ThreatQuotient

Extract FQDNs Action User Guide

Version 1.0.0

January 29, 2024

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	1.0.0
Compatible with ThreatQ Versions	>= 5.12.1
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Extract FQDNs action enables the automatic extraction of FQDNs (or IP Addresses) from URLs within your Threat Library.

The integration provides the following action:

- **Extract FQDNs** - extracts a URL's FQDN, or IP Address, add it your Threat Library, and relate it to the URL.

The action is compatible with URL type indicators.

The action returns the following enriched indicator types:

- FQDN
- IP Address

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 the following URL type indicators.

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

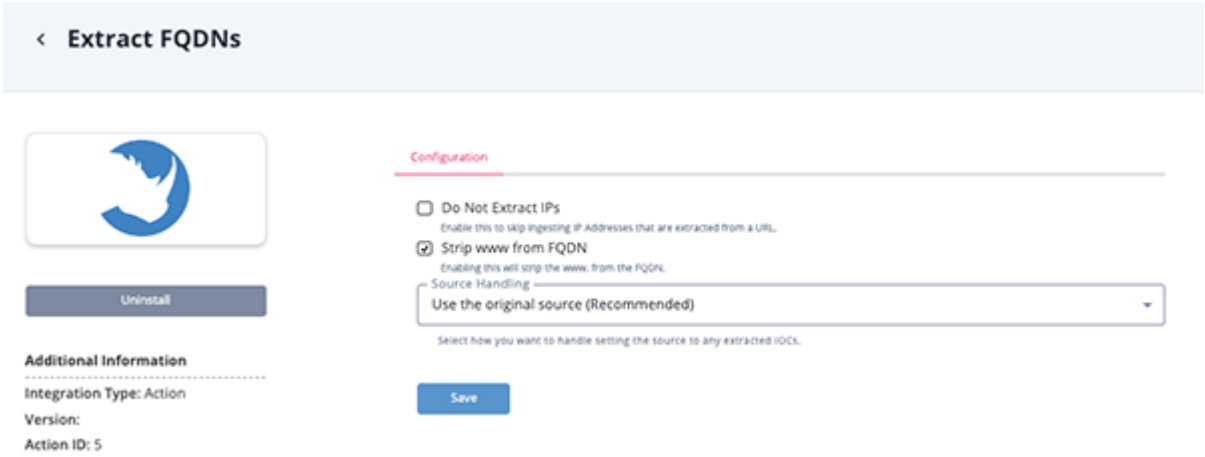
> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

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
Do Not Extract IPs	Enabling this option will result in the action skipping ingestion of IP Addresses extracted from a URL. This option is disabled by default.
Strip www from FQDN	Enabling this parameter will result in the www being stripped from the FQDN. This option is enabled by default.
Source Handling	Select how the action will handle the source of the extracted IoCs. Options include: ◦ Use the original source (default) - **this method is recommended.** ◦ Use the name of the workflow. Example: Extract FQDNs. ◦ Use both the original source and the workflow name.



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
Extract FQDNs	Extracts FQDNs and IP Addresses from a URL in a given data collection.	Indicator	URL

Extract FQDNs

The Extract FQDNs action will extract a URL's FQDN (or IP Address), add it to your Threat Library, and relate it to the URL.

> There are no samples, endpoints, or data mapping tables for this action as it works with existing data in your ThreatQ Threat Library. No additional data is submitted or ingested to/from third-party providers.

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	184

Use Case Example

I have a feed that reports URLs to my Threat Library, but do not extract or report the underlying FQDNs. I want to send the FQDNs to my DNS resolver to be blocked, but I can't because they are reported as URLs. Using this action, I can extract those FQDNs so they can be disseminated to my downstream tools for blocking.

Change Log

- **Version 1.0.0**
  - Initial release