ThreatQuotient

Palo Alto Firewall Exports Guide

Version 1.0.0

April 06, 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

ThreatQuotient makes it easy for customers to export IOCs to their Palo Alto Firewall.

The implementation is done using Palo Alto’s External Dynamic List (EDL) functionality. An export with IOCs is first created on ThreatQ and the export URL is provided to Palo Alto as an EDL.

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

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

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

Palo Alto: PANOS and Panorama Exports

This section describes the implementation between ThreatQ and Palo Alto firewall. The implementation is done using Palo Alto's External Dynamic List (EDL) functionality. An export with IOCs is first created on ThreatQ and the export URL is provided to Palo Alto as an EDL. The following details go over the steps to create, and add the EDL to ThreatQ.

Prerequisites

Before you begin the integration between Palo Alto and ThreatQ, confirm that there is a route between both hosts.

Create an export in ThreatQ

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

The following link lists the guidelines for the format of the export list in ThreatQ.

There are separate guidelines for IP, FQDN and URL lists.

These guidelines are both for PANOS and Panorama:

https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/9-0/pan-os-admin/pan-os-admin.pdf

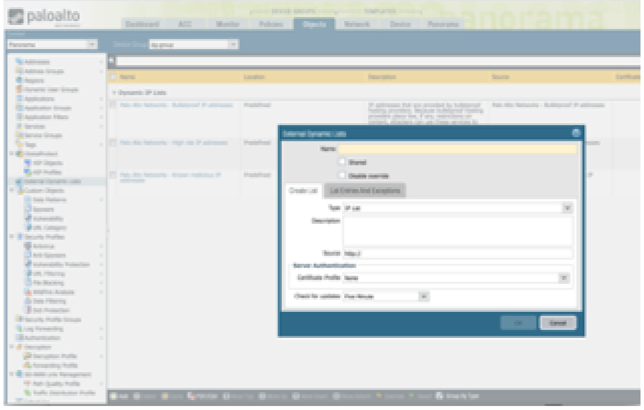
Configure an External Dynamic List (EDL) in PANOS

To add the dynamic list to Palo Alto, follow the instructions on page 1419 of the following guide:

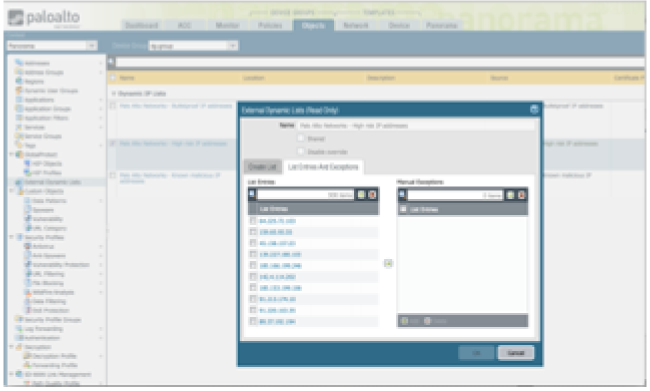
https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/9-0/pan-os-admin/pan-os-admin.pdf

Configure an External Dynamic List (EDL) in Panorama

1. Navigate to **Device Groups > Objects**, and then click on the **External Dynamic List** in the left pane, about half way down.
2. Add a new dynamic list by clicking on the **Add** button at the bottom of the screen.



3. Provide a **Name**, **Type**, and for source provide the **ThreatQ exports URL**.


paloalto
External Dynamic Lists (Read Only)
Name
Palo Alto Networks - High risk IP addresses
Shared
Disable override
Create List
List Entries And Exceptions
List Entries
Manual Exceptions
OK
Cancel

4. Click **OK**.

Retrieve an External Dynamic List from the Source

Once the list has been configured you can retrieve the indicators from that list.

Follow the steps on page 1434 in the following PDF: https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/9-0/pan-os-admin/pan-os-admin.pdf

Enforce Policy on an External Dynamic List

To create a policy to enforce rules for the indicators from the EDL, follow the steps on page 1436 in the following PDF: https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/9-0/pan-os-admin/pan-os-admin.pdf

Change Log

- **Version 1.0.0**
  - Initial release