ThreatQuotient

ANY.RUN CDF Guide

Version 1.0.0

May 17, 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 >= `4.34.0`

Introduction

The ANY.RUN CDF for ThreatQ enables a ThreatQ user to automatically ingest malware samples, malware analysis reports, and related IOCs from samples that your organization submitted to ANY.RUN. The integration then parses the data and ingests it into ThreatQ.

The integration provides the Any.Run feed, which utilizes five endpoints when performing a run:

- **Analysis Endpoint (JSON) -** Returns a rolling history of your organization's submissions to the ANY.RUN sandbox. It does not include the actual reports
- **Report Endpoint (JSON) -** Returns the actual report/analysis results for a given task
- **IOC Endpoint (JSON) -** Returns IOCs related to a given analysis.
- **Analysis HTML Report (Attachment) -** Returns an HTML file containing a formatted report for the given sample. See the Known Issues / Limitations topic for important details regarding this endpoint.
- **TQ Attachments Endpoint (TQ) -** Allows you to search for an existing report for a sample to avoid uploading duplicate reports.

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.

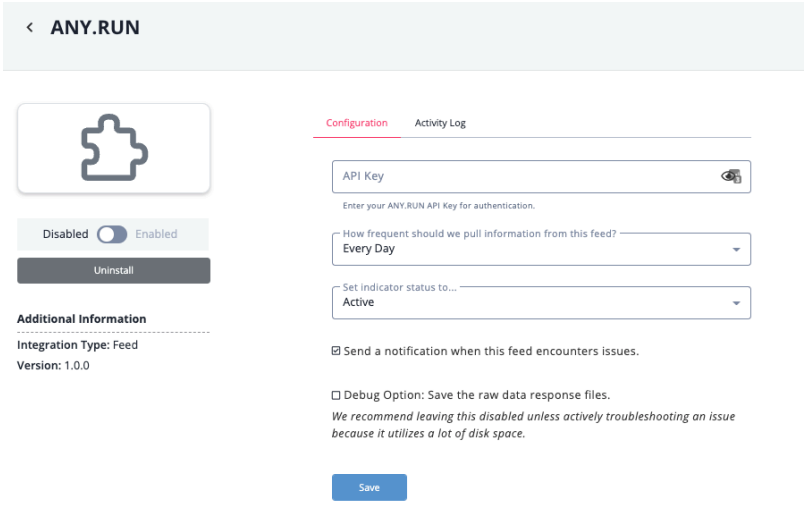
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > 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 parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
API Key	Your ANY.RUN API Key for authentication.



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.

Known Issues / Limitations

- Malware samples and malware analysis reports are not related to each other. This is caused by a limitation with attachments endpoint.
- The `Analysis Endpoint` (history) does not allow you to filter by date. As a result, you will need to filter by date within the filter section of the CDF. Another limitation is that the endpoint returns a single date field. This date reflects the date the sample was submitted. There is no date when the analysis was finished, and the analysis will only appear in the `Analysis Endpoint` when the analysis is finished. This may result in missing reports.

Change Log

- **Version 1.0.0**
  - Initial Release