ThreatQuotient

Broadcom ProxySG 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

This guides describes the implementation between ThreatQ and the Broadcom ProxySG appliance. The implementation is done using the Local Database Content Filtering functionality available in the ProxySG. An export with IOCs is first created on ThreatQ and the export URL is installed on the proxy.

> This guide replaces the export steps for Symantec ProxySG. Symantec is now known as Broadcom.

Prerequisites

You should confirm that there is route between ThreatQ and Broadcom ProxySG.

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

- Broadcom ProxySG CLI: https://techdocs.broadcom.com/content/dam/broadcom/techdocs/symantec-security-software/web-and-network-security/proxysg/6-7/generated-pdfs/CLI67.pdf
- Local Content Filtering Database: https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/proxysg/7-3/getting-started/page-help-administration/page-help-data-services/page-help-providers/page-help-local.html

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:

FIELD	VALUE
Type of information you would like to export?	Indicators
Output type	plain text
Special Parameters	`indicator.status=Active&indicator.deleted=N&indicator.type=URL&indicator.type=FQDN&indicator.type=IP Address&indicator.type=CIDR Block`

Output Template	<> `define category threatq_iocs`
	`{foreach $data as $indicator}`
	`{assign var=parts value="/"| explode:$indicator.value}`
	`{assign var=hostname value=":"| explode:$parts[2]}`
	`{assign var=fqdn value=":"| explode:$parts[0]}`
	`{if $fqdn[0] eq "http" or $fqdn[0] eq "https"}`
	`{assign var=domain value=$hostname[0]}`
	`{else}{assign var=domain value=$fqdn[0]}{/if}`
	`{$domain}`
	`{/foreach}`
	`end`
	
	This will strip the port and URL path from the IOCs.

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

Configure ProxySG to Download Indicators from ThreatQ

There are two methods to install the dynamic list in the ProxySG -

- via the Management Console
- via the Proxy's CLI

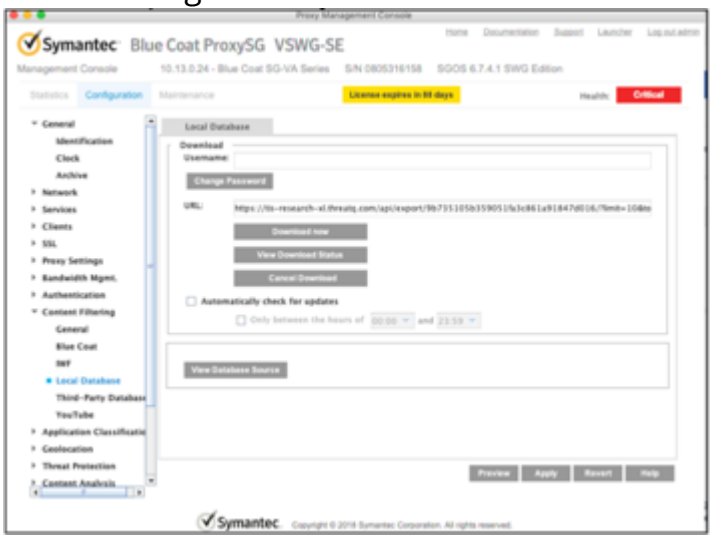
The management console UI can accept only a single block list. Starting with ProxySG v6.7.4, you can configure the proxy to read from up to seven dynamic lists. The following two sections go over the methods for installing dynamic block lists.

Via the Management Console

1. Open the ProxySG management console.

2. Navigate to **Configuration > Content Filtering Local Database**.

   The following screen will load.



3. Insert the **export URL** from TQ in the **URL** space and click on the **Download now** button.

   This will initiate a pull of the indicators from the ThreatQ into the proxy. To check on the status of the download, click on **View Download Status**. Any download related messages will be shown in the download status window.

Via the ProxySG CLI

In addition to the Management Console UI, the proxy has a CLI which provides more configuration options. In the reference section at the end of this document, you can find a PDF document with the CLI commands. To help with testing of the integration below is a sequence of commands that allows a user to install the exports from ThreatQ in a local content database on the proxy.

1. Log into the Blue Coat CLI:

   ```
   <> ssh <username>@<BlueCoat Hostname/IP>
   ```

   Use the password set in the initial configuration.

2. Enable the admin mode:

   ```
   <> enable
   ```

   You will be prompted for a password which is usually the account password.

3. Enter the following command access the config model of the appliance.

   ```
   <> config
   ```

4. Select **TERMINAL** at the prompt.
5. Start working with the content filtering database:

   ```
   <> content-filter
   ```

6. Enter the Local Content Filtering DB mode.

   ```
   <> local
   ```

7. Create a new database name if needed.

   ```
   <> create tq_test
   ```

8. Enter db edit mode to download the URL.

   ```
   <> edit tq_test
   ```

9. Bind the URL of the ThreatQ export to the content database on the ProxySG.

> ⚠ Put double quotes around the URL.

```
<> download url "https://<TQ>/api/export/<hash>/?
   limit=1000&token=<token>"
```

10. Download the database now.

```
<> download get-now
```

11. View the status of the current, and older, download

```
<> view
```

12. Show the contents of the downloaded local database file.

```
<> source
```

13. If you want to configure auto downloads there are various options available. To list all the download options use the following command

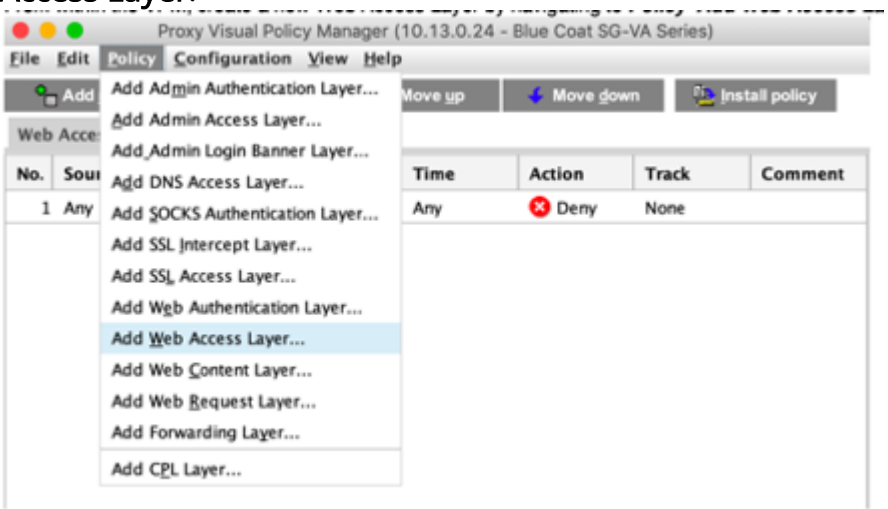
```
<> download ?
```

Create and Install a Content Filtering Policy

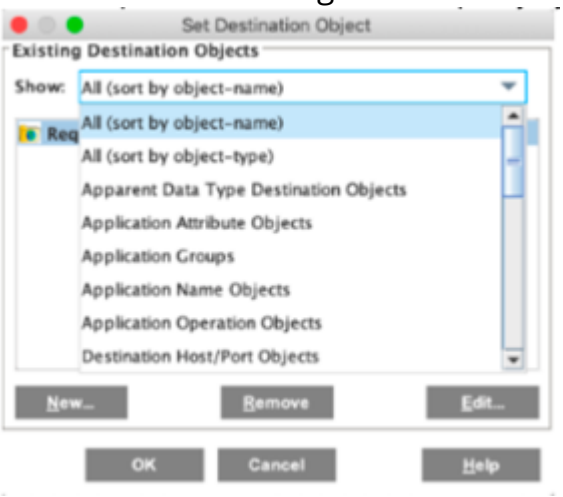
The final step is to install a content filtering policy using the indicators from the ThreatQ export which are being downloaded to a content filtering database on the proxy.

1. Open ProxySG (the example here uses the virtual proxy appliance).
2. Navigate to **Configuration Policy > Visual Policy Manager** and click on **Launch Java VPM**.

3. From within the VPM, create a new **Web Access Layer** by navigating to **Policy Add > Web Access Layer**.



4. Assign a name for the new layer, and after it's created right click on the **Destination object** and select **Set**.
5. Under the drop down in the modal window select **All (sort by object name)** and then click on **Edit** in the lower right corner.



This will open a new window, in which you can select all the categories to be blocked by the ProxySG appliance. The list of URLs exported from ThreatQ will be available under the Local category.

6. Expand **Local** and select the name you've given the export from ThreatQ. In this example, the name is **tq_malicious_url**.

7. Click **OK**, and then again **OK** to go back to the **VPM**.
8. Highlight the newly created policy layer, and click on the **Install policy** button in the upper right corner.

> Before installing the policy, make sure that the type of **Action** on the policy is **Deny**. If it shows **Allow**, make sure to change it to **Deny**. The action instruction what type action ProxySG should enforce when it detects that a user sends a request to any of the indicators in the list exported from ThreatQ.

9. The new policy is now installed and any active indicators exported from ThreatQ will be blocked by the ProxySG.

Change Log

- **Version 1.0.0**
  - Initial release