ThreatQuotient

RST Noise Control Action User Guide

Version 1.0.0

November 26, 2024

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

Developer Supported

Support
Email: support@rstcloud.net
Web: N/A
Phone: N/A

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 **Developer Supported**.

Support Email: support@rstcloud.net
Support Web: N/A
Support Phone: N/A

Integrations designated as **Developer Supported** are supported and maintained by the developer who submitted the integration to the ThreatQ Marketplace. The developer's contact information can be found on the integration's download page within the Marketplace as well as in this guide.

You are responsible for engaging directly with the developer of Developer Supported integrations/ apps/add-ons to ensure proper functionality and version compatibility with the applicable ThreatQuotient Software.

If functional or compatibility issues that may arise are not resolved, you may be required to uninstall the app or add-on from their 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 for any issues caused by Developer Supported integrations/apps/add-ons.

ThreatQuotient reserves the right to remove the Developer-Supported designation of third-party apps and add-ons if the developer is not, in ThreatQuotient's determination, fulfilling reasonable obligations for support and maintenance.

> Failure by the developer to update compatibility of an app or add-on within 90 days of the release of a new version of applicable ThreatQuotient Software will result in reclassification to Not Actively Supported.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 5.6.0
ThreatQ TQO License Required	Yes
Support Tier	Developer Supported

Introduction

The RST Noise Control Action integration sends a collection of indicators to RST to automatically check if the indicators are likely to create noise when used for real-time detection or may cause problems when applied for prevention.

The integration provides the following action:

- **RST Noise Control** - retrieves the benign state of an indicator from RST Cloud and ingests it into the ThreatQ platform.

The action is compatible with, enriches, and returns the following indicator types:

- FQDN
- IP Address
- URL
- MD5
- SHA-1
- SHA-256

This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one of the following indicator types:
  - FQDN
  - IP Address
  - URL
  - MD5
  - SHA-1
  - SHA-256
- A RST API Key and RST URL to perform indicator Lookups.

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 action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
    - Drag and drop the zip file into the dialog box
    - Select **Click to Browse** to locate the zip file on your local machine

> ThreatQ will inform you if the action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

You will still need to configure the action.

Configuration

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

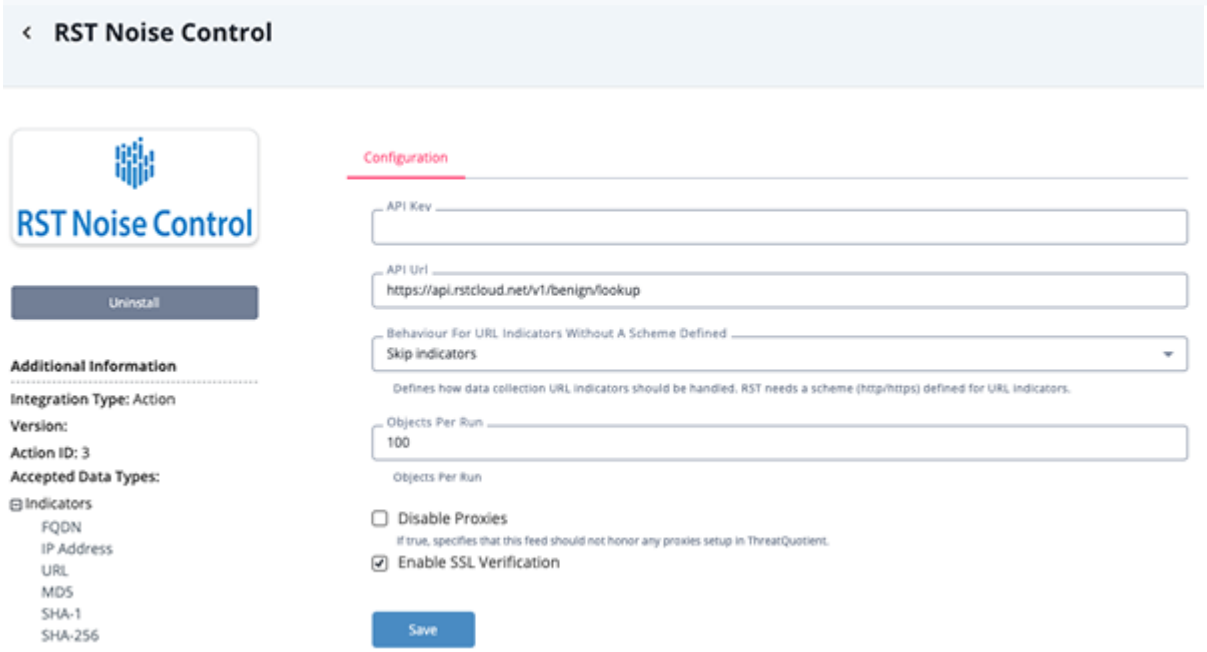
To configure the integration:

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

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
API Key	You r RST API Key.
API Url	Your RST API URL used for indicator lookup.
Behavior for URL Indicators without a Scheme Defined	Defines how data collection URL indicators without a scheme should be handled. Options include: ◦ Skip Indicators ◦ Add "http" ◦ Add "https" ⚠ RST needs a scheme (http/https) defined for URL indicators.
Objects per run	Enter the maximum number of objects to submit per run
Enable SSL Verification	Enable this for the action to validate the host-provided SSL certificate.

PARAMETER	DESCRIPTION
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.



5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
RST Noise Control	Checks the benign state on the RST and ingests it in TQ	Indicator	FQDN, IP Address, URL, MD5, SHA-1, SHA-256

RST Noise Control

RST Noise Control Action sends a collection of indicators to RST to automatically check if the indicators are likely to create noise when used for real-time detection or may cause problems when applied for prevention.

`GET {api_url}/{ioc}`

Sample Response:

```
{
        "benign": "false",
        "reason": "Not Found in our database",
        "type": "ip",
        "value": "77.238.245.11"
    }
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
benign	Indicator.Attribute	Benign	N/A	false	N/A
.reason	Indicator.Attribute	Reason for Benign	N/A	Not Found in our database	N/A

Enriched Data

Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

METRIC	RESULT
Run Time	1 minute
Indicators	100
Indicator Attributes	200

Use Case Example

1. A user submits a collection of indicators using the RST Noise Control action to the RST.
2. The RST checks if indicators is likely to create noise when used for real-time detection or may cause problems when applied for prevention.
3. The action enriches the indicators with attributes extracted from the provider.

Change Log

- **Version 1.0.0**
  - Initial release