

ThreatQuotient



FireEye AX Operation Guide

Version 1.0.2

November 22, 2021

ThreatQuotient

11400 Commerce Park Dr., Suite 200
Reston, VA 20191

 ThreatQ Supported

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

Support	4
Versioning.....	5
Introduction	6
Installation.....	7
Configuration	8
Actions	10
Submit.....	11
Result Example.....	12
Get Reports	13
Result Example.....	13
Related Report Example	13
Detected Malware Example	14
Malicious Alerts Example.....	14
API Calls Example.....	15
Add YARA Rule	16
Successful Result Example	16
Unsuccessful Result Example.....	17
Remove YARA Rule.....	18
Successful Result Example	18
Unsuccessful Result Example.....	19
Query Alerts	20
Result Example.....	22
Change Log.....	23

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 © 2021 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.

Versioning

- Current integration version 1.0.2
- Compatible with ThreatQ versions \geq 4.10.0

Introduction

The ThreatQuotient for FireEye AX Operation provides a ThreatQ user with the ability to interact with their FireEye AX appliance.

Users can submit files for analysis, as well as retrieve the reports back so the results can be added to ThreatQ as context.

ThreatQ users can also query their FireEye AX appliance using indicators from ThreatQ to find any alerts related to those indicators. The operation also allows you to seamlessly add and remove YARA rules from their FireEye AX appliance.

The operation can be run on the following object types:

- Files
- Indicators (Email Address, FQDN, IP Address, MD5, URL)
- Signatures (YARA Rule)

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 feed 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.

6. 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).



If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER

DESCRIPTION

Host URL

The Host or IP of your FireEye AX instance.

Username

Your FireEye AX username for the API.

Password

Your FireEye AX password for the API.

Profiles

The sandboxing profiles to use to sandbox the samples.

Example: win-7sp1m - see the FireEye AX UI for more options.


You can specify multiple profiles using a comma-separated format.



This parameter can be overridden using action-specific parameters.


Configuration

Host Url



Username

Password



Profiles

☐ Bypass system proxy configuration for this operation

Save

5. Click **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable the operation.

Actions

The FireEye AX Operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUB-TYPE
Submit	Submits a file or URL/FQDN to FireEye AX.	File, Indicator	File, URL, FQDN
Get Reports	Retrieves all reports for the sample from FireEye AX.	File, Indicator	File, URL, FQDN
Add YARA Rule	Adds a YARA rule to ThreatQ from FireEye AX.	Signature	YARA
Remove YARA Rule	Removes YARA rules from ThreatQ.	Signature	YARA
Query Alerts	Queries alerts in FireEye AX.	Indicator, File	FQDN, Filename, Email, IP Address

Submit

The Submit action will submit a file (attachment) or a URL/FQDN to FireEye AX for sandboxing.

The action provides the following parameters:

PARAMETER	DESCRIPTION
Run Using Custom Application	<p>Allows you to run the sample with a specific application within the sandbox profile. This value is a number that corresponds to the custom application.</p> <p>The default setting is 0 - this tells FireEye to determine the application to use.</p>
Timeout	Determines how long the sandbox will take to "timeout" after inactivity. The default setting is 500.
Priority	<p>Sets a priority for the task. Options include:</p> <ul style="list-style-type: none">• Normal (default)• Urgent
Profiles List (overrides config)	This parameter is a list of profiles to use to sandbox the sample. The action will use the profiles set in the UI configuration if this is left blank. Otherwise, this will override the profiles listed in the UI configuration
Force	This parameter will force resubmit a sample. If this is set to False, it will mark the sample as a duplicate and will not resubmit it.
Analysis Type	Set the Analysis Type. The default setting is Sandbox.
Prefetch	Determine the file target based on an internal determination rather than browsing to the target location.

PARAMETER

DESCRIPTION



The Analysis Type must be set to **1** if you are using the Sandbox.

Operation: FireEye AX ×

Run using custom application (number; optional) ⓘ

ⓘ

Timeout ⓘ

Priority ⓘ

Profiles List (overrides config) ⓘ

Force ⓘ

Analysis Type (override; default: Sandbox) ⓘ

Prefetch ⓘ

Run Cancel

Result Example


Successfully submitted attachment to sandbox (ID: 43)

Raw Response Show


Get Reports

The Get Reports action will get all the reports for the sample, with the only condition being that the sample (in ThreatQ) has an attribute with the name "FireEye AX Submission ID" and the value will be the submission ID.

For each of these attributes, it will fetch a report correlating to the submission ID. If submission results are found, results will be shown and the full JSON report will be uploaded and related to the sample in ThreatQ

Result Example

Submission 1 Hide


Successfully uploaded related report for submission 1

Alert Information

<input type="checkbox"/> Name	Value
<input type="checkbox"/> Search	<input type="text"/>
<input type="checkbox"/> Alert URL	https://10.20.0.210/malware_analysis/analyses?malid=1
<input type="checkbox"/> Appliance ID	AC1F6B720474
<input type="checkbox"/> Occurred	2019-02-20 19:57:38 +0000
<input type="checkbox"/> Malicious	yes
<input type="checkbox"/> FireEye Name	MALWARE_OBJECT
<input type="checkbox"/> Severity	MALR
<input type="checkbox"/> Action	notified

Add Selected Attributes

Detected Malware Show

Malicious Alerts Show

File Interactions Show

Popup Windows Show

API Calls Show

Related Report Example

☐  cerber.exe-submission-1-20190220T1957.json

 FireEye AX

02/22/2019 08:14pm

Detected Malware Example

Detected Malware Hide

Detected Malware Indicators

<input type="checkbox"/>	Value	Type
<input type="checkbox"/>	<input type="text" value="Search"/>	<input type="text" value="Search"/>
<input type="checkbox"/>	8b6bc16d137c09a08b02bbe1bb7d670	MD5
<input type="checkbox"/>	e67834d1e8b38ec5864cfa101b140aeaba8f1900a6e269e6a94c90fcbfe56678	SHA-256
<input type="checkbox"/>	cerber.exe	Filename

Add Selected Indicators

Detected Malware Attributes

<input type="checkbox"/>	Name	Value
<input type="checkbox"/>	<input type="text" value="Search"/>	<input type="text" value="Search"/>
<input type="checkbox"/>	Name	Ransomware.Cerber
<input type="checkbox"/>	SType	avs
<input type="checkbox"/>	Type	exe
<input type="checkbox"/>	Name	Trojan.Cerber.FEC3
<input type="checkbox"/>	SType	vm-bot-command
<input type="checkbox"/>	Name	fe_ml_heuristic

Add Selected Attributes

Malicious Alerts Example

Malicious Alerts Hide

Malicious Alerts

Showing 1 to 10 of 21 Row count: 10

<input type="checkbox"/>	Alert
<input type="checkbox"/>	<input type="text" value="Search"/>
<input type="checkbox"/>	Static Analysis fe_ml_heuristic
<input type="checkbox"/>	Static Analysis
<input type="checkbox"/>	Static Analysis Ransomware.Cerber
<input type="checkbox"/>	Static Analysis Trojan.Cerber.FEC3
<input type="checkbox"/>	Direct disk access
<input type="checkbox"/>	Suspicious Wmiquery Executed
<input type="checkbox"/>	Suspicious WMI Query
<input type="checkbox"/>	Malicious Cerber Indicator
<input type="checkbox"/>	Ransomware Activity
<input type="checkbox"/>	Suspicious Ransom PT-C

Previous Next

Add Selected Attributes

API Calls Example

API Calls

Hide

API Calls

Showing 1 to 10 of 10

Row count: 25

<input type="checkbox"/>	API
	<input type="text" value="Search"/>
<input type="checkbox"/>	GetSystemDirectoryW
<input type="checkbox"/>	GetComputerNameA
<input type="checkbox"/>	CryptAcquireContextW
<input type="checkbox"/>	GetTokenInformation
<input type="checkbox"/>	GetSystemDirectoryA
<input type="checkbox"/>	GetComputerNameExW
<input type="checkbox"/>	Sleep
<input type="checkbox"/>	GetVolumeNameForVolumeMountPointW
<input type="checkbox"/>	ShellExecuteW
<input type="checkbox"/>	GetComputerNameW

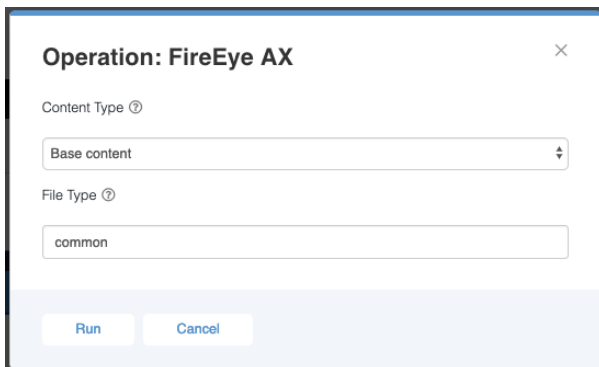
Add Selected Attributes

Add YARA Rule

The Add YARA Rule action allows you to add YARA rules from ThreatQ to FireEye AX.

The action provides the following parameters:

PARAMETER	DESCRIPTION
Content Type	<p>Specify which content type the new YARA rule should be applied to. Options include:</p> <ul style="list-style-type: none">• Active content: Extracts the macros from files and executes special YARA rules on them.• Base (default): If file contains a macro, don't extract and analyze macros; only analyze the base file.• All: Does both
File Type	<p>The file type of the YARA rules file being submitted, such as exe, pdf, or ppt. The default setting is Common.</p>



Operation: FireEye AX

Content Type ⓘ

Base content

File Type ⓘ

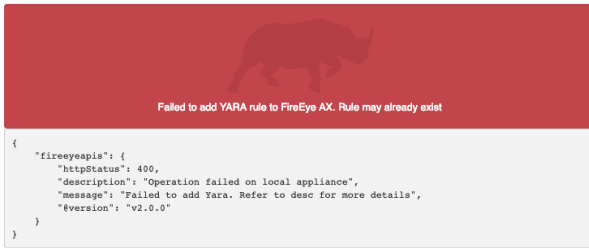
common

Run Cancel

Successful Result Example



Unsuccessful Result Example

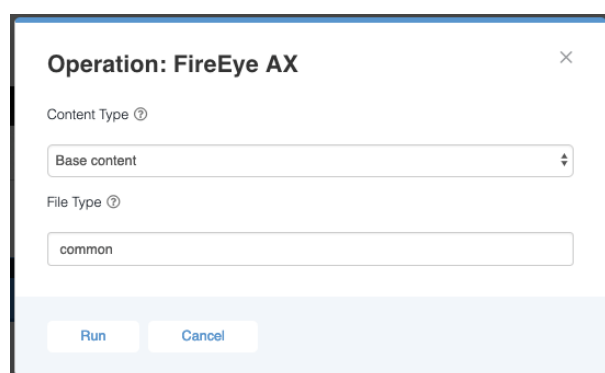


Remove YARA Rule

The Remove YARA Rule action allows you to remove YARA rules from ThreatQ.

The action provides the following parameters:

PARAMETER	DESCRIPTION
Content Type	<p>Specify which content type the new YARA rule should be applied to. Options include:</p> <ul style="list-style-type: none">• Active content: Extracts the macros from files and executes special YARA rules on them.• Base (default): If file contains a macro, don't extract and analyze macros; only analyze the base file.• All: Does both
File Type	<p>The file type of the YARA rules file being submitted, such as exe, pdf, or ppt. The default setting is Common.</p>



Operation: FireEye AX

Content Type ⓘ

Base content

File Type ⓘ

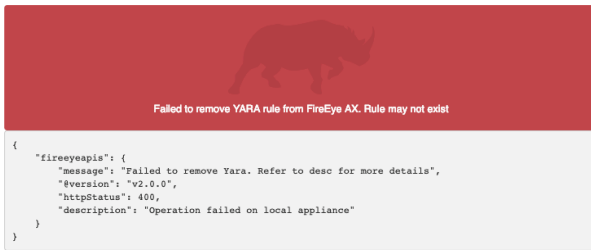
common

Run Cancel

Successful Result Example



Unsuccessful Result Example




Query Alerts

The Query Alerts action allows you to query alerts in FireEye AX.



This action only applies to FQDNs, Filenames, Emails, and IP Addresses.

The action provides the following parameters:

PARAMETER	DESCRIPTION
Start Time	<p>Set the start time to search for alerts. This is used in conjunction with the <code>Duration</code> parameter. You cannot use this at the same time as using the <code>End Time</code> parameter</p> <ul style="list-style-type: none">• Format: YYYY-MM-DDTHH:mm:ss.sss-OH:om• Example: 2019-02-21T16:30:00.000-07:00
End Time	<p>Set the end time to search for alerts. This is used in conjunction with the <code>Duration</code> parameter. You cannot use this at the same time as using the <code>Start Time</code> parameter.</p> <ul style="list-style-type: none">• Format : YYYY-MM-DDTHH:mm:ss.sss-OH:om• Example: 2019-02-21T16:30:00.000-07:00 <div> If no end time or start time is provided, the end time will be set to the current date/time</div>
Duration	<p>Set the amount of time you want to either look after a start time or before an end time. The default setting is 12 hours.</p>
Info Level	<p>Set the detail level of the alerts. Options include:</p> <ul style="list-style-type: none">• Concise (default)• Normal• Extended

PARAMETER

DESCRIPTION



Normal and Extended options will provide a very large alert and may take longer to download.

Operation: FireEye AX ×

Start Time (optional; example: 2019-02-25T19:26:28.000+00:00) ?

End Time (optional; example: 2019-02-25T19:26:28.000+00:00) ?

Duration (How much time after/before start date/end date to look) ?

Info Level ?

Notes ?

- You cannot use the start date and end date options together
- Start Date and End Date are optional
- When searching for MD5s the API will ignore any duration/dates
- If no start or end date is set, the end date will default to the current date/time

Result Example

Total alerts found: 1

Alert 1

Alert Information

<input type="checkbox"/>	Name	Value
<input type="checkbox"/>	<input type="text" value="Search"/>	<input type="text" value="Search"/>
<input type="checkbox"/>	Alert URL	https://10.20.0.210/malware_analysis/analyses?maid=1
<input type="checkbox"/>	Appliance ID	AC1F6B720474
<input type="checkbox"/>	Occurred	2019-02-20 19:57:39 +0000
<input type="checkbox"/>	Severity	MAJR
<input type="checkbox"/>	Action	notified
<input type="checkbox"/>	Malicious	yes
<input type="checkbox"/>	FireEye Name	MALWARE_OBJECT

Add Selected Attributes

Detected Malware

Show

Raw Response

Show

Change Log

- **Version 1.0.2**
 - Fixed an issue where users were unable to add attributes for certain tables.
- **Version 1.0.1**
 - Fixed an issue with mapping popup windows.
 - Added failsafe to mapper to improve stability.
- **Version 1.0.0**
 - Initial Release