ThreatQuotient

Fidelis Elevate 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
Compatible with ThreatQ Versions	>= 4.40.0
Support Tier	ThreatQ Supported
Fidelis Elevate CommandPost Version	9.3.3

Introduction

ThreatQ exports to send indicators of compromise (Email Address, IP Address, MD5, URL and FQDN) to Fidelis Elevate. Elevate has the capability to ingest IOCs from external threat feeds and use them to create rules and policies, and define the reaction by the sensors if such a policy is violated. The exports defined here are in an XML format, although Elevate offers also the option to ingest feed in CSV format.

More details about custom threat feeds and their configuration in Elevate can be found on the help pages of a Fidelis Elevate device:

https://<Fidelis Elevate Host or IP>/help/MyWebHelp/Content/FidelisCreatePoliciesHelpVersion/P_InsightCustomFeed.htm

Exporting Steps per Type

The following section provides the steps required to created exports for specific indicator types.

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

Exporting an Email Address

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
Type of information you would like to export?	Indicators
Output type	text/plain
Special Parameters	`indicator.status=Active&indicator.deleted=N&indicator.type=EmailAddress&indicator.class=network&differential=1`

6. Under **Output Format Template**, enter:

```
<ThreatQEmailAddressFeed>
  <description>Email addresses feed from ThreatQ</description>
  <entries>
  {foreach $data as $indicator}
  <entry>
      <email>{$indicator.value}</email>
      <extra_info>{$indicator.id}</extra_info>
    </entry>
  {if !$indicator.last}{/if}
  {/foreach}
</entries>
</ThreatQEmailAddressFeed>
```

7. Click **Save Setting**s.
8. Under **On/Off**, toggle the switch to enable the export.
9. Click on the export URL with the data.

> Make sure to remove the limit parameter from the URL: `limit=10&`.
> The URL should be similar to this one:
> `https://<ThreatQ Host>/api/export/<export ID>/?token=<Authentication Token>`

Exporting IP Addresses

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
Type of information you would like to export?	Indicators
Output type	text/plain
Special Parameters	`indicator.status=Active&indicator.deleted=N&indicator.type=IP Address&indicator.class=network&differential=1`

6. Under **Output Format Template**, enter:

```
<ThreatQIPAddressFeed>
  <description>IP address feed from ThreatQ</description>
  <entries>
  {foreach $data as $indicator}
  <entry>
      <ip>{$indicator.value}</ip>
      <extra_info>{$indicator.id}</extra_info>
    </entry>
  {if !$indicator.last}{/if}
  {/foreach}
</entries>
</ThreatQIPAddressFeed>
```

7. Click **Save Settings**.
8. Under **On/Off**, toggle the switch to enable the export
9. Click on the export URL with the data.

> Make sure to remove the limit parameter from the URL: `limit=10&`.
> The URL should be similar to this one:
> `https://<ThreatQ Host>/api/export/<export ID>/?token=<Authentication Token>`

Exporting MD5 Hashes

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
Type of information you would like to export?	Indicators
Output type	text/plain
Special Parameters	`indicator.status=Active&indicator.deleted=N&indicator.type=MD5&indicator.class=network&differential=1`

6. Under **Output Format Template**, enter:

```
<ThreatQMD5Feed>
  <description>MD5 feed from ThreatQ</description>
  <entries>
  {foreach $data as $indicator}
  <entry>
      <md5>{$indicator.value}</md5>
      <extra_info>{$indicator.id}</extra_info>
    </entry>
  {if !$indicator.last}{/if}
  {/foreach}
</entries>
```

```
</ThreatQMD5Feed>
```

7. Click **Save Settings**.
8. Under **On/Off**, toggle the switch to enable the export.
9. Click on the export URL with the data. Make sure to delete from the URL this parameter `limit=10&`. The URL should be similar to this one `https://<ThreatQ Host>/api/export/<export ID>/?token=<Authentication Token>`

Exporting FQDNs and URLs

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
Type of information you would like to export?	Indicators
Output type	text/plain
Special Parameters	`indicator.status=Active&indicator.deleted=N&indicator.type=URL&indicator.type=FQDN&indicator.class=network&differential=1`

6. Under **Output Format Template**, enter:

```
<ThreatQFQDNURLFeed>
  <description>Threat feed from ThreatQ with FQDNs and URLs</description>
  <entries>
  {foreach $data as $indicator}
  <entry>
      <url>{$indicator.value}</url>
      <extra_info>{$indicator.id}</extra_info>
    </entry>
  {if !$indicator.last}{/if}
  {/foreach}
</entries>
</ThreatQFQDNURLFeed>
```

7. Click **Save Settings**.

8. Under **On/Off**, toggle the switch to enable the export.
9. Click on the export URL with the data.

> Make sure to remove the limit parameter from the URL: `limit=10&`.
> The URL should be similar to this one:
> `https://<ThreatQ Host>/api/export/<export ID>/?token=<Authentication Token>`

Adding Exports as Custom Threat Feeds in Fidelis Elevate

For a detailed description of the configuration steps, visit the following page on your Fidelis Elevate CommandPost appliance:

https://<Fidelis Elevate Host>/help/MyWebHelp/Content/FidelisCreatePoliciesHelpVersion/P_InsightAddCustomFeed.htm.

To add a new feed:

1. Go to **Policies -> Threat Feeds -> Feed Config** and click on **Add Feed**.
2. Enter the name of the feed.

   > The entered name must be unique among all custom feeds on CommandPost.

3. Optional - Add a description that will be displayed in the list of feeds on the Feed Config page.
4. Select **XML** as the feed format.
5. Enter **entry** for the XML format descriptor.
6. Click the **Add** button.
7. Enter a **Description** of the feed on the detailed configuration page.
8. Select the feed content for the indicator type that is being ingested.
9. Make sure the following boxes are checked, at a minimum:
   - Enable
   - Dynamic
   - Verify SSL Certificate
10. Select the **Refresh Frequency** that is needed for the environment.
11. Enter the **ThreatQ export URL** in the *Location (URL)* box.
12. Click the *Save* button to save the configuration. To test the feed click on the *Download Now* button

> Custom feeds can be set up for a one-time manual upload, manual refresh, or automated refresh.

Change Log

- **Version 1.0.0**
  - Initial release