

ThreatQuotient



Cisco TID 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

Export Details..... 5

Introduction 6

Creating the Export..... 7

Cisco FMC Configuration 14

Change Log..... 16

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 © 2023 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.

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

This guide will provide you with the steps to create exports to enable IOCs to be exported to Cisco TID via the Cisco FMC to be published to Cisco FTD Devices.

The constraints of the Cisco Threat Intelligence Director will only allow the following ThreatQ exports to be used:

- SHA-256
- Domain (FQDN)
- URL
- IPv4
- IPv6
- Email
 - To
 - From
 - Sender
 - Subject

Creating the Export

The following section will detail how to create the exports in ThreatQ.



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

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:



See the Output Format Options topic for more information on using logical operators in exports. If a specific score or ranges of scores is required, then the following should be added to the end of the special parameters configuration.

In the example below, this will ensure only IP Address IoCs that are equal to 7 or above are exported.

Example

```
: indicator.status=Active&indicator.deleted=N&indicator.type=IPAddress&indicator.class=network&indicator.score>=7
```

SHA-256

FIELD	VALUE
Export Name	Cisco TID – SHA-256
Which type of information would you like to export?	Indicator
Output Type	Text/plain
Special Parameters	indicator.status=Active&indicator.deleted=N&indicator.type=SHA-256
Output Format Template	{foreach \$data as \$indicator} {\$indicator.value} {/foreach}

FQDN

FIELD	VALUE
Export Name	Cisco TID – FQDN
Which type of information would you like to export?	Indicator
Output Type	Text/plain
Special Parameters	indicator.status=Active&indicator.deleted=N&indicator.type=FQDN &indicator.class=network&indicator.score>=11
Output Format Template	{foreach \$data as \$indicator} {\$indicator.value} {/foreach}

URL

FIELD	VALUE
Export Name	Cisco TID – URL
Which type of information would you like to export?	Indicator
Output Type	Text/plain
Special Parameters	indicator.status=Active&indicator.type=URL&indicator.class=network
Output Format Template	{foreach \$data as \$indicator} {\$indicator.value} {/foreach}

IPv4 Address

FIELD	VALUE
Export Name	Cisco TID – IPv4
Which type of information would you like to export?	Indicator
Output Type	Text/plain
Special Parameters	indicator.status=Active&indicator.deleted=N&indicator.type=IPAddress&indicator.class=network
Output Format Template	{foreach \$data as \$indicator} { \$indicator.value} {/foreach}

IPv6 Address

FIELD	VALUE
Export Name	Cisco TID – IPv6
Which type of information would you like to export?	Indicator
Output Type	Text/plain
Special Parameters	Indicator.Status=Active&Indicator.Type=IPv6 Address
Output Format Template	{foreach \$data as \$indicator} { \$indicator.value} {/foreach}

Email Address

FIELD	VALUE
Export Name	Cisco TID – Email Address
Which type of information would you like to export?	Indicator
Output Type	Text/plain
Special Parameters	indicator.status=Active&indicator.type=Email Address&indicator.class=network
Output Format Template	{foreach \$data as \$indicator} {\$indicator.value} {/foreach}

- Click on each of the URL's for the exports. A new browser widow will open displaying the first 10 results, make a note of this URL and the IoCs it is associated with it. The URL is made up off the following sections

```
<> https://<TQ Server>/api/export/<endpoint>/?  
limit=10&token=<token>
```

- Remove the limit section and trailing & symbol, examples are below.

```
<> https://192.168.1.85/api/export/  
9bc092ce1e318f6c0d10009228729ad6/?  
token=uEyVyzIeYRGBdF2VKcHo9WKYDJvNftSo
```


This new URL format is needed to configure Cisco TID

```
<> https://192.168.1.85/api/export/  
9bc092ce1e318f6c0d10009228729ad6/?  
token=uEyVyzIeYRGBdF2VKcHo9WKYDJvNftSo
```

- Click **Save Settings**.
- Under **On/Off**, toggle the switch to enable the export.

Cisco FMC Configuration

1. Navigate to the Intelligence director on the Firepower Management Center.
2. Choose **Intelligence > Sources**.
3. Click the **add icon (+)**.
4. Choose **URL** as the Delivery method for the source.
5. Complete the Add Source form.

FIELD	ENTRY
Type	Flat File
Content	Select a Content type that describes the data contained within the source.
URL	Use the URL format outlined in step 8 of the <i>To export to Cisco TID</i> steps.
Self-Signed Certificate	Toggle the Self-Signed Certificate to active.
Name	<p>Use a descriptive name as we used on the ThreatQ exports.</p> <p>Example: ThreatQ - IP Address</p> <div> This will help simplify sorting and handling of incidents based on TID indicators, use a consistent naming scheme across sources.</div>
Action	You can either Block or Monitor.
Update Every	Select a time in minutes that the source is to be updated (the minimum is 30 mins, Maximum is 14,400).

FIELD

ENTRY

TTL

Specify the number of days for the TTL interval.

- TID deletes all the source's indicators that are not included in subsequent upload.
- All observables not referenced by a surviving indicator.

6. Confirm that the **Publish** toggle is set to **Active** if you want to immediately begin publishing to elements.



If you do not publish the source at ingestion, you cannot publish all source indicators at once later. Instead, you must publish each observable individually.

7. Click **Save**.

Change Log

- Version 1.0.0
 - Initial release