ThreatQuotient

Fortinet Fortigate 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
FortiOS	>= 6.0

Introduction

ThreatQuotient makes it easy for customers to export IOCs to their Fortinet FortiGate Firewall. The implementation is done using the Threat Feed Connectors feature available in FortiOS v6.0 and above. An export with IOCs is first created on ThreatQ and the export URL is installed FortiGate appliance.

> This integration only works on FortiOS v6.0 and above.

Prerequisites

Before starting the integration, users are encouraged to familiarize themselves with the following documents:

- Fortinet Fortigate cookbook on blocking malicious domains using threat feeds - https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/85580
- Using Threat Feed Connectors in FortiOS v6.0 and above - https://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortigate-security-profiles/Web_Filter/Overriding%20FortiGuard%20website%20categorization.htm#External

Creating the Export

The export is a dynamic list of IOCs which should be configured on ThreatQ and provided to a FortiGate instance to read from.

> 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:

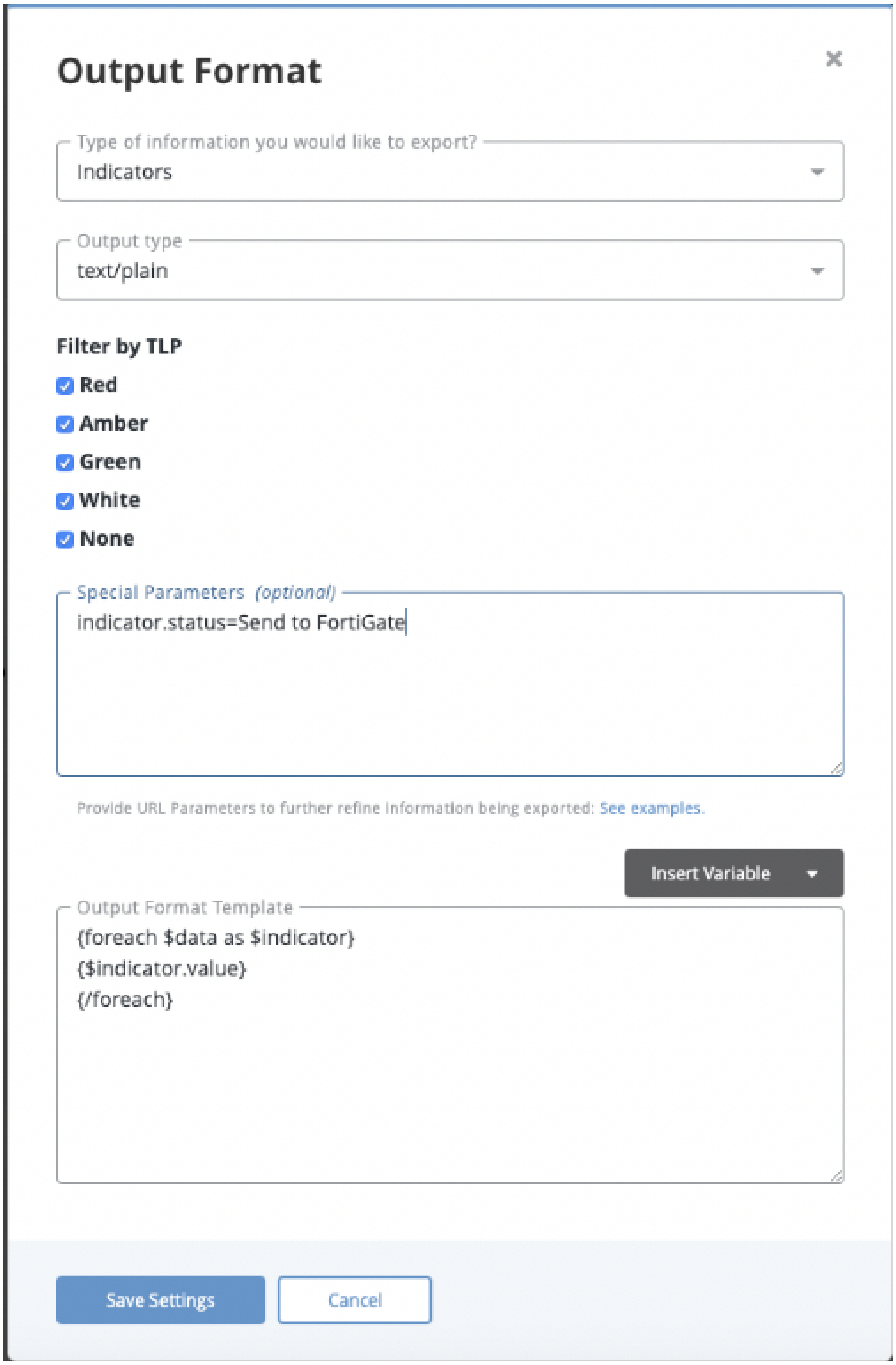
FIELD	VALUE
Type of information you would like to export	Indicators
Output Type	text/plain
Special Parameters	There are two options for special parameters: **If the security policy of your organization requires that all IP Addresses and FQDNs are sent to FortiGate, use these filters for the special parameters:**

FIELD	VALUE

	`indicator.status=Active&indicator.deleted=N&indicator.type=IP Address& indicator.type=FQDN`
	To send only the IOCs that have a custom status, e.g. Send to FortiGate, use the special parameters below.
	To create the custom status:
	1. Click on the **Settings** gear icon and select **Object Management**.
	2. Click on **Add New Status** button located to the top-right of the page.
	3. Enter **Send to FortiGate** as the status name, add an optional description, and click on **Add Status**.
	4. Use the following special parameter for your export:
	`indicator.status=Send to FortiGate`

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

Once configured, the export will look similar to the snapshot below.



Output Format

Type of information you would like to export?
Indicators

Output type
text/plain

Filter by TLP

- ☑ Red
- ☑ Amber
- ☑ Green
- ☑ White
- ☑ None

Special Parameters *(optional)*
indicator.status=Send to FortiGate

Provide URL Parameters to further refine information being exported: See examples.

Output Format Template

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

Configuring FortiGate

The following section will provide you with steps and related resources to configure ForitGate to work with the export.

Configure FortiGate to Download Indicators from ThreatQ

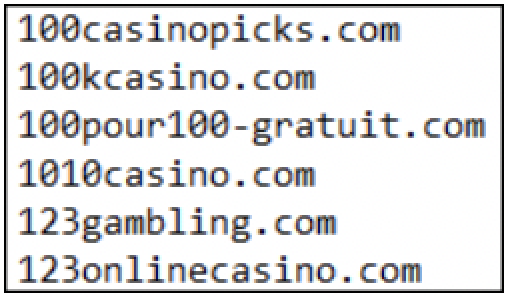
The following detailed steps have been copied from the FortiGate support center and provided here for convenience. The source is https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/85580

Blocking Malicious Domains using Threat Feeds

This example uses a domain name threat feed and FortiGate DNS filtering to block malicious domains. The text file in this example is a list of gambling site domain names.

Threat feeds allow you to dynamically import external block lists in the form of a text file into your FortiGate. These text files, stored on an HTTP server, can contain a list of web addresses or domains. You can use threat feeds to deny access to a source or destination IP address in Web Filter and DNS Filter profiles, SSL inspection exemptions, and as a source/destination in proxy policies. You can use Fabric connectors for FortiGate that do not belong to a Fortinet Security Fabric.

1. Create an external block list. The external block list should be a plain text file with one domain name per line. The use of simple wildcards is supported. You can create your own text file or download it from an external service. Upload the text file to the HTTP file server.

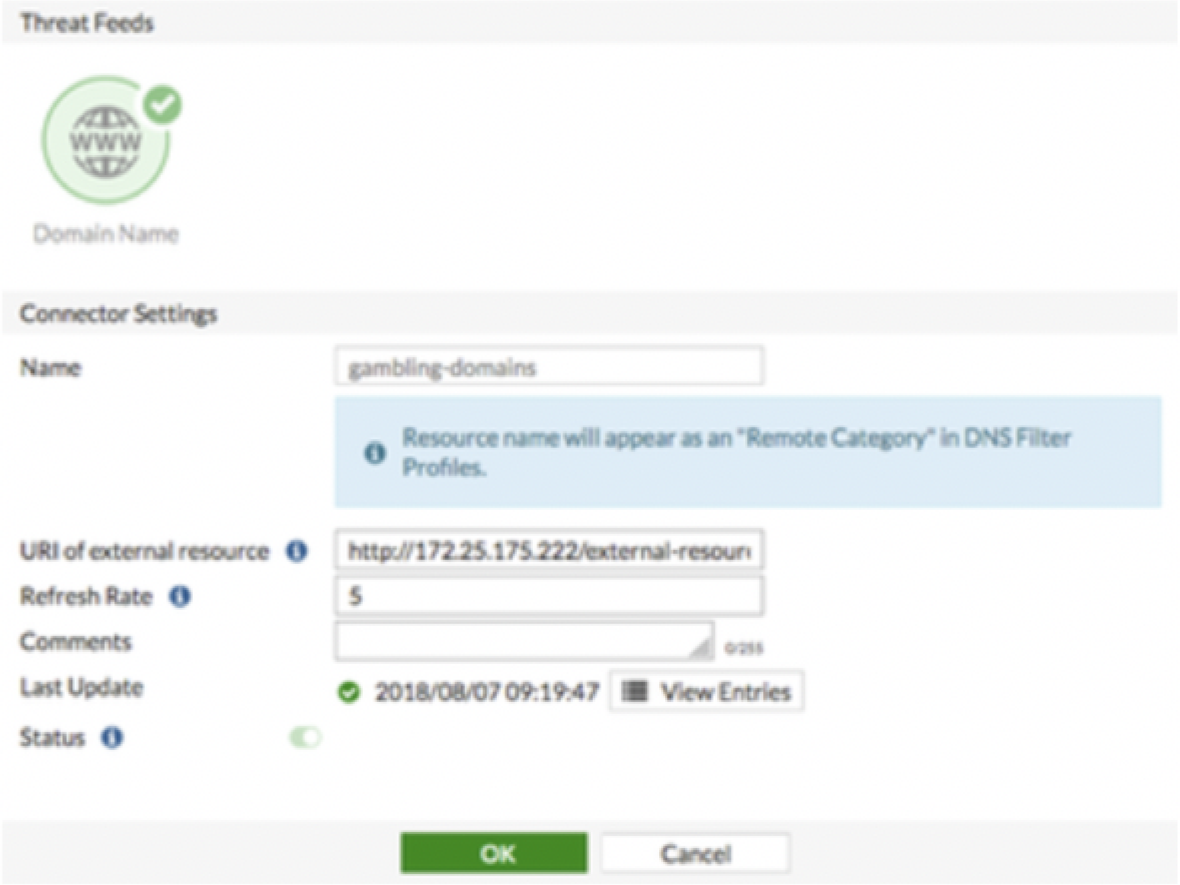


```
100casinopicks.com
100kcasino.com
100pour100-gratuit.com
1010casino.com
123gambling.com
123onlinecasino.com
```

2. Configure the threat feed:
    a. In FortiOS, go to Security Fabric -> Fabric Connectors. Click Create New.

b. Under Threat Feeds, select Domain Name.

c. Configure the Name, URI of external resource, and Refresh Rate fields. In the URI of external resource field, enter the location of the text file on the HTTP file server. By default, the FortiGate rereads the file and uploads any changes every five minutes.



Threat Feeds

Domain Name

Connector Settings

Name: gambling-domains

Resource name will appear as an "Remote Category" in DNS Filter Profiles.

URI of external resource: http://172.25.175.222/external-resour

Refresh Rate: 5

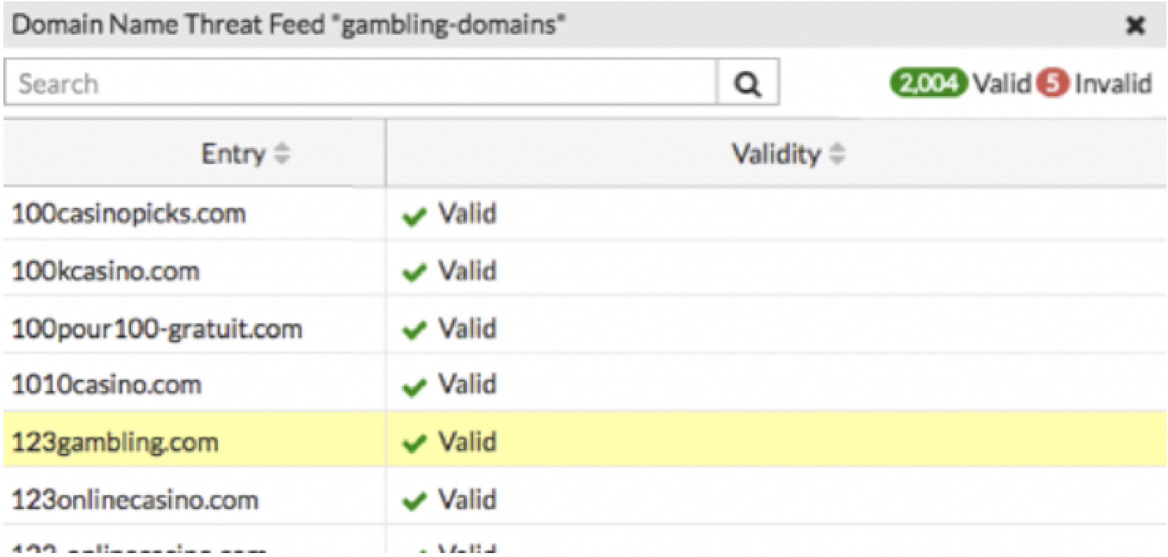
Comments: 0/255

Last Update: 2018/08/07 09:19:47 View Entries

Status

OK Cancel

d. Click View Entries to see the text file's domain list.



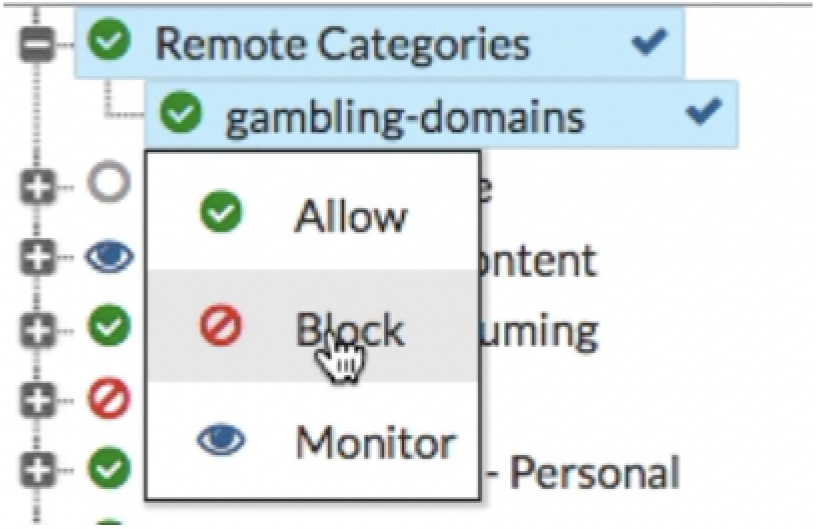
Domain Name Threat Feed "gambling-domains" ✖

Search 2,004 Valid 5 Invalid

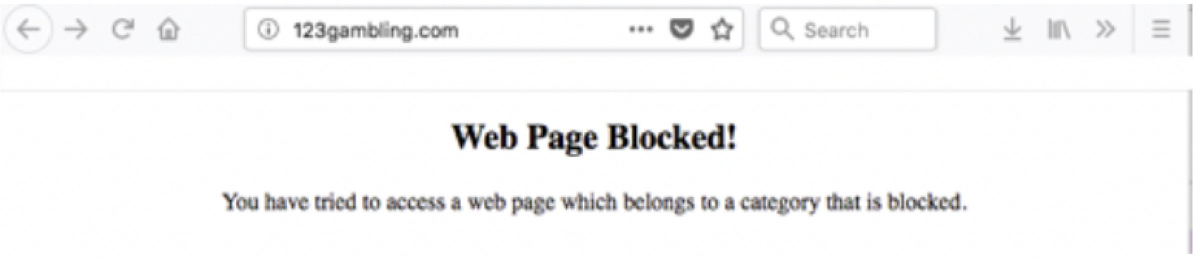
Entry	Validity
100casinopicks.com	✓ Valid
100kcasino.com	✓ Valid
100pour100-gratuit.com	✓ Valid
1010casino.com	✓ Valid
123gambling.com	✓ Valid
123onlinecasino.com	✓ Valid

e. Click **OK**.

3. Add the threat feed to the DNS filter:
    a. Go to Security Profiles -> DNS Filter.
    b. Scroll to the list of preconfigured FortiGuard filters.
    c. The resource file uploaded earlier is listed under Remote Categories. Set the action for this category to Block.



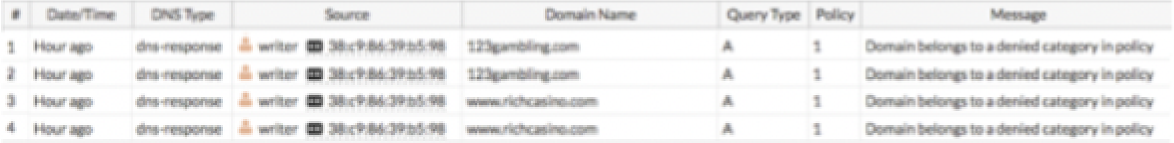
4. Configure the outgoing Internet policy:
    a. Go to **Policy & Objects -> IPv4 Policy**.
    b. Enable the **DNS Filter** under the *Security Profiles*.
    c. From the SSL Inspection dropdown list, select an SSL inspection profile.
5. View the results:
    a. Visit a domain on the external resource file. This example visits 123gambling.com. A Web Page Blocked! message appears.



Web Page Blocked!

You have tried to access a web page which belongs to a category that is blocked.

    b. In FortiOS, go to **Log & Report -> DNS Query**. The logs show that the 123gambling.com domain belongs to a blocked category.



#	Date/Time	DNS Type	Source	Domain Name	Query Type	Policy	Message
1	Hour ago	dns-response	writer 38:c9:86:39:b5:98	123gambling.com	A	1	Domain belongs to a denied category in policy
2	Hour ago	dns-response	writer 38:c9:86:39:b5:98	123gambling.com	A	1	Domain belongs to a denied category in policy
3	Hour ago	dns-response	writer 38:c9:86:39:b5:98	www.richcasino.com	A	1	Domain belongs to a denied category in policy
4	Hour ago	dns-response	writer 38:c9:86:39:b5:98	www.richcasino.com	A	1	Domain belongs to a denied category in policy

Change Log

- **Version 1.0.0**
  - Initial release