

# ThreatQuotient



## ThreatQuotient for Broadcom Content Analysis and Sandboxing Operation User Guide

Version 1.0.0

October 24, 2023

**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
- Installation..... 7
- Configuration ..... 8
- Actions ..... 9
  - Scan..... 10
    - Action Parameters..... 10
  - Sandbox..... 11
    - Action Parameters..... 11
- Known Issues / Limitations ..... 12
- Change Log ..... 13

# 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 © 2023 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	>= 3.6.0
Support Tier	ThreatQ Supported

# Introduction

The Broadcom Content Analysis and Sandboxing (CAS) operation allows a ThreatQ user to submit files to Broadcom's Content Analysis System. You can either submit a file to Broadcom CAS, which will give you scan and reputation information or you can submit a file directly to the sandbox (Bluecoat), which will return a risk score and other sandbox details. The operation can then be used to retrieve PDF reports from Broadcom CAS.

The operation provides the following actions:

- **Scan** - scans a file by sending it to CAS. A report will be returned to the operation window and a PDF report will be uploaded to ThreatQ and related to the sample.
- **Sandbox** - sends a file or attachment to CAS Sandbox.



This operation was formerly known as **Symantec Content Analysis System (CAS)** operation.

# 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. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Host URL	The Host or IP of your CAS instance.
API Token	Your API token from CAS.
MAA Host URL	<p>The Host or IP of your MAA instance.</p> <div>  <p>This host may be the same as your CAS instance. This is an option in case your MAA appliance is different than your CAS instance.</p> </div>
MAA API Token	<p>Your API token from MAA.</p> <div>  <p>This token may be the same as your CAS token.</p> </div>
Username	The user's username to use as an "owner" for the samples.

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. 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	OBJECT SUBTYPE
<a href="#">Scan</a>	Scans a file by sending it to CAS. A report will be returned to the operation window and a PDF report will be uploaded to ThreatQ and related to the sample.	File	N/A
<a href="#">Sandbox</a>	Sends a file or attachment to CAS Sandbox.	File	N/A

## Scan


The Scan action allows you to scan a file by sending it to CAS. A report will be returned to the operation window and a PDF report will be uploaded to ThreatQ and related to the sample.

The following fields/sections parsed from the Scan action are supported:

- File Reputation
- Cylance
- Policy
- Symantec
- Sophos
- Last Line
- Fire Eye
- Kaspersky
- Malware Analysis
- Cloud Sandboxing
- Score
- MD5/SHA-1/SHA-256
- User Hash List

## Action Parameters

The Scan action offers the following configuration parameters:

PARAMETER	DESCRIPTION
<b>Sensitivity Level</b>	This controls the threshold and aggressiveness at which Advanced Machine Learning (AML) file blocking occurs. With a high detection sensitivity, AML will be aggressive in its determination of whether a file may be a threat, at the risk of blocking files that may not actually be malicious. With a lower sensitivity, AML will block fewer files, but with a risk of some threats not being detected.
<b>Response Wait Timeout</b>	<p>The amount of time (in milliseconds) to wait for a scan to be finished.</p> <div>  <p>This option can be ignored, as it is just informing the user that the operation may take more than 30 seconds to run, depending on the scan. The operation runs synchronously with CAS, and waits for the scan to be finished.</p> </div>

## Sandbox

The Sandbox action allows a user to send a file or attachment to CAS's Sandbox (known as MAA). This action will upload the sample and then create a task for that sample. The Task ID will be stored in the ThreatQ Object's attributes, so that you can query for the reports later

### Action Parameters

The Scan action offers the following configuration parameters:

PARAMETER	DESCRIPTION
<b>Sandbox Environment</b>	This option allows a user to change the type of sandbox environment to use. By default, this is set to <b>sbx</b> , which is a simulated windows environment.
<b>IVM Profile Name</b>	Enter in your IVM profile name if you have selected ivm as the sandbox environment.
<b>Priority</b>	Set the priority of the sandbox task. The default setting is Medium.
<b>Description</b>	Give the sample a description.
<b>Sample Label</b>	Set the sample a label. This field is optional.
<b>Filename</b>	The file name can be overridden here and new sample's filename given.
<b>File Extension</b>	Override a sample's file extension.
<b>Execution Arguments</b>	Override a tasks' execution arguments.
<b>Resubmit the Sample</b>	If this is set to Yes, the operation will submit the sample to the sandbox even if has already submitted it. Setting this to No will prevent samples from being resubmitted (if already submitted)

## Known Issues / Limitations

- If a returned result says None, this means the response timed out. This is a limitation of the Broadcom CAS API endpoint, not the operation. This does not mean that the file was not scanned. The file will still be scanned and if it is deemed malicious, it will show up as a threat within Broadcom CAS. Increasing the Response Wait Time parameter may fix the issue, but it is not a guarantee.
- This action waits for Broadcom to return scanning results, so running this action may take more than 30 seconds. We cannot save a scan ID and fetch the results later because the Broadcom CAS API does not provide us with the required endpoints for that.
- The results of this action are not always consistent. For instance, sometimes a scan may return results from Kaspersky. If scanned again, Kaspersky results are not guaranteed to be returned. This is not a limitation of the operation, but rather, of the Broadcom CAS API.

# Change Log

- Version 1.0.0
  - Initial release