

ThreatQuotient

A Securonix Company



ThreatQ Integration Health Alerts Action

Version 1.0.0

October 20, 2026

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147



ThreatQ Supported

Support

Email: tq-support@securonix.com

Web: <https://ts.securonix.com>

Phone: 703.574.9893

Contents

Warning and Disclaimer	3
Support	4
Integration Details	5
Introduction	6
Prerequisites	7
Creating a Microsoft Teams Webhook URL	7
Creating a Slack Webhook URL	7
Installation	9
Configuration	10
Actions	12
How the Integration Works	12
Requirements	12
Known Issues / Limitations	13
Change Log	14

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 © 2026 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: tq-support@securonix.com

Support Web: <https://ts.securonix.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	>= 6.13.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The ThreatQ Integration Health Alerts Action monitors integrations for health issues and sends alerts to your team through Microsoft Teams or Slack when problems are detected. This helps teams identify and address issues that could disrupt intelligence flows and security operations.

The integration provides the following action:

- **Send Feed Health Alerts** - monitors ThreatQ for any feed health issues and sends alerts to Microsoft Teams or Slack when problems are detected.

The integration is compatible with ThreatQ report objects.



This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

The following is required to run the integration:

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one report object.
- A Microsoft Teams or Slack webhook URL for sending alerts.

Creating a Microsoft Teams Webhook URL

To create a Microsoft Teams Webhook URL, follow the instructions in the [Microsoft Teams documentation](#), or use these steps:

1. In Microsoft Teams, open the channel where you want to receive alerts. The channel must be public because incoming webhooks cannot post to private channels.
2. Select the ellipsis (. . .) next to the channel name, then select **Workflows**.
3. In the **Find workflows** search bar, enter **Send webhook alerts to a chat**, then select the workflow.
4. Follow the prompts to create a connection with your Microsoft Teams account or workspace, then select **Next**.
5. In the **Details** section, use the **Microsoft Teams Group chat** dropdown to select the channel for alerts, then select **Add workflow**.

After the workflow is added, Teams displays a **Workflow added successfully** message with the Webhook URL. Copy the URL and enter it in the action's [configuration](#) to enable Microsoft Teams alerts.

Creating a Slack Webhook URL

To create a Slack Webhook URL, follow the instructions in the [Slack documentation](#), or use these steps:

1. Sign in to Slack in your browser.
2. Open the [Slack Apps page](#) and select **Create New App**.
3. In the **Create an app** dialog, select **From scratch**.
4. Enter an **App Name** (for example, *ThreatQ Alerts*), select the Slack workspace where you want to receive alerts, and select **Create App**.
5. In the left sidebar, under **Features**, select **Incoming Webhooks**.

-
6. Turn on **Activate Incoming Webhooks**.
 7. Select **Add New Webhook** at the bottom of the page.
 8. From the **Channel for webhook** dropdown, select the channel where you want to receive alerts, then select **Allow**.

Your new Webhook URL will appear under **Webhook URLs for Your Workspace**. Copy it and enter it in the action's [configuration](#) to enable Slack alerts.

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
ThreatQ Domain / IP	This parameter is required. Enter the domain for your ThreatQ instance, such as <code>mytenant.threatq.com</code> , so alerts can include links to relevant ThreatQ pages. The default value is <code><tenant>.threatq.online</code> .
Alert for Trigger Types	This parameter is required. Select the feed run trigger types for which you want to receive alerts. Available options are Scheduled (<i>default</i>) and Manual .
Send Slack Alerts	Enable this option to send alerts to the configured Slack channel using its webhook URL.
Slack Webhook URL	Enter the Slack Webhook URL configured to post messages to the desired channel.
	 This parameter is only accessible if you have enabled the Send Slack Alerts parameter.

PARAMETER	DESCRIPTION
Send Microsoft Teams Alerts	Enable this option to send alerts to the configured Microsoft Teams using its webhook URL.
Microsoft Teams Webhook URL	Enter the Microsoft Teams Webhook URL configured to post messages to the desired channel. This channel must be a public channel.  This parameter is only accessible if you have enabled the Send Microsoft Teams Alerts parameter.
Objects per Run	This required parameter defines the number objects to enrich per run. Due to the nature of this action, the default value is 1.  Do not modify the default 1 value for any reason.

- 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
Send Feed Health Alerts	Monitors ThreatQ for any feed health issues and sends alerts to Microsoft Teams or Slack when problems are detected.	Report	N/A

How the Integration Works

The ThreatQ Integration Health Alerts Action monitors feeds for health issues and sends alerts to Microsoft Teams or Slack when a feed completes with errors or stops unexpectedly with a **Run Failed** error. The action runs through a workflow and requires the configured Threat Library Data Collection to return at least one **Report**, even though it does not use the Report's data.

Requirements

1. Create a dedicated Data Collection that always returns at least one **Report**. To reduce the amount of data retrieved and improve run time, configure it to target a specific Report. Do not use this Data Collection in other workflows.
2. In the workflow settings, enable **Allow data to be reprocessed** and set its value to $\emptyset$. This allows the workflow to run repeatedly on the same data without requiring new items in the Data Collection.
3. Set the workflow schedule to **Hourly** for the most frequent health alerts.

Known Issues / Limitations

- The action requires the configured Threat Library Data Collection to return at least one **Report** for the workflow to run, even though it does not use the Report's data. If the collection returns no Reports, the workflow will not run and feed health alerts will not be sent.
- **Alert Coverage Limitation:** Alerts are generated only for issues detected in CDFs (feeds). Issues with Operations, Custom Connectors, and TQO Workflow Actions do not trigger alerts.

Change Log

- **Version 1.0.0**
 - Initial release