (Optional)	The new value (or title/name) to give to the cloned object. If none provided, a prefix will be added. Example: `<original value> - CLONE`.
Cloned Object Type	Select the type of object to clone this object to. The default is the original object type. Options include: ◦ Adversary ◦ Asset ◦ Attack Pattern ◦ Campaign ◦ Course Of Action ◦ Event ◦ Exploit Target ◦ Identity ◦ Incident ◦ Indicator ◦ Intrusion Set ◦ Malware ◦ Report ◦ Signature ◦ Tool ◦ TTP ◦ Vulnerability

PARAMETER	DESCRIPTION
Copy Selected Relationships	Select the relationships to copy to the cloned object. Options include: ◦ Adversary ◦ Asset ◦ Attack Pattern ◦ Campaign ◦ Course Of Action ◦ Event ◦ Exploit Target ◦ Identity ◦ Incident ◦ Indicator ◦ Intrusion Set ◦ Malware ◦ Report ◦ Signature ◦ Tool ◦ TTP ◦ Vulnerability
Copy Descriptions	Enable this to copy all the descriptions to the cloned object.
Copy Tags	Enable this to copy all tags to the cloned object.
Copy Attributes	Enable this to copy all attributes (including their sources) to the cloned object.
Relate Cloned Object to Original	Enable this to relate the cloned object to the original object.
Objects per run	Maximum number of objects per-run.



ThreatQ Object Inherit from Children Parameters

PARAMETER	DESCRIPTION
Select the objects you want to inherit context from	Select which objects you'd like context inherited from.
Select the sub-relationships you'd like to inherit	Select which objects you'd like to inherited from this object's sub-relationships.
Inherit Tags	Check this to bubble up tags to this object
Inherit Attributes	Check this to bubble up attributes to this object
Objects per run	Maximum number of objects per-run.



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

Enriched Data

Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

ThreatQ Object Clone

METRIC	RESULT
Run Time	1 minute
Adversaries	100
Adversary Attributes	260
Reports	100
Report Attributes	420

ThreatQ Object Inherit from Children

METRIC	RESULT
Run Time	1 minute
Adversaries	100
Adversary Attributes	260
Reports	100

METRIC	RESULT
Report Attributes	420

Use Case Example

ThreatQ Object Clone

1. A user submits a collection of Adversaries that have tags, attributes, descriptions and other related objects.
2. The user sets `Cloned Object Type` to `Report` and checks the information that should be added to the new reports from the adversaries.
3. The action creates a new Report based on the original Adversary.

ThreatQ Object Inherit from Children

1. A user submits a collection of Adversaries that have related objects
2. The action enriches each Adversary with information from the related objects according to the user configuration.

Known Issues / Limitations

- The `ThreatQ Object Clone` action cannot create objects that have a required type (Indicators, Events) or status (Indicators) if the original object that not also have it.

Change Log

- **Version 1.0.0**
  - Initial release