ThreatQuotient

Joe Sandbox CDF Guide

Version 1.0.0

May 16, 2022

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

Not Actively Supported

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 **Not Actively Supported**.

Integrations, apps, and add-ons designated as **Not Actively Supported** are not supported by ThreatQuotient's Customer Support team.

While you can report issues to ThreatQ's Customer Support team regarding the integration/app/add-on, you are solely responsible for ensuring proper functionality and version compatibility of Not Supported designations with the applicable ThreatQuotient software.

If unresolvable functional or compatibility issues are encountered, you may be required to uninstall the integration/app/add-on from your ThreatQuotient environment in order for ThreatQuotient to fulfill support obligations.

> ⚠ For ThreatQuotient Hosted instance customers, the Service Level Commitment and Service Level Credit in the ThreatQuotient Service Level Schedule will not apply to issues caused by Not Actively Supported integrations/apps/add-ons.

Versioning

- Current integration version: `1.0.0`
- Compatible with ThreatQ versions >= `4.40.0`

Introduction

The Joe Sandbox CDF for ThreatQ enables analysts to automatically ingest analysis reports for samples submitted to Joe Sandbox.

The integration provides the following feed:

- **Joe Sandbox Submissions** - pulls analysis reports for samples submitted to Joe Sandbox.

The integration ingests the following system objects:

- Reports
- Indicators
- Malware

Along with the system objects listed above, the integration ingests the following support context:

- Joe Sandbox Link
- Disposition
- Classification
- Threat Score
- Related Malware
- Tags
- Comments
- Sample MD5 Hash
- Sample SHA-1 Hash
- Sample SHA-256 Hash
- Sample Filename / URL
- Sandbox Environment
- Sandbox Script
- Triggered YARA Rule
- Triggered Sigma Rule

Prerequisites

The Joe Sandbox CDF integration for ThreatQ requires the following:

- A Joe Sandbox API Key which can be located under User Settings for your Joe Sandbox account.

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 feed 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 feed and will require user confirmation before proceeding.
6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to configure and then enable the feed.

Configuration

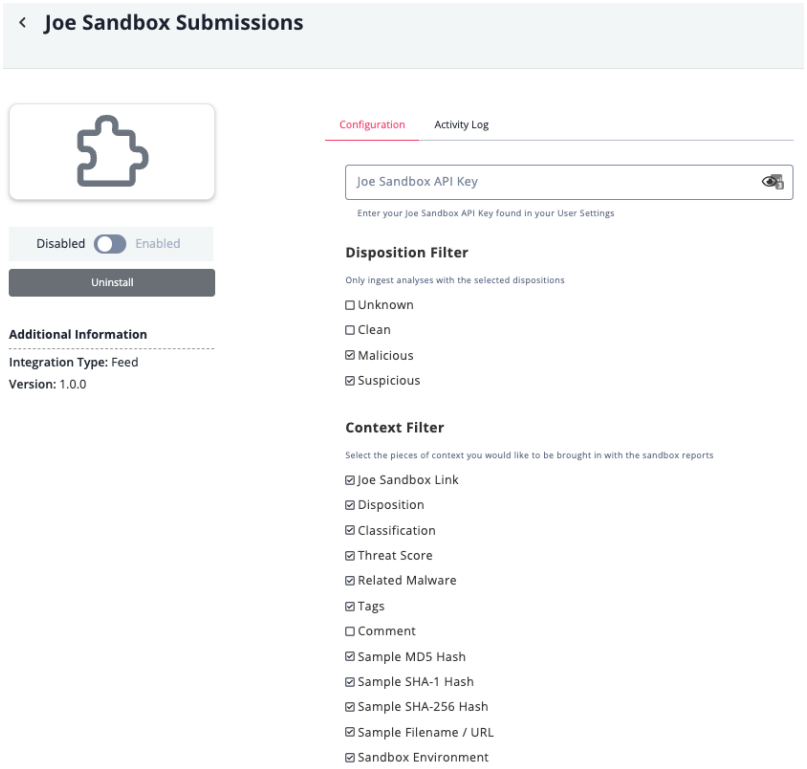
> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).
3. Click on the integration to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Joe Sandbox API Key	Your Joe Sandbox API Key. This can be found under your User Settings in Joe Sandbox site.
Disposition Filter	Select the dispositions to ingest analysis for in ThreatQ. Options include: ◦ Unknown ◦ Clean ◦ Malicious (default) ◦ Suspicious (default)
Context Filter	Select the pieces of context you would like to be brought in with the sandbox reports. Options include: • Joe Sandbox Link (default) • Disposition (default) • Classification (default) • Sample SHA-1 Hash (default) • Sample SHA-256 Hash (default) • Sample Filename / URL (default)

PARAMETER	DESCRIPTION
	• Threat Score (default) • Related Malware (default) • Tags (default) • Comments • Sample MD5 Hash (default) • Sandbox Environment (default) • Sandbox Script • Triggered YARA Rule • Triggered Sigma Rule



5. Review the **Settings** configuration, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Change Log

- **Version 1.0.0**
  - Initial release