



ThreatQuotient for Palo Alto Wildfire Operation

August 17, 2018

Version 1.1.0

**11400 Commerce Park Dr
Suite 200,
Reston, VA
20191, USA
<https://www.threatq.com/>
Support: support@threatq.com
Sales: sales@threatq.com**

Contents

CONTENTS	2
LIST OF FIGURES AND TABLES	3
ABOUT THIS THREATQUOTIENT FOR PALO ALTO WILDFIRE OPERATION	4
DOCUMENT CONVENTIONS	4
INTRODUCTION	5
1.1 APPLICATION FUNCTION	5
1.2 PREFACE	5
1.3 AUDIENCE	5
1.4 SCOPE	5
1.5 ASSUMPTIONS	5
IMPLEMENTATION OVERVIEW.....	6
1.6 PREREQUISITES	6
1.7 SECURITY AND PRIVACY	6
THREATQUOTIENT FOR PALO ALTO WILDFIRE OPERATION INSTALLATION.....	7
1.8 SETTING UP THE INTEGRATION	7
1.9 CONFIGURING THE OPERATION	9
1.10 PALO ALTO NETWORKS WILDFIRE SUPPORTED FILE TYPES.....	10
TRADEMARKS AND DISCLAIMERS	11

List of Figures and Tables

FIGURE 1: TIME ZONE CHANGE EXAMPLE	6
FIGURE 2: OPERATIONS MANAGEMENT – INSTALL	7
FIGURE 3: INSTALL OPERATION	7
FIGURE 4: ADD OPERATION	8
FIGURE 5: ADD OPERATION	8
FIGURE 6: OPERATIONS MANAGEMENT – CONFIGURATION	9
FIGURE 7: OPERATION CONFIGURATION.....	9
FIGURE 12: WILDFIRE FILE SUBMISSION EXAMPLE OUTPUT.....	10
TABLE 3: THREATQUOTIENT SOFTWARE & APP VERSION INFORMATION	5
TABLE 4: PALO ALTO NETWORKS WILDFIRE SUPPORTED FILE TYPES.....	10

About This ThreatQuotient for Palo Alto Wildfire Operation

Author

ThreatQuotient Professional Services

Document Conventions



Alerts readers to take note. Notes contain suggestions or references to material not covered in the document.



Alerts readers to be careful. In this situation, you may do something that could result in equipment damage or loss of data.



Alerts the reader that they could save time by performing the action described in the paragraph.



Alerts the reader that the information could help them solve a problem. The information might not be troubleshooting or even an action.

Introduction

1.1 Application Function

The ThreatQuotient for Palo Alto Wildfire Operation provides the ability to submit a file to Palo Alto WildFire for analysis, via the Palo Alto WildFire API.

1.2 Preface

This guide provides the information necessary to implement the ThreatQuotient for Palo Alto Wildfire Operation. This document is not specifically intended as a site reference guide. It is assumed that the implementation engineer has experience installing and commissioning ThreatQuotient Apps and integrations covered within the document, as well as experience necessary to troubleshoot at a basic level.

1.3 Audience

This document is intended for use by the following parties:

1. ThreatQ and Security Engineers.
2. ThreatQuotient Professional Services Project Team & Engineers.

1.4 Scope

This document covers the implementation of the application only.

Table 1: ThreatQuotient Software & App Version Information

Software/App Name	File Name	Version
ThreatQ	Version 3.6.x or greater	
ThreatQuotient for Palo Alto Wildfire Operation	1.1.0	

1.5 Assumptions

The following criteria is assumed to be in place and functional to allow the implementation of the ThreatQuotient for Palo Alto Wildfire Operation into the managed estate:

- All ThreatQuotient equipment is online and in service.
- Infrastructure/transmission at all sites and between sites is in place to support the network traffic.
- All required firewall ports have been opened.
- All equipment is powered from permanent power supplies.
- A clock source of sufficient accuracy is connected to the network and the network and devices are using it as the primary clock source.

Implementation Overview

This document provides direction for installing and configuring the ThreatQuotient for Palo Alto Wildfire Operation found within the ThreatQ instance.

1.6 Prerequisites



You must have a valid Palo Alto Wildfire API Key.

Throughout this implementation document, we will refer to several files and directories, some of which will be symbolic, and others may change depending on specifics of the environmental setup.

Ensure that all ThreatQ devices are set to the correct time, time zone and date, and using a clock source available to all.

For Example:

Figure 1: Time Zone Change Example

```
sudo ln -sf /usr/share/zoneinfo/America/Los_Angeles /etc/localtime
```

1.7 Security and Privacy

For ThreatQuotient Professional Services engineers to configure the system, local network access is required to connect to the managed estate. Therefore, the implementation must occur at an office or data center location.

Passwords have not been provided in this document. Please contact your project team for this information, if required.

All engineers are reminded that all data belonging and pertaining to the business is strictly confidential and should not be disclosed to any unauthorized parties.

The data held within this document is classed as confidential due to its nature.

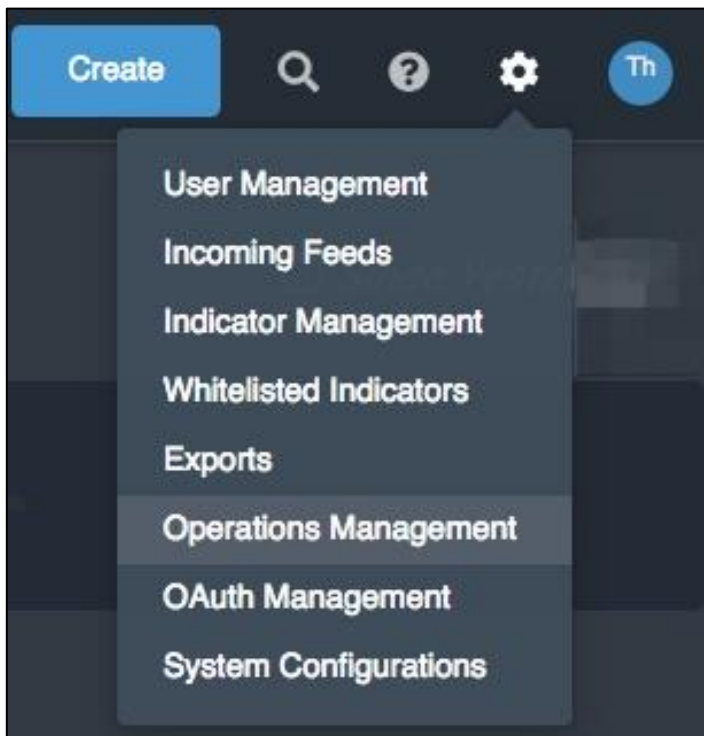
ThreatQuotient for Palo Alto Wildfire Operation Installation

1.8 Setting up the Integration

Ensure that the file `tq_op_palo_alto_networks_wildfire-1.1.0-py3-none-any.whl` is available on the device being used to administer the ThreatQ instance where the ThreatQuotient for Palo Alto Wildfire Operation is being installed or upgraded.

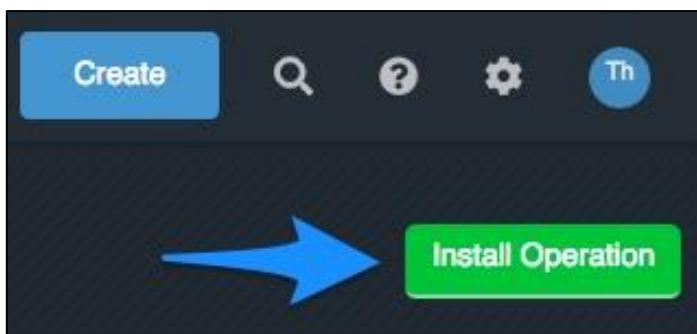
1. Navigate to **Settings > Operations Management**.

Figure 2: Operations Management – Install



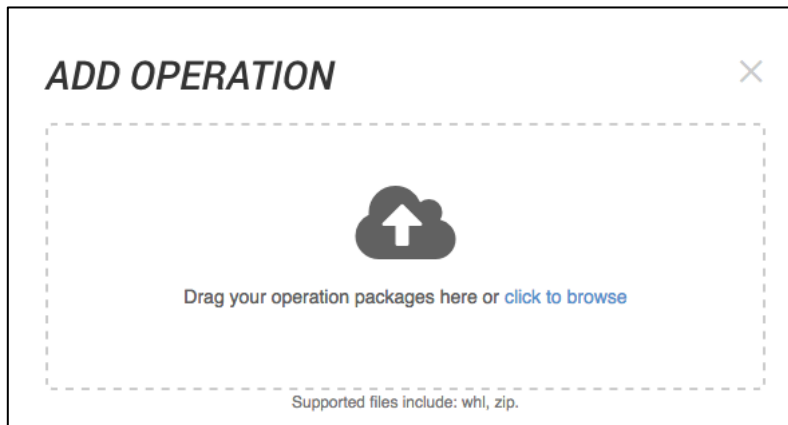
2. Click **Install Operation** in the upper right corner.

Figure 3: Install Operation



3. Drag the `tq_op_palo_alto_networks_wildfire-1.1.0-py3-none-any.whl` to the Add Operation Popup or click to browse to the required file.

Figure 4: Add Operation

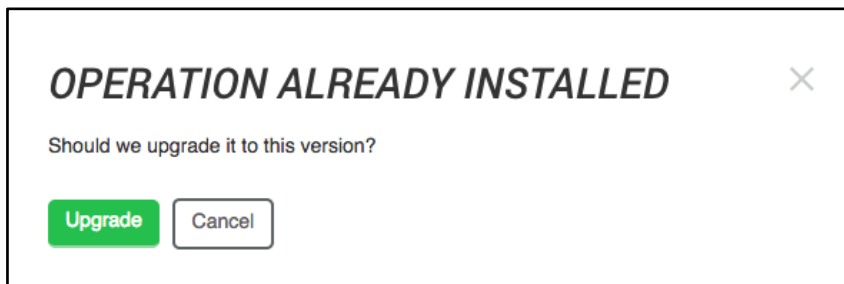


4. Click on the install/upgrade button.



You may be presented with **OPERATION ALREADY INSTALLED** as shown below.

Figure 5: Add Operation



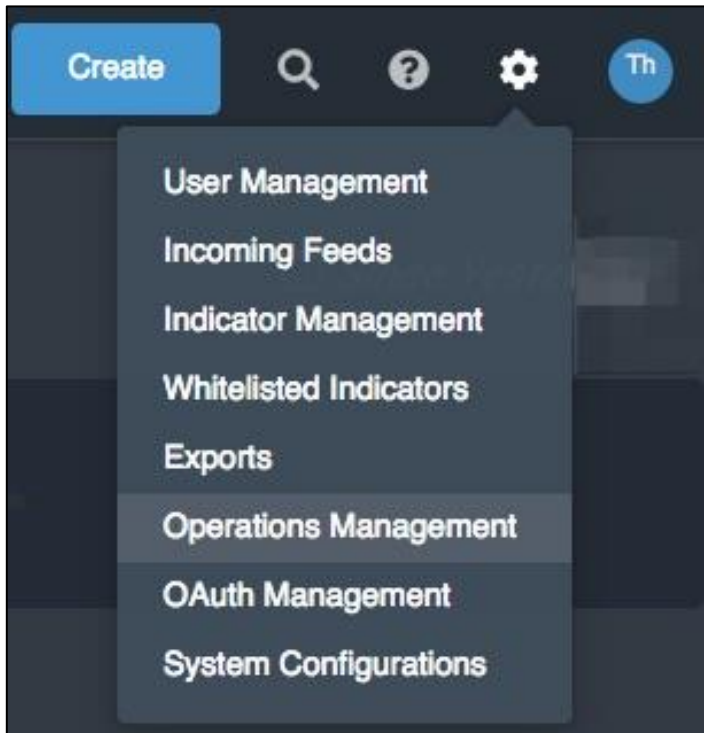
Installation/Upgrade is now complete.

1.9 Configuring the Operation

The following section covers the configuration of the ThreatQuotient for Palo Alto Wildfire Operation.

1. Navigate to **Settings > Operations Management**.

Figure 6: Operations Management – Configuration



2. Expand the **Palo Alto WildFire** Operation Settings.

Figure 7: Operation Configuration

A screenshot of the 'Palo Alto Networks WildFire' operation configuration page in ThreatQuotient. The page has a header with a toggle switch for 'Palo Alto Networks WildFire', a 'Submit/Query WildFire' button, and a link to 'Operation Settings'. The main content area includes a logo for ThreatQ, the author 'ThreatQ', version '1.1.0', required ThreatQ version '2.1', and a link 'Works with: Attachment'. There is a checkbox for 'Bypass system proxy configuration for this operation'. Below this is a text input field for 'Wildfire On Premise URL (Cloud URL used if not provided)'. Another text input field is for 'Wildfire API Key', with a password mask and a visibility toggle. At the bottom left is a green 'Save Changes' button, and at the bottom right is a red 'Delete Operation' button.

3. Enter the **Wildfire On Premise URL (Cloud URL used if not provided)**.
4. Enter the **Wildfire API Key** from Palo Alto.
5. Click **Save Changes**.
6. Click the toggle in next to **Palo Alto Networks WildFire** to enable the operation.


1.10 Palo Alto Networks WildFire Supported File Types

Table 2: Palo Alto Networks WildFire Supported File Types

File Types Supported	WildFire Global Cloud	WildFire Private Cloud (WildFire Appliance)
Links contained in emails	Yes	Yes
Android application package (APK) files	Yes	No
Java Archive (JAR) files	Yes	Yes
Microsoft Office files	Yes	Yes
Portable executable (PE) files	Yes	Yes
Portable document format (PDF) files	Yes	Yes
Mac OS X files	Yes	No
Linux (ELF) files	Yes	No
Archive (RAR and 7-Zip) files	Yes	No

WildFire Submit Example

Figure 8: WildFire File Submission Example Output


Palo Alto Networks WildFire:
Submit File

WildFire

Success!

Indicators

<input type="checkbox"/>	Value	Type
<input type="checkbox"/>	Search	Search
<input type="checkbox"/>	056e4a359fb7b620cedd832af1d5e2a1	MD5
<input type="checkbox"/>	00b32c3428362e39e4df2a0c3e0950947c147781fdd3d2f0b5f96989bb002	SHA-256

[Add Indicators](#)

Raw Response

```
<?xml version="1.0" encoding="UTF-8"?>
<wildfire>
  <upload-file-info>
    <url></url>
    <filetype>adobe PDF document</filetype>
    <filename>rombles.pdf</filename>
    <sha256>00b32c3428362e39e4df2a0c3e0950947c147781fdd3d2f0b5f96989bb002</sha256>
    <md5>056e4a359fb7b620cedd832af1d5e2a1</md5>
    <size>309500</size>
  </upload-file-info>
</wildfire>
```

[Hide](#)

Trademarks and Disclaimers

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR THREATQUOTIENT REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THIRD PARTY SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. THREATQUOTIENT AND THIRD-PARTY SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL THREATQUOTIENT OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF THREATQUOTIENT OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

ThreatQuotient and the ThreatQuotient Logo are trademarks of ThreatQuotient, Inc. and/or its affiliates in the U.S. and other countries.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

©2018 ThreatQuotient, Inc. All rights reserved.