ThreatQuotient

Fortinet FortiSIEM IOC Exports User Guide

Version 1.0.0

January 22, 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

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 Fortinet version	7.x
Support Tier	ThreatQ Supported

Introduction

This guides describes the steps required to export IoCs from ThreatQ and import them into Fortinet ForiSIEM.

Prerequisites

The following is required to perform the steps outline in this guide:

- ThreatQ Account with an Administrator role in order to create the export.
- Fortinet Account with an Administrator role to create the import.

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 the following in **Export Name** field: `FortiSIEM Malware Domains`.
4. Click **Next Step**.
   The Output Format dialog box appears.
5. Provide the following information:

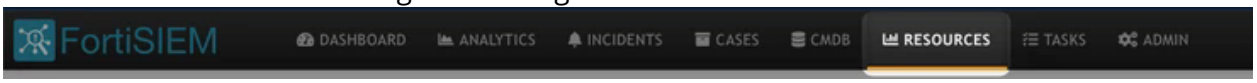
FIELD	VALUE
Type of information you would like to export?	Indicators
Output type	text/plain
Special Parameters	Enter your special parameters to filter the objects. **Example:** `indicator.deleted=N&indicator.type=FQDN&indicator.score=>=4` > See the Output Format Options and Filtering Special Parameters topic for further details on special parameters.

Output Template	`{foreach $data as $indicator}`
	`{$indicator.value}`
	`{/foreach}`

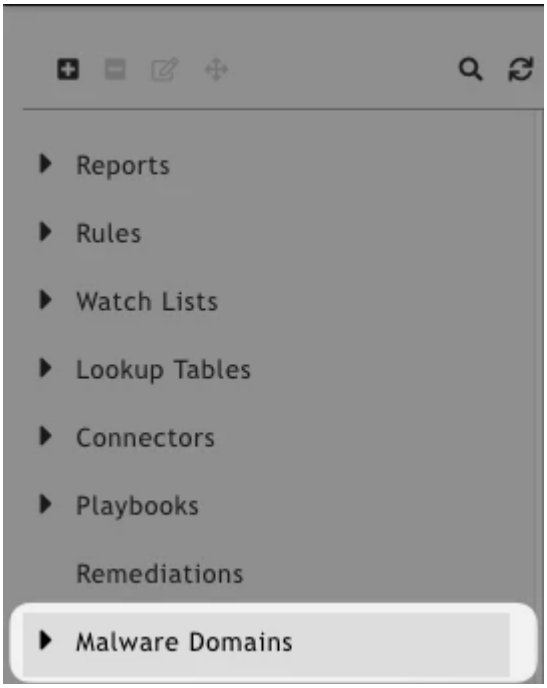
6. Click on **Save Settings** and enable the export via the On/Off toggle switch.

Creating the Import in FortiSIEM

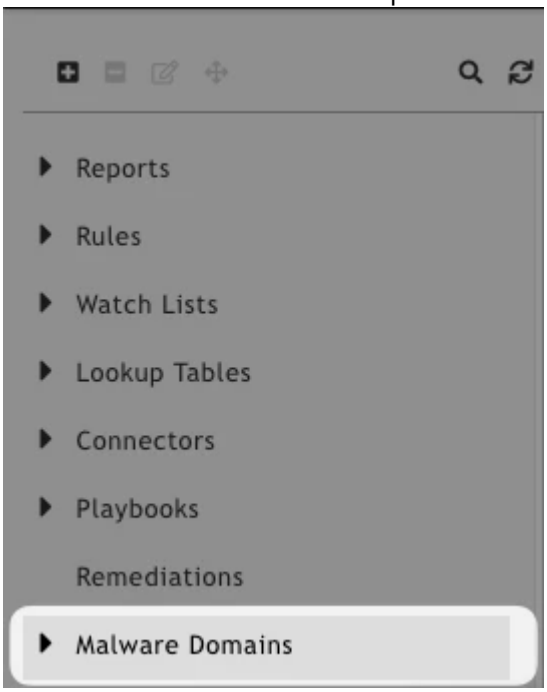
1. Log into FortiSIEM.
2. Click on the **Resources** heading in the navigation bar.



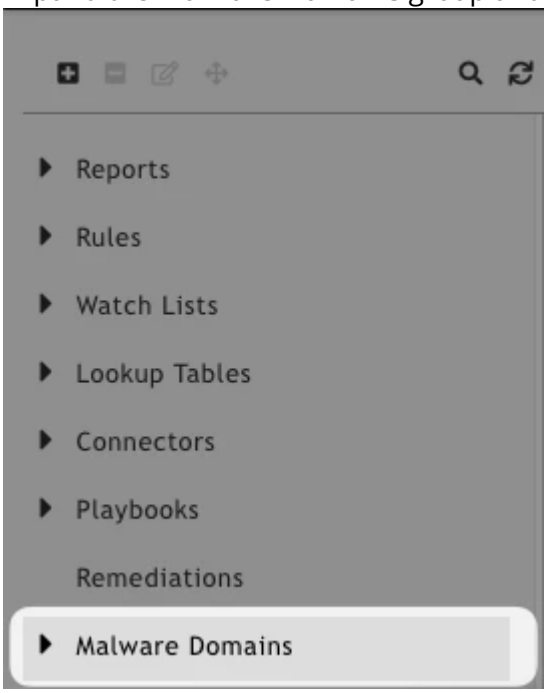
3. Click on the **Malware Domains** section located on the sidebar.



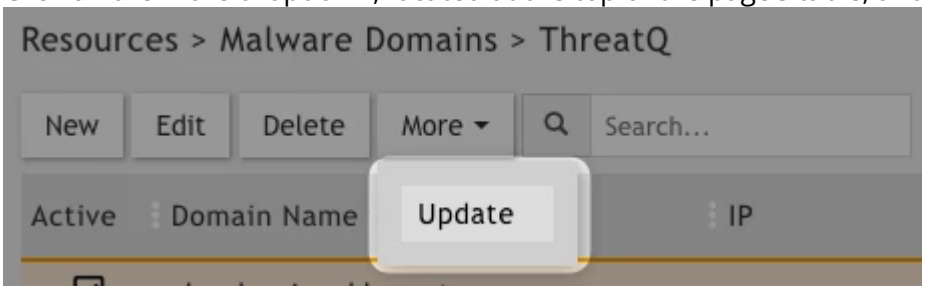
4. Click on the + button at the top of the sidebar.



5. Enter a **Group Name** and an optional **Description**.
6. Save the group.
7. Expand the **Malware Domains** group and select your new group.



8. Click on the More dropdown, located at the top of the page's table, and select **Update**.

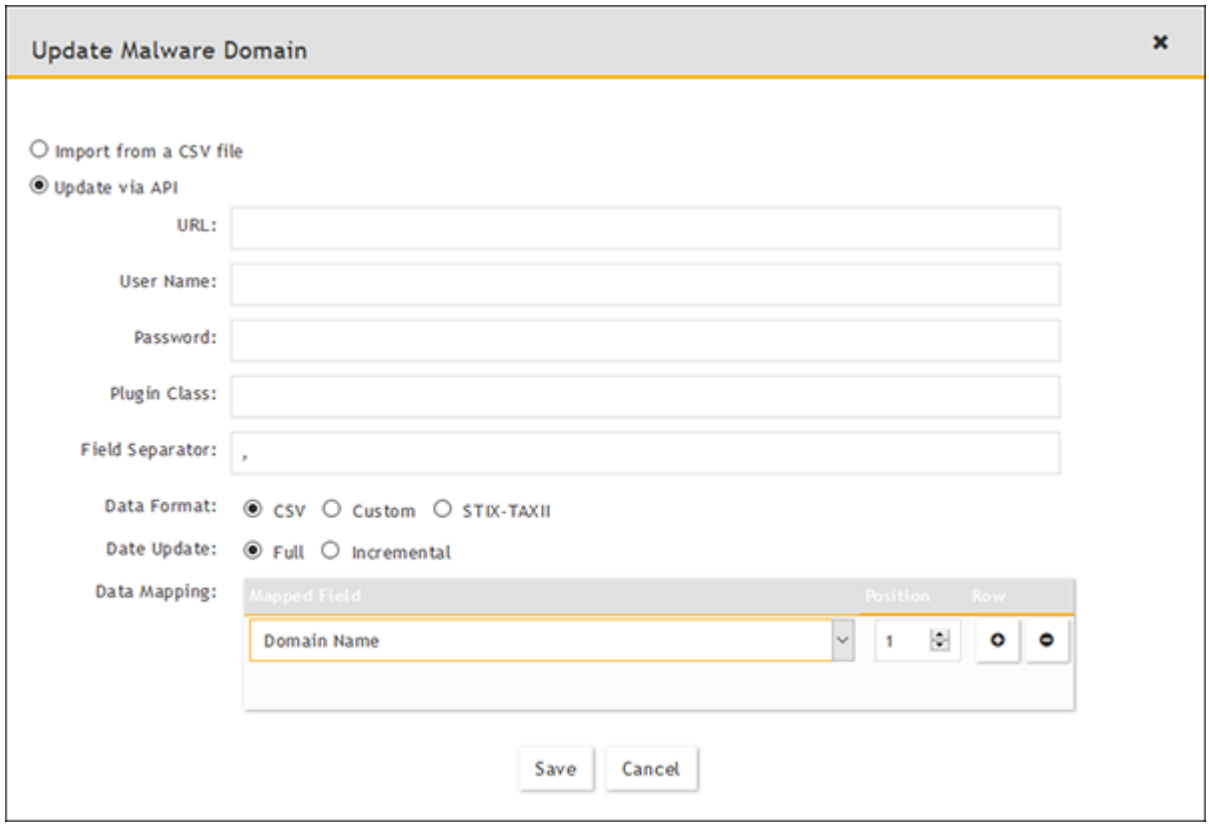


9. Select the **Update via API radio** button.
10. Click on the **Edit** button to expand the dialog box.
11. Complete the following fields:

> Anything not specified below can be left at the default.

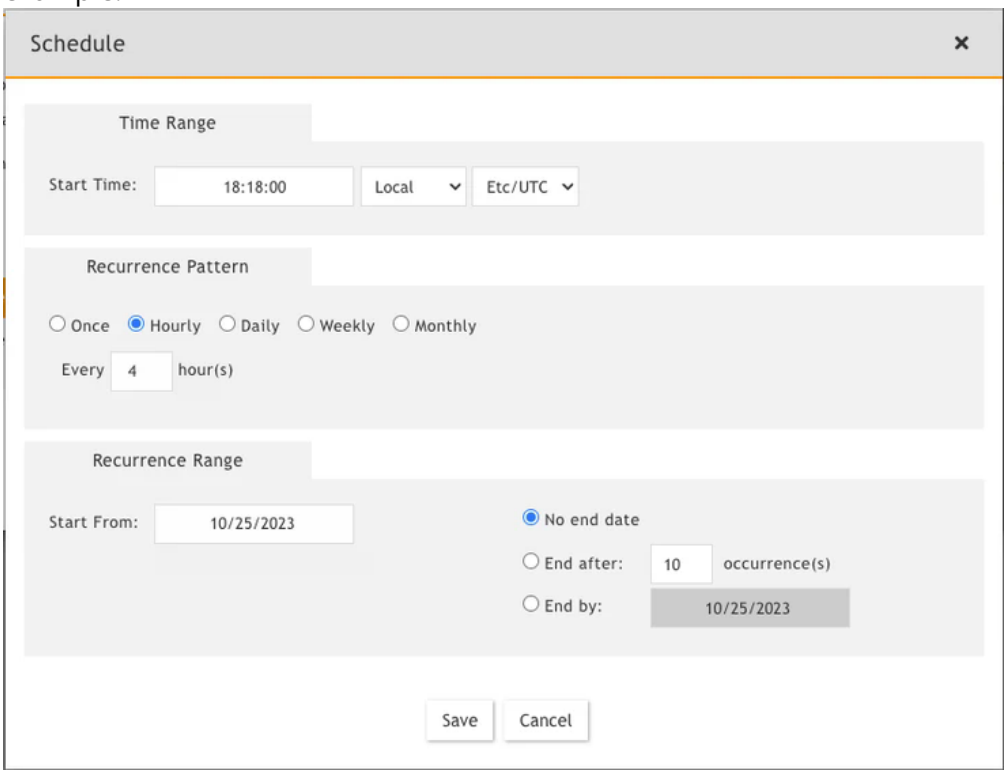
FIELD	DESCRIPTION
URL	Paste your ThreatQ export url into the field. Make sure to remove the limit parameter when you have finished testing.

FIELD	DESCRIPTION
Data Format	CSV
Data Update	Full
Data Mapping	Select **Domain Name** from the dropdown and set the **Position** to **1**.



12. Click **Save**.
13. Click on the + icon next the Schedule text, to open the new schedule form.

14. Create your new recurring or one-time schedule. It should look similar to the following example:



15. Click **Save** and then close the dialog box.
16. The ThreatQ export will now be pulled into FortiSIEM on the specified schedule.

Change Log

- **Version 1.0.0**
  - Initial release