ThreatQuotient

Darktrace Action

Version 1.0.0

October 01, 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 **3**
Support **4**
Integration Details **5**
Introduction **6**
Prerequisites **7**
Installation **8**
Configuration **9**
Actions **11**
Darktrace Export 12
Change Log **13**

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	>= 5.25.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Darktrace Action takes a Threat Library collection and exports the collection's FQDN and IP Address indicators to Darktrace.

The integration performs the following action:

- **Darktrace Export** - exports FQDN and IP Address IOCs to Darktrace and sets the expiration of the IOC based on user field input.

The action is compatible with the following indicator types:

- FQDN
- IP Address

The action does not enrich any system objects.

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
- A Darktrace Host.
- Darktrace private and public tokens.

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.

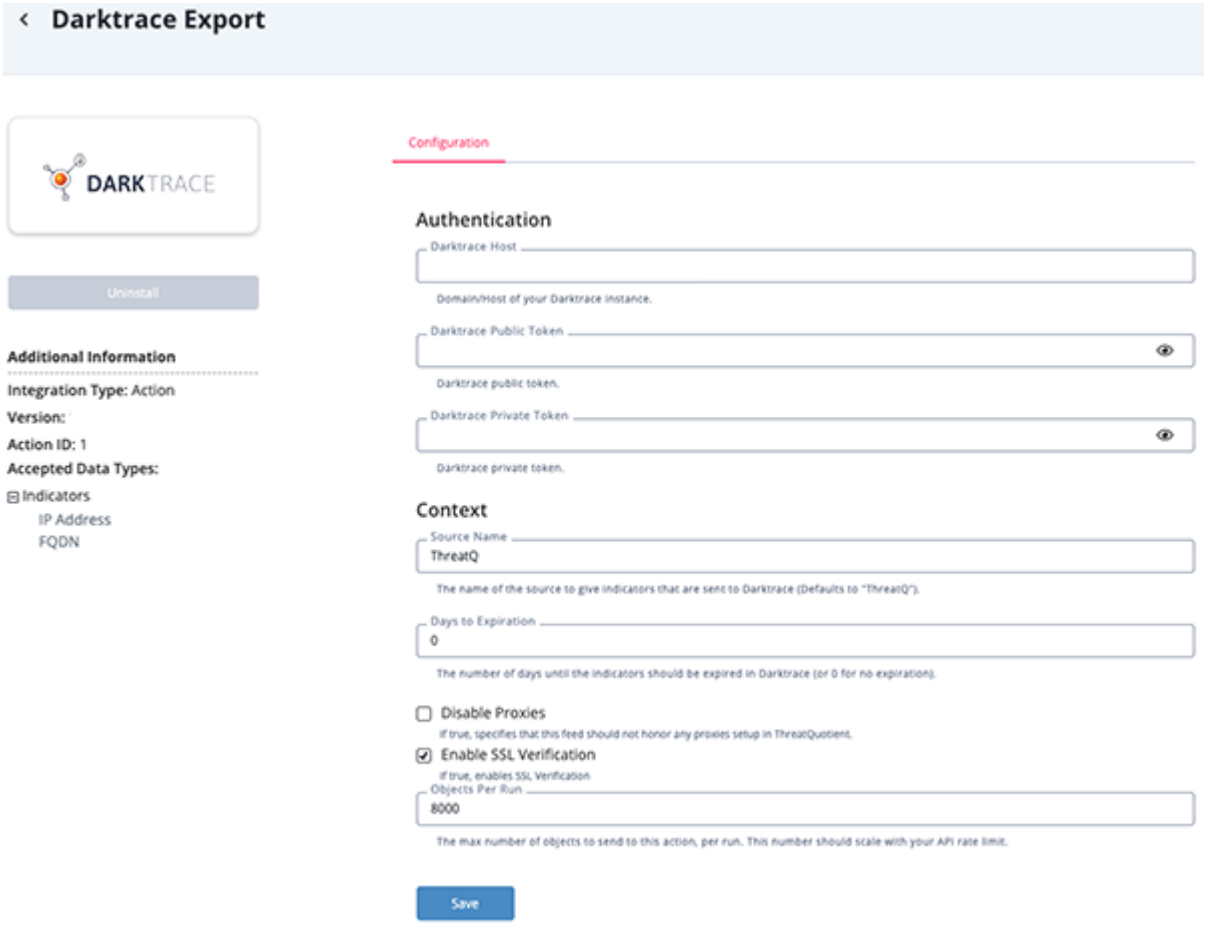
To configure the integration:

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
Darktrace Host	The Domain/Host of your Darktrace instance.
Darktrace Public Token	You Darktrace public token.
Darktrace Private Token	Your Darktrace private token.
Source Name	The name of the source to give indicators that are sent to Darktrace. The default value is `ThreatQ`.
Days to Expiration	The number of days until the indicators should be expired in Darktrace. Enter `0` for no expiration.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Enable SSL Verification	Enable this for the feed to validate the host-provided SSL certificate.

PARAMETER	DESCRIPTION
Objects Per Run	The max number of objects to send to this action, per run. This number should scale with your API rate limit.



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
Darktrace Export	Exports FQDN and IP Address IOCs to Darktrace, setting the expiration of the IOC based on user field input.	Indicators	FQDN, IP Address

Darktrace Export

The Darktrace Export action exports FQDN and IP Address IOCs to Darktrace, setting the expiration of the IOC based on user field input.

`POST https://{{host}}/intelfeed`

Sample Request:

```
{"addlist":"77.238.245.11,149.28.106.252,149.28.99.61,qxdyihiiid.duckdns.org,nffuasnath.duckdns.org","expiry":"2024-09-27T12:00:00","source":"ThreatQ"}
```

Sample Response:

```
{
  "response": "SUCCESS",
  "added": 5,
  "updated": 5,
  "addedList": [
    "nffuasnath.duckdns.org",
    "qxdyihiiid.duckdns.org",
    "149.28.99.61",
    "149.28.106.252",
    "77.238.245.11"
  ],
  "updatedList": [
    "nffuasnath.duckdns.org",
    "qxdyihiiid.duckdns.org",
    "149.28.99.61",
    "149.28.106.252",
    "77.238.245.11"
  ]
}
```

Change Log

- **Version 1.0.0**
  - Initial release