

ThreatQuotient



ThreatQ Bulk Changes Action Bundle

Version 1.1.0

June 17, 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 | 3 |
| Support | 4 |
| Integration Details..... | 5 |
| Introduction | 6 |
| Prerequisites | 7 |
| Installation..... | 8 |
| Configuration | 9 |
| Add / Remove Attributes..... | 9 |
| Add / Remove Relationships | 10 |
| Add / Remove Tags | 11 |
| Change Expiration Policy | 11 |
| Change Status..... | 12 |
| Change Point of Contact | 12 |
| Actions | 13 |
| Use Case Examples..... | 14 |
| Known Issues / Limitations | 15 |
| Change Log | 16 |

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.

Copyright © 2024 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

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 | 1.1.0 |
| Compatible with ThreatQ Versions | >= 5.24.0 |
| ThreatQ TQO License Required | Yes |
| Support Tier | ThreatQ Supported |

Introduction

The ThreatQ Bulk Changes Action Bundle allows you to automate the bulk update process of your system objects by creating a workflow that will execute bulk updates on objects that meet the specified criteria.

The integration provides the following actions:

- **Add / Remove Tags** - add or remove Tags for an object in the Threat Library.
- **Add / Remove Attributes** - add or remove Attributes for an object in the Threat Library.
- **Change Status** - change the Status of Indicators and/ or Signatures in the Threat Library.
- **Change Expiration Policy** - change the Expiration Policy for Indicators in the Threat Library.
- **Add / Remove Relationships** - add or remove Relationships for an object in the Threat Library.
- **Change Point of Contact** - change the Point of Contact from the Threat Library.

The action is compatible with the following system object types:

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



The **Change Expiration Policy** action is only compatible with indicator objects and the **Change Status** action is only compatible with indicator and signature objects. All other objects types included in data collections submitted to these two actions will be ignored.

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
6. When prompted, select which actions to install on your instance.



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(s).

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.

Add / Remove Attributes

| PARAMETER | DESCRIPTION |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Object Selection | <p>Select the objects to apply these changes to from the list provided. Options include:</p> <ul style="list-style-type: none"> ◦ Adversaries ◦ Assets ◦ Attack Patterns ◦ Campaigns ◦ Courses of Action ◦ Events ◦ Exploit Targets ◦ Files ◦ Identities ◦ Indicators ◦ Intrusion Sets ◦ Malware ◦ Reports ◦ Signatures ◦ Tools ◦ TTPs ◦ Vulnerabilities |
| Add Attributes | <p>Enter a line-separated list of attributes to add to the selected objects. You must provide both a name and value, separated by an equals sign (i.e. "Confidence=High").</p> <p>To provide a Source & TLP marking, append the Source & TLP to the</p> |

| PARAMETER | DESCRIPTION |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | attribute name, in brackets, separated by a colon (i.e. "Confidence[Analyst:RED]=High"). |
| Remove Attributes | Enter a line-separated list of attributes to remove from the selected objects. You can provide just the name, or the name and value, separated by an equals sign (i.e. "Confidence=High"). If no value is specified, all attributes with the given name will be removed. |


Add / Remove Relationships

| PARAMETER | DESCRIPTION |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Object Selection | <p>Select the object types to bulk update based on the data collection filters. Options include:</p> <ul style="list-style-type: none"> ◦ Adversaries ◦ Assets ◦ Attack Patterns ◦ Campaigns ◦ Courses of Action ◦ Events ◦ Exploit Targets ◦ Files ◦ Identities ◦ Indicators ◦ Intrusion Sets ◦ Malware ◦ Reports ◦ Signatures ◦ Tools ◦ TTPs ◦ Vulnerabilities |
| Add Relationships | Enter a line-separated list of relationships to add to the selected objects. You must provide both a name and value, separated by an equals sign (i.e. "Malware=Lockbit"). |
| Remove Relationships | Enter a line-separated list of relationships to remove from the selected objects. You must provide both a name and value, separated by an equals sign (i.e. "Adversary=APT1"). |

Add / Remove Tags

| PARAMETER | DESCRIPTION |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Object Selection | <p>Select the object types to bulk update based on the data collection filters. Options include:</p> <ul style="list-style-type: none"> ◦ Adversaries ◦ Assets ◦ Attack Patterns ◦ Campaigns ◦ Courses of Action ◦ Events ◦ Exploit Targets ◦ Files ◦ Identities ◦ Indicators ◦ Intrusion Sets ◦ Malware ◦ Reports ◦ Signatures ◦ Tools ◦ TTPs ◦ Vulnerabilities |
| Add Tags | Enter a line-separated list of tags to add to the selected objects. |
| Remove Tags | Enter a line-separated list of tags to remove from the selected objects. |

Change Expiration Policy

| PARAMETER | DESCRIPTION |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Select Expiration Status | <p>Select the type of expiration change to apply to the indicators. Options include:</p> <ul style="list-style-type: none"> ◦ Extend the Expiration Date (default) ◦ Protect from Auto-Expiration ◦ Remove Expiration Date |
| Enter Days to Extend | <p>Enter the number of days to extend the expiration for the selected indicators.</p> <div>  <p>This field is only visible when the Select Expiration Status field is set to Extend the expiration date.</p> </div> |

Change Status

| PARAMETER | DESCRIPTION |
|------------------|---------------------------------------------------------------------------------------|
| Object Selection | Select the object types you want to bulk update based on the data collection filters. |
| Change Status | Select the status you want to apply to the selected objects. |

Change Point of Contact

| PARAMETER | DESCRIPTION |
|----------------------------|--------------------------------------------------------------------------------------------|
| Change Point of Contact to | Type the name of the Point of Contact to add/change to. |
| Object Selection | Select the object types you want to bulk update based on the data collection filters. |
| Select a Function | Select the function you want to perform (Change Point of Contact/Remove Point of Contact). |
| Objects Per Run | Select the number of objects to process per run of the workflow. |

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

Actions

The following actions are available:

| ACTION | DESCRIPTION | OBJECT TYPE |
|-----------------------------------|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Add / Remove Tags | Add or remove tags from objects | Adversaries, Assets, Attack Patterns, Campaigns, Courses of Action, Events, Exploit Targets, Files, Identities, Indicators, Intrusion Sets, Malware, Reports, Signatures, Tools, TTPs, Vulnerabilities |
| Add / Remove Attributes | Add or remove attributes from objects | Adversaries, Assets, Attack Patterns, Campaigns, Courses of Action, Events, Exploit Targets, Files, Identities, Indicators, Intrusion Sets, Malware, Reports, Signatures, Tools, TTPs, Vulnerabilities |
| Add / Remove Relationships | Add or remove relationships from objects | Adversaries, Assets, Attack Patterns, Campaigns, Courses of Action, Events, Exploit Targets, Files, Identities, Indicators, Intrusion Sets, Malware, Reports, Signatures, Tools, TTPs, Vulnerabilities |
| Change Status | Change the status of objects | Indicators, Signatures |
| Change Expiration Policy | Change the expiration of indicators | Indicators |
| Change Point of Contact | Change the point of contact of indicators | Asset, Attack Pattern, Campaign, Course Of Action, Event, Exploit Target, Identity, Incident, Intrusion Set, Malware, Note, Report, Tool, TTP, Vulnerability |



This action bundle guide does not have a mapping section as data is not being submitted or ingested in the ThreatQ platform.

Use Case Examples

Add / Remove Attributes

1. As an analyst, I want to automatically add an attribute to all indicators with a Malware Relationship so I can score them higher in my ThreatQ Scoring Policy.
2. As an analyst, I want to automatically add an attribute to all objects with a specific attribute so I can normalize it for a specific downstream tool.

Add / Remove Relationships

1. As an analyst, I want to automatically add a relationship to an attack pattern to all reports that contain a specific MITRE ATT&CK Technique ID (TID).
2. As an analyst, I want to automatically remove a relationship to a specific adversary, and switch it to a different adversary entry (alias).

Add / Remove Tags

1. As an analyst, I want to automatically add a tag to all reports that contain keywords related to my organization's industry, so that I can easily identify them in the Threat Library.
2. As an analyst, I want to automatically tag all indicators that have have a relation to a specific adversary or malware family, so that I can easily identify them in the Threat Library.

Change Expiration Policy

1. As an analyst, I want to set specific indicators to never expire, when they are related to a specific adversary or malware family, so that I can ensure they are always being monitored and alerted on.

Change Status

1. As an analyst, I want to automatically change the status of all indicators related to a specific ransomware family to 'Active' so that I can ensure they are being monitored and alerted on.
2. As an analyst, I want to automatically change the status of all indicators with a specific attribute to 'Whitelisted' so that I can ensure they are not being accidentally blocked.

Change Point of Contact

1. As an analyst, I want to automatically change the Point Of Contact of all supported object related to a specific ransomware family.

Known Issues / Limitations

- The actions provided in this bundle are not compatible with custom objects or tasks.
- For point of contact changes, only valid users can be assigned. If an invalid user is typed, the function will fail and return a **Point Of Contact is not valid** error.

Change Log

- **Version 1.1.0**
 - Adds the option to change points of contact.
- **Version 1.0.0**
 - Initial release