ThreatQuotient

Trellix EX Operation Guide

Version 1.1.0

February 22, 2023

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

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.

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	>= 4.31.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/trellix-ex-operation

Introduction

The ThreatQuotient for Trellix EX Operation allows you to search for emails alerts in a Trellix EX appliance that contains specific indicators. If any alerts are returned, the data and indicators are parsed and listed in the ThreatQ UI.

The operation provides the following action:

- **Search for Alerts** - submits data to Trellix EX and returns matching alerts.
- **Search for Indicators** - searches for Trellix EX alerts containing Malware or URL/Filename indicators.

The operation is compatible with the following object types:

- Indicators (Email Address, Filename, MD5, URL)
- Malware

> ⚠ The Trellix EX operation replaces the FireEye EX operation as of version 1.1.0.

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.

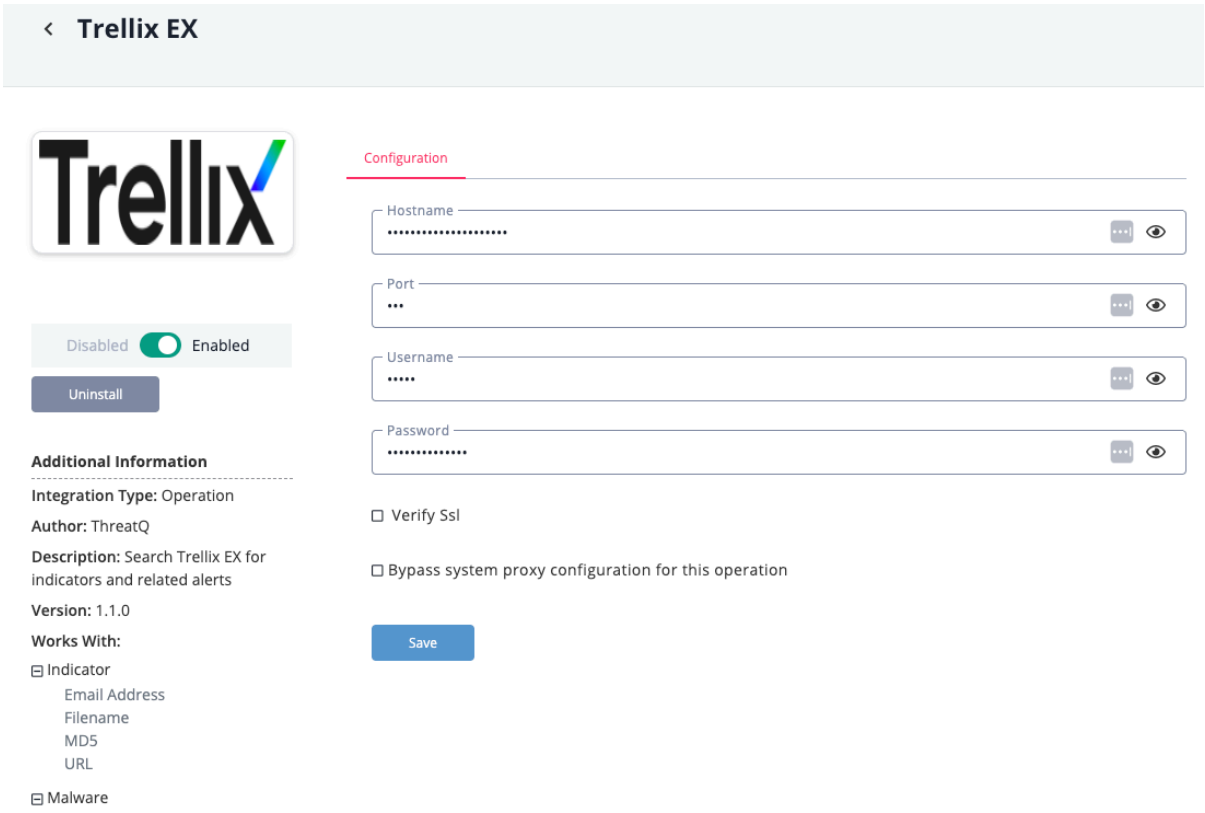
Configuration

> 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
Hostname	Your Hostname or IP address of Trellix EX.
Port	The Communication port. The default value is 443.
Username	Your Username for connecting to Trellix.
Password	Your Password for authenticating with Trellix.
Verify SSL	Enable this parameter to verify SSL when connecting to the Trellix EX instance.



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
Search for Alerts	Searches for Trellix EX alerts containing indicators on MD5 and Email Address.	Indicator	MD5, Email Address
Search for Alerts with Indicator	Searches for Trellix EX alerts containing Malware or URL/ Filename indicators	Indicator, Malware	Indicator (Email Address, Filename, MD5, URL)

Search For Alerts, Search for Alerts with Indicator

The Search for Alerts and Search for Alerts with Indicator actions utilize the same endpoint and responses while specific filtering parameters are available based on the object type.

```
GET https://{hostname}/wsapis/v2.0.0/alerts/{filtering_parameters}
```

Sample Response:

```
    {
    "alert": [],
    "appliance": "eMPS",
    "version": "eMPS (eMPS) 8.4.2.888088",
    "msg": "extended",
    "alertsCount": 0
}
```

ThreatQ provides the following default mapping for these actions:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.alert[].alertUrl	Indicator.Attribute	Trellix Alert URL	N/A	N/A	N/A
.alert[].severity	Indicator.Attribute	Severity	N/A	N/A	N/A
.alert[].src	Indicator.Attribute	Email Sender	N/A	N/A	N/A
.alert[].src	Related Indicator	Email Address	N/A	N/A	N/A
.alert[].explanation.osChanges[].network.ipaddress	Related Indicator	IP Address	N/A	N/A	N/A
.alert[].explanation.malwareDetected.malware[].md5Sum	Related Indicator	MD5	N/A	N/A	N/A
.alert[].explanation.malwareDetected.malware[].md5sum	Related Indicator	MD5	N/A	N/A	N/A
.alert[].explanation.malwareDetected.malware[].sha1	Related Indicator	SHA-1	N/A	N/A	N/A
.alert[].explanation.malwareDetected.malware[].sha256	Related Indicator	SHA-256	N/A	N/A	N/A
.alert[].explanation.malwareDetected.malware[].sha256sum	Related Indicator	SHA-256	N/A	N/A	N/A
.alert[].explanation.malwareDetected.malware[].url	Related Indicator	URL	N/A	N/A	N/A
.alert[].explanation.malwareDetected.malware[].fqdn	Related Indicator	FQDN	N/A	N/A	N/A
.alert[].explanation.malwareDetected.malware[].domain	Related Indicator	FQDN	N/A	N/A	N/A
.alert[].explanation.malwareDetected.malware[].src_ip	Related Indicator	IP Address	N/A	N/A	N/A

Configuration Options

The two operation actions provide their own configuration options upon run.

Search for Alerts

The Search for Alerts provides the following configuration options:

PARAMETER	DESCRIPTION
The ID Number for the Alert to Retrieve	Enter the ID number of the alert to retrieve.

Search for Alerts with Indicator

The Search for Alerts with Indicator provides the following configuration options:

PARAMETER	DESCRIPTION
Enter the Start Time for the Search	Enter the Start Time of the search in the timezone of the Trellix EX appliance in the following format: YYYY-MM-DD HH:MM
Enter the End Time for the Search	Enter the End Time of the search in the timezone of the Trellix EX appliance in the following format: YYYY-MM-DD HH:MM
The ID Number for the Alert to Retrieve	Enter the ID number of the alert to retrieve.

Filter Options per Object Type

The operation supports different filters for each of the objects it is executed on. The following table lists the supported filters.

OBJECT TYPE	ACTION	SUPPORTS TIME FILTERING	SUPPORTS ALERT ID FILTERING (OPTIONAL)
URL	Search for alerts containing URL.	Yes	Yes
MD5	Search for alerts that contain MD5 hash.	No	Yes
Email Address	Search for alerts that match the email address of the malware object sender.	No	Yes
Filename	Search for alerts that contain a malware filename that matches the ThreatQ indicator.	Yes	Yes
Malware Name	Search for alerts that contain a specific malware.	Yes	Yes

Change Log

- Version 1.1.0
  - Resolved import errors.
  - Rebranded operation from FireEye to Trellix to match provider's naming scheme.
- Version 1.0.0
  - Initial release