

ThreatQuotient



NetSkope Guide

Version 1.0.0

Friday, June 12, 2020

ThreatQuotient

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

Support

Email: support@threatq.com

Web: Support.threatq.com

Phone: 703.574.9893

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.

Copyright © 2020 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Contents

Warning and Disclaimer	2
Contents	3
Versioning.....	4
Introduction	5
Installation	6
Configuration	7
Known Limitations.....	11
Change Log	12

Versioning

- Integration Version: 1.0.0
- ThreatQ Version: 4.24.0 or greater

Introduction

The ThreatQ-Netskope plugin package allows users to sync MD5, SHA-256, and URL type indicators from ThreatQ into the Netskope CTE.

Installation

Users must install the ThreatQ-Netskope on the Netskope CTE server.

1. SSH into the system containing the Netskope CTE.
2. Enter the core docker container 'docker exec -it core /bin/sh'

```
docker exec -it core /bin/sh
```

3. Install the ThreatQ SDK and then re-install the proper version of requests

```
pip install -i
```

```
https://<user>:<password>@extensions.threatq.com/threatq/sdk
```

```
threatqsdk==1.8.0 && pip install requests==2.22.0
```

You can now terminate the SSH session.

4. Log into the Netskope CTE.
5. Navigate to the **Plugins** page.
6. Press the **Add new Plugin** button.
7. Select the tq_mw_netskope tar.gz package and click the upload button.
8. You should now see a ThreatQ plugin button, as well as a **Plugin Successfully Uploaded** toast.

Configuration

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

To configure the connector:

1. Click on the **ThreatQ** plugin button to pull up the prompt.
2. Enter the follow parameters under the **Basic information** tab for the plugin:

Note: Fields annotated with a * are required.


Parameter	Description
* Configuration Name	Plugin Configuration Name
Sharing Filters: Filter Query	Filter indicators while sharing with this plugin. Filter query can be generated from the Threat loc Page
Sharing Filters: Age of Indicators	Set this filter to limit the indicators while sharing whose age (Last Seen) is within the time specified
* Poll Interval	Interval to fetch data from source
* Aging Criteria	Expire indicators after specific time
Override Reputation	Set value to override reputation of indicators received from this configuration. Set 0 to keep default
Enable SSL Verification	Enable SSL Certificate verification
Use System Proxy	Use system proxy configured in settings

ThreatQ Configuration v0.0.1

×

Basic Information

Plugin Configuration



This is a threatq plugin

Configuration Name ⓘ

Score10

...

Sharing Filters

Filter Query ⓘ

test Is equal false

...

Age of Indicators ⓘ

In Days ⓘ

In Days

Poll Interval ⓘ

60

minutes ▾

Aging Criteria ⓘ

90

In Days

Override Reputation ⓘ

0

☐ Enable SSL verification ⓘ

☐ Use System Proxy ⓘ

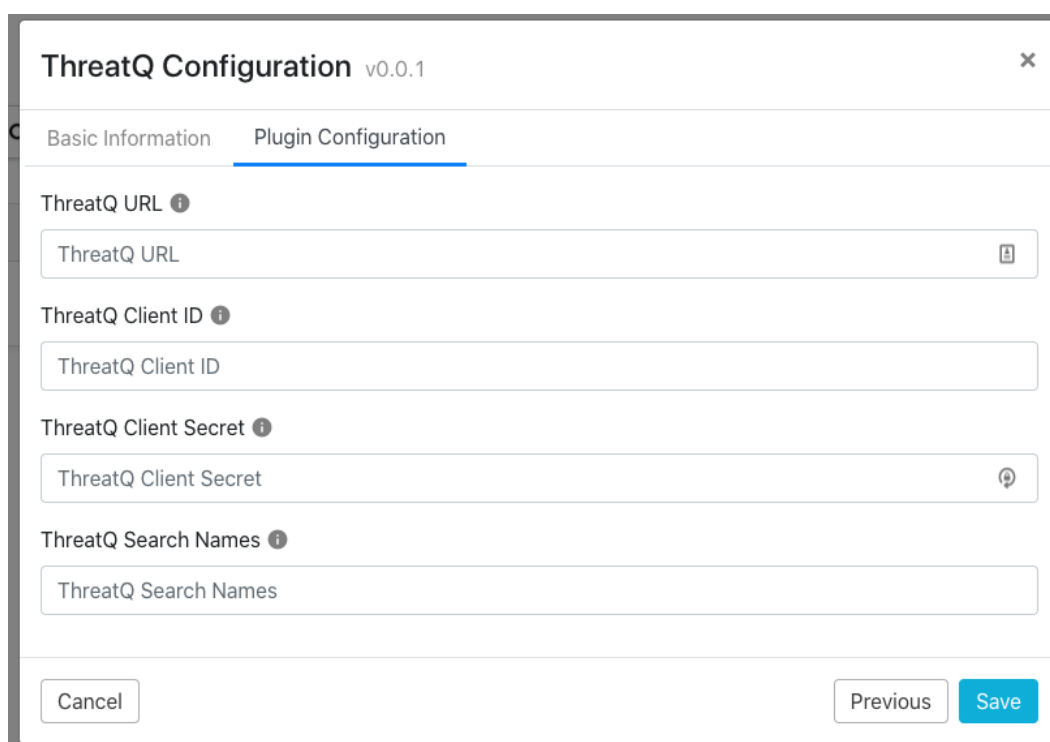
Cancel

Next

- Click **Next** to navigate to the **Plugin Configuration** tab.

- Enter the following configuration parameters under the **Plugin Configuration** tab:

Parameter	Description
* ThreatQ URL	The full URL including scheme to the ThreatQ instance.
* ThreatQ Client ID	Client ID generated by the threatq:oauth2-client cli command
* ThreatQ Client Secret	Client Secret generated by the threatq:oauth2-client cli command
* ThreatQ Search Names	ThreatQ Threat Library Search name. This can also be a comma delimited list of ThreatQ Threat Library search names.



ThreatQ Configuration v0.0.1

Basic Information **Plugin Configuration**

ThreatQ URL ⓘ

ThreatQ Client ID ⓘ

ThreatQ Client Secret ⓘ

ThreatQ Search Names ⓘ

Cancel Previous Save

- Click on **Save**.
- You should now see your ThreatQ Configuration in the Configured Plugins.

ThreatQ OAuth Client Credentials

In order to successfully have the app authenticate with ThreatQ, we first need to generate oauth2 client credentials. We can do this on the command line of the ThreatQ Appliance.

1. SSH into the console for the ThreatQ Appliance
2. Execute the Oauth2Client command (Note: You can change this name to match your needs)

```
sudo /var/www/api/artisan threatq:oauth2-client -name=Netskope
```

3. Copy the client_id and client_secret for use in the ThreatQ-Netskope Plugin

```
Sudo /var/www/api/artisan threatq:oauth2-client -name=Netskope

session_timeout_minutes: 1440

name: Netskope

type: private

client_id: ywewmmymmm4mde3y2uyzdc2ytk2mjdh

client_secret:

MjY1OWUyM2RlZTQwZjdiODUxN2MzNGM5ZDZhMTA0MjE1M2VkOTdlNjUxMTI0MGY0

created_at: 2020-05-13 16:47:20

updated_at: 2020-05-13 16:47:20
```

Known Limitations

- At the time of writing Netskope CTE only allowed for the use of MD5, SHA-256, and URL type indicators.

Change Log

Version	Details
1.0.0	Initial Release