ThreatQuotient

Netwitness Exports Guide

Version 1.0.0

April 05, 2023

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.

Export Details

ThreatQuotient provides the following details for this export:

Current Guide Version	1.0.0
Support Tier	ThreatQ Supported

Introduction

ThreatQuotient makes it easy for customers to export Netwitness indicators for use with an external threat detection system.

The following export data will be used:

- FQDN
- IP Address

Creating the Export

The following section will detail how to create exports for FDQN and IP Addresses.

> See the Managing Exports topic for more details on ThreatQ exports.

Exporting to Netwitness FQDN

1. Select the **Settings icon > Exports**.

   The Exports page appears with a table listing all exports in alphabetical order.

2. Click **Add New Export**

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:

FIELD	VALUE
Which type of information would you like to export?	Indicators
Output Type	text/csv; charset=utf-8
Special Parameters	indicator.status=Active&indicator.deleted=N& indicator.type=FQDN&indicator.class=network

FIELD	VALUE
Output Template	<> {foreach $data as $indicator} "{$indicator.value}","{foreach $indicator.Sources as $source} {$source.value}, {foreachelse}{/foreach}","https://{$http_host}/indicators/{$indicator.id}/details" {/foreach}

6. Click on **Save Settings** and enable the export via the On/Off toggle switch.

Exporting to Netwitness IP

1. Select the **Settings icon > Exports**.

   The Exports page appears with a table listing all exports in alphabetical order.

2. Click **Add New Export**

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:

FIELD	VALUE
Which type of information would you like to export?	Indicators
Output Type	text/csv; charset=utf-8

FIELD	VALUE
Special Parameters	indicator.status=Active&indicator.deleted=N&indicator.type=IP Address&indicator.class=network
Output Template	<> {foreach $data as $indicator} "{$indicator.value}","{foreach $indicator.Sources as $source} {$source.value},{foreachelse}{/foreach}","https://{$http_host}/indicators/{$indicator.id}/details" {/foreach}

6. Click on **Save Settings** and enable the export via the On/Off toggle switch.

Change Log

- **Version 1.0.0**
  - Initial release