

# ThreatQuotient



## AskSage.ai Action Bundle

**Version 1.0.0**

January 28, 2025

### ThreatQuotient

20130 Lakeview Center Plaza Suite 400  
Ashburn, VA 20147

 **ThreatQ Supported**

### Support

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [support.threatq.com](https://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
Train Dataset Parameters.....	9
Generate Report Parameters.....	11
Actions .....	14
AskSage.ai - Train Dataset .....	15
AskSage.ai - Generate Report.....	16
Enriched Data.....	17
Generate Report .....	17
Use Case Example.....	18
Known Issues / Limitations .....	19
Change Log .....	20

# 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 © 2025 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](mailto: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	>= 6.1.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

# Introduction

The AskSage.ai Action Bundle for ThreatQ enables organizations to train datasets using content from their Threat Library, then query the trained models to generate reports and insights based on the organization's specific requirements.

AskSage.ai specializes in providing government-grade secure environments to train and query a variety of AI models. It supports over 20 large language models (LLMs) and hundreds of plugins/personas to provide a wide range of capabilities and perspectives. Using these models, organizations can securely train models against specific datasets, allowing them to query the models for curated insights based on the organization's needs.

The integration provides the following actions:

- **AskSage.ai - Train Dataset** - submits selected reports to an AskSage Dataset for training.
- **AskSage.ai - Generate Report** - queries an AskSage Dataset to generate a report based on the organization's specific requirements.

The actions are compatible with and return enriched Report objects.



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 the Report objects.
- A valid AskSage.ai API Key.



A free trial is available at <https://asksage.ai>.

# Installation

Perform the following steps to install the integration:



The same steps can be used to upgrade the integration to a new version.

1. Contact the ThreatQuotient support team, [support@threatq.com](mailto:support@threatq.com), to request the integration file.



This integration cannot be downloaded from the ThreatQ Marketplace.

2. Navigate to the integrations management page on your ThreatQ instance.
3. Click on the **Add New Integration** button.
4. 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
5. Select the actions to install, when prompted, and click on **Install**.



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.

## Train Dataset Parameters

PARAMETER	DESCRIPTION
Accept the User Agreement	Click on <b>Accept the User Agreement</b> checkbox to reveal the User Agreement and then select <b>I Agree</b> .
Email	Enter the AskSage.ai email address that you use to authenticate with AskSage.ai.  <div>            You must click on the <b>I Agree</b> checkbox in order to access this parameter.         </div>
API Key	Enter your AskSage.ai API key.  <div>            You must click on the <b>I Agree</b> checkbox in order to access this parameter.         </div>
Model Selection	Select which model to use for generating the intelligence report. Options include:

## PARAMETER

## DESCRIPTION

- |                        |                     |
|------------------------|---------------------|
| ◦ GPT 4o Gov (default) | ◦ GPT4 32k          |
| ◦ AWS Bedrock Titan    | ◦ GPT35 16k         |
| ◦ LLMA3                | ◦ GPT4 Vision       |
| ◦ Claude2              | ◦ GTP 4o            |
| ◦ Claude 3 Opus        | ◦ GTP 4o Mini       |
| ◦ Claude 3 Sonnet      | ◦ DALL-E 2          |
| ◦ Claude 35 Sonnet     | ◦ DALL-E 3          |
| ◦ Cohere               | ◦ Google Bison      |
| ◦ Mistral Large        | ◦ Google Gemini Pro |
| ◦ GPT Gov              | ◦ Groq 70b          |
| ◦ GPT4 Gov             | ◦ GPT O1            |
| ◦ GPT                  | ◦ GPT O1 Mini       |
| ◦ GPT4                 | ◦ XAI Grok          |



You must click on the **I Agree** checkbox in order to access this parameter.

### Threat / Topic (Dataset Name)

Enter the threat or topic that this report is about. This will allow us to train a specific dataset for this threat. You can also set up multiple workflows pointing to the same dataset to train the model on different reports.



You must click on the **I Agree** checkbox in order to access this parameter.

### Enable SSL Certificate Verification

Enable this for the action to validate the host-provided SSL certificate.

### Disable Proxies

Enable this option if the action should not honor proxies set in the ThreatQ UI.

## AskSage.ai - Train Dataset



Uninstall

### Additional Information

Integration Type: Action

Version:

Action ID: 8

Accepted Data Types:

Report

### Configuration

#### Accept the User Agreement

In order to run this action, you must accept the User Agreement.

#### User Agreement

By checking the box below, you understand that this action will send the selected data to the third-party vendor, AskSage.ai. You understand that the primary description for the data will be sent to AskSage.ai for processing and that you are giving AskSage.ai permission to create Datasets using the selected data. You also understand that this integration acts as an interface between your data collection in ThreatQ and the AskSage.ai API, and it will only send the data that you have selected.

☒ I Accept

#### Overview

This action will allow you to train a Dataset in your AskSage.ai tenant. This action can only be run manually, by selecting multiple objects through the ThreatQ Threat Library or from a single object's details page.

The selected data will be shared to AskSage.ai for processing & training. This data will not be shared outside of your AskSage.ai tenant, and will only be used when querying a model using a dataset. The Dataset name will be automatically generated based on the provided threat/topic.

#### Authentication

Email

Enter your AskSage.ai email to authenticate.

API Key

Enter your AskSage.ai API Key to authenticate. You can generate an API Key from the Settings page in the AskSage.ai platform.

#### LLM Options

Threat / Topic (Dataset Name)

Enter the threat or topic that this report is about. This will allow us to train a specific dataset for this threat. You can also set up multiple workflows pointing to the same dataset to train the model on different reports.

## Generate Report Parameters

### PARAMETER

### DESCRIPTION

Accept the User Agreement

Click on **Accept the User Agreement** checkbox to reveal the User Agreement and then select **I Agree**.

Email






Enter the AskSage.ai email address that you use to authenticate with AskSage.ai.



You must click on the **I Agree** checkbox in order to access this parameter.

API Key

Enter your AskSage.ai API key.

PARAMETER	DESCRIPTION
	 You must click on the <b>I Agree</b> checkbox in order to access this parameter.
<b>Threat / Topic (Dataset Name)</b>	<p>Enter the threat or topic that this report is about. This will allow you to link the report to the dataset that was trained for this threat. If no threat/dataset is entered, the report will be generated using the global, All dataset (not recommended).</p>  You must click on the <b>I Agree</b> checkbox in order to access this parameter.
<b>System Prompt / Backstory</b>	<p>Enter the system prompt for the LLM model. This will be used to set the scene for the model when asking it to generate the report.</p>  You must click on the <b>I Agree</b> checkbox in order to access this parameter.
<b>Prompt</b>	<p>Enter a prompt for the LLM model. This will be used to generate the report, in addition to the system prompt.</p>  You must click on the <b>I Agree</b> checkbox in order to access this parameter.
<b>Industry</b>	<p>Enter the industry that this report is for. This will be used when asking the model to generate the report for this threat.</p>  You must click on the <b>I Agree</b> checkbox in order to access this parameter.
<b>Enable SSL Certificate Verification</b>	<p>Enable this for the action to validate the host-provided SSL certificate.</p>

## PARAMETER

## DESCRIPTION

Disable Proxies

Enable this option if the action should not honor proxies set in the ThreatQ UI.

### ◀ AskSage.ai - Generate Report



Uninstall

#### Additional Information

Integration Type: Action

Version:

Action ID: 9

Accepted Data Types:

Report

#### Configuration

##### ☒ Accept the User Agreement

In order to run this action, you must accept the User Agreement.

##### User Agreement

By checking the box below, you understand that this action will send the selected data to the third-party vendor, AskSage.ai. You understand that the primary description for the data will be sent to AskSage.ai for processing and that you are giving AskSage.ai permission to create Datasets using the selected data. You also understand that this integration acts as an interface between your data collection in ThreatQ and the AskSage.ai API, and it will only send the data that you have selected.

☒ I Accept

#### Overview

This action will generate a report based on the trained dataset and the provided prompts. This action cannot be ran on a schedule, and must be ran manually from the ThreatQ Threat Library, an object details page, or the Workflow page.

Generated reports will vary based on the prompts provided. Response length will also vary based on the selected model and its capabilities.

#### Authentication

Email

Enter your AskSage.ai email to authenticate.

API Key

Enter your AskSage.ai API Key to authenticate. You can generate an API Key from the Settings page in the AskSage.ai platform.

#### LLM Options

Model Selection

GPT 4o Gov

Select which model to use for generating the intelligence report.

Threat / Topic (Dataset Name; Recommended)

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

# Actions

The following actions are available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
<a href="#">Train Dataset</a>	Trains a dataset using report content from your Threat Library.	Report	N/A
<a href="#">Generate Report</a>	Queries a dataset to generate a report based on the dataset's training.	Report	N/A

---

## AskSage.ai - Train Dataset

The AskSage.ai Train Dataset action takes reports from your Threat Library and submits the content to AskSage.ai to train a dataset. The action can only be run manually, by selecting multiple objects through the ThreatQ Threat Library or from a single object's details page.

POST <https://api.asksage.ai/server/train>

### Sample Response:

```
{
  "status": 200,
  "response": [-1.01596829346, 0.23845782520925, 1.23293754928234]
}
```

## AskSage.ai - Generate Report

The AskSage.ai - Generate Report action queries an AskSage Dataset to generate a report based on the organization's specific requirements.

POST <https://api.asksage.ai/server/query>

### Sample Response:

```
{
  "status": 200,
  "response": "<The generated report>",
  "references": ["[1] Source Content 1", "[2] Source Content 2"]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
N/A	Report.Value	N/A	N/A	Generated Report for <code>{{ topic_or_dataset }}</code> on <code>{{ date }}</code>	The title is generated using the user-field configured topic/dataset and the current date.
N/A	Report.Attribute	Dataset	N/A	<code>{{ topic_or_dataset }}</code>	The Attribute is generated using the user-field configured topic/dataset.
.response	Report.Description	N/A	N/A	N/A	The LLM's response to the prompt.
.references[]	Report.Description	N/A	N/A	N/A	Added to the description, under the response.



# 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.

## Generate Report

METRIC	RESULT
Run Time	1 minute
Reports	1
Report Attributes	1

# Use Case Example

**Premise:** I am an Analyst that wants to get weekly reports on the latest happenings with a threat actor targeting my organization, FIN7. I already have blog posts, news, and threat reports being ingested into my Threat Library as reports.

## Training a Dataset

1. I create a Threat Library data collection targeting those reports, but only the ones that mention FIN7.
2. I create and enable a workflow that uses the AskSage.ai - Train Dataset action to train a dataset on the FIN7 reports.
3. I reload my Threat Library data collection, and run the workflow I just created.



The selected reports will be sent to your AskSage.ai tenant for processing and training.

## Generating a Report

1. I create a new workflow that uses the AskSage.ai - Generate Report action.
2. In the action's configuration, I select the same FIN7 Dataset that I trained in the previous step I do this by entering the same name for the Topic / Dataset field as I did for the training action.
3. I provide a system prompt and a prompt for the model to generate the report I enable and run the workflow to generate the report.
4. I wait up to a couple of minutes for the report to be generated and indexed in the Threat Library.
5. I open my Threat Library to the Report objects and find the generated report by searching for reports with the source, AskSage.ai and review the it to see the insights generated by the model

---

## Known Issues / Limitations

- Both actions, **Train Dataset** and **Generate Reports**, will use your allocated AskSage tokens. Because of this, the action can currently only be run manually. You can invoke the actions from the Threat Library, an Object Details page, or the Workflow configurator page. This is to ensure that you understand what you are sending to AskSage and prevent accidental overuse of your tokens.

# Change Log

- Version 1.0.0
  - Initial release