

# ThreatQuotient



## ThreatQuotient for Palo Alto Wildfire Operation

Version 1.2.0

March 22, 2019

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [support.threatq.com](http://support.threatq.com)

Phone: + 1 703.574.9893

## 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.

Copyright © 2019 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Last Updated: Wednesday, March 22, 2019

# Contents

---

<b>WARNING AND DISCLAIMER.....</b>	<b>2</b>
<b>CONTENTS .....</b>	<b>4</b>
<b>LIST OF FIGURES AND TABLES .....</b>	<b>5</b>
<b>ABOUT THIS THREATQUOTIENT FOR PALO ALTO WILDFIRE OPERATION .....</b>	<b>6</b>
DOCUMENT CONVENTIONS .....	6
<b>INTRODUCTION .....</b>	<b>7</b>
1.1 APPLICATION FUNCTION .....	7
1.2 PREFACE .....	7
1.3 AUDIENCE .....	7
1.4 SCOPE .....	7
<b>THREATQUOTIENT FOR PALO ALTO WILDFIRE OPERATION INSTALLATION.....</b>	<b>8</b>
1.5 SETTING UP THE INTEGRATION .....	8
1.6 CONFIGURING THE OPERATION .....	10
1.7 PALO ALTO NETWORKS WILDFIRE SUPPORTED FILE TYPES .....	10
<b>TRADEMARKS AND DISCLAIMERS .....</b>	<b>13</b>

# List of Figures and Tables

---

FIGURE 1: OPERATIONS MANAGEMENT – INSTALL .....	8
FIGURE 2: INSTALL OPERATION .....	8
FIGURE 4: ADD OPERATION .....	9
FIGURE 5: ADD OPERATION .....	9
FIGURE 5: OPERATIONS MANAGEMENT – CONFIGURATION .....	10
FIGURE 7: OPERATION CONFIGURATION.....	10
FIGURE 8: WILDFIRE FILE SUBMISSION EXAMPLE OUTPUT.....	11
FIGURE 8: WILDFIRE REPORT EXAMPLE OUTPUT .....	12
FIGURE 8: WILDFIRE VERDICT EXAMPLE OUTPUT .....	12
TABLE 1: THREATQUOTIENT SOFTWARE & APP VERSION INFORMATION .....	7
TABLE 2: 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 allows a ThreatQ user to execute three (3) actions on Palo Alto Networks Wildfire. It gives users the ability to submit files to Wildfire, as well as retrieve the report back from Wildfire based on its hash. It also provides the user with a way to query Wildfire to get a verdict on a hash (MD5/SHA-256). Possible verdicts include: Malware, Phishing, Grayware, or Benign.

## 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 the 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	1.2.0	

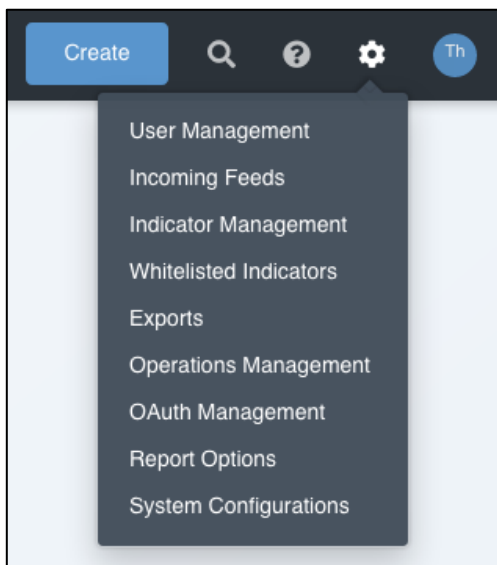
# ThreatQuotient for Palo Alto Wildfire Operation Installation

## 1.5 Setting up the Integration

Ensure the file `tq_op_palo_alto_networks_wildfire-1.2.0-py3-none-any.whl` is available on the device being used to administer the ThreatQ instance in which the ThreatQuotient for Palo Alto Wildfire Operation is being installed or upgraded.

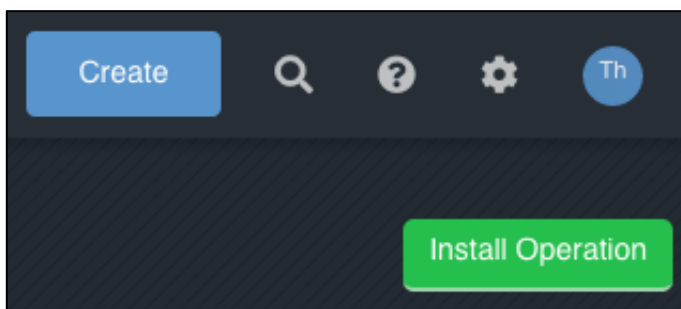
1. Navigate to the **Settings icon > Operations Management**.

*Figure 1: Operations Management – Install*



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

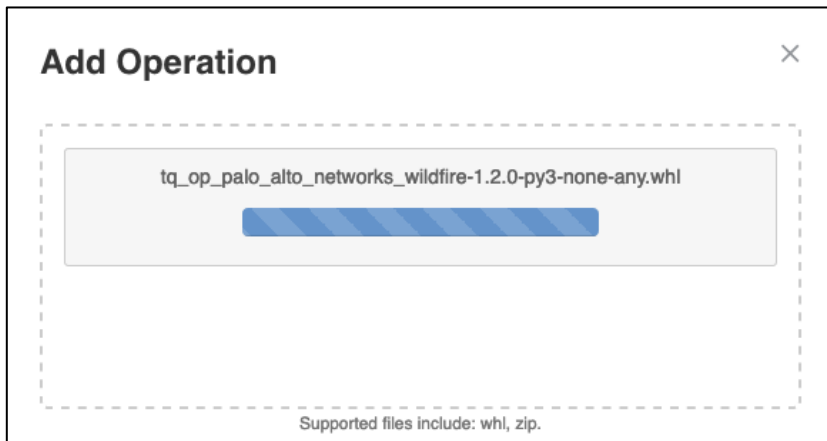
*Figure 2: Install Operation*



3. Drag the `tq_op_palo_alto_networks_wildfire-1.2.0-py3-none-any.whl` to the Add Operation Popup or click to Browse and browse to the required file.



Figure 3: Add Operation

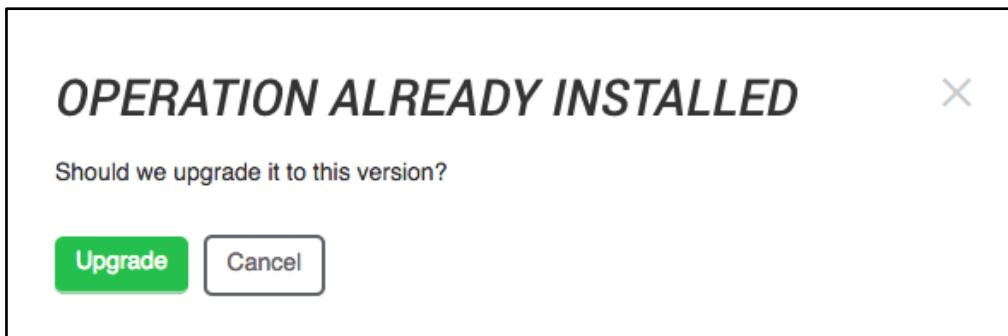


4. Click **Install** or **Upgrade**.



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

Figure 4: Add Operation



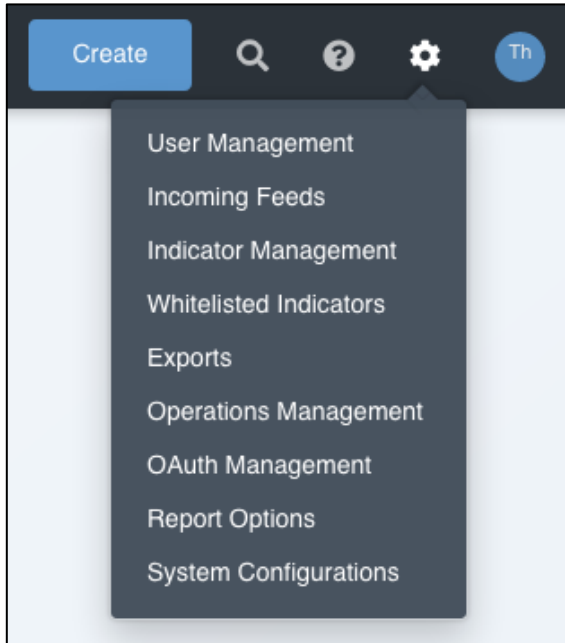
Installation or upgrade is now complete.

## 1.6 Configuring the Operation

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

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

**Figure 5: Operations Management – Configuration**



2. Expand the “**Palo Alto WildFire**” configuration.

**Figure 6: Operation Configuration**



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

## 1.7 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 File Example

This action allows you to submit a file to Wildfire's file analysis engine. The response will include the hashes for the given file so you can relate them and fetch the report once the analysis is finished.

**Figure 7: WildFire File Submission Example Output**

The screenshot shows the Palo Alto Networks WildFire 'Submit File' interface. It displays a 'Success!' message and a table of indicators. The table has columns for 'Value' and 'Type'. Below the table is a 'Raw Response' section showing an XML document.


Value	Type
056e4a359fb7b620cedd832af1d5e2a1	MD5
00b32c3428362e39e4df2a0c3e0950947c147781fdd3d2fdd0bf5f96989bb002	SHA-256

```
<?xml version="1.0" encoding="UTF-8"?>
<wildfire>
  <upload-file-info>
    <url></url>
    <filetype>Adobe PDF document</filetype>
    <filename>zombies.pdf</filename>
    <sha256>00b32c3428362e39e4df2a0c3e0950947c147781fdd3d2fdd0bf5f96989bb002</sha256>
    <md5>056e4a359fb7b620cedd832af1d5e2a1</md5>
    <size>399500</size>
  </upload-file-info>
</wildfire>
```

## Wildfire Get Report Example

This action allows you to query Wildfire for any hits on a hash. If found, it will return a report for the hash in two forms. First, it will download a PDF report, and then upload and relate it to the ThreatQ hash. Second, it will parse the returned XML report and display some results immediately to your operation results window. Here is an example result when you run the action.

**Figure 8: Wildfire Report Example Output**



Successfully uploaded/report!

### File Information

<input type="checkbox"/>	Name	Value
<input type="checkbox"/>	Search	Search
<input type="checkbox"/>	File Type	PE64
<input type="checkbox"/>	Size	932864
<input type="checkbox"/>	Malware	yes

Add Selected Attributes

Report from Windows 7 x64 SP1, Adobe Reader 11, Flash 11, Office 2010

Show

Report from Windows 10 x64, Flash 22, Adobe Reader 11, Office 2010

Show

Report from PE Static Analyzer

Show

Raw Response

Show

## Wildfire Verdict Example

This action allows you to query Wildfire for any hits on a hash. If found, it will return a single attribute informing you of the verdict on the hash. The available verdicts are: Malware, Grayware, Phishing, or Benign.

**Figure 9: Wildfire Verdict Example Output**

### Wildfire Verdict

<input type="checkbox"/>	Verdict
<input type="checkbox"/>	Search
<input type="checkbox"/>	Malware

Add Selected Attributes

Raw Response

Show

# Trademarks and Disclaimers

---

THE SUBJECT AND SPECIFICATIONS INCLUDING ALL INFORMATION REGARDING THE PRODUCTS IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE AT THE TIME OF WRITING 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 TERMS AND CONDITIONS WHEN PURCHASED. 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.

It is wholly the customers responsibility for any design requirements and the utilization of any recommendations provided by ThreatQuotient. ThreatQuotient recommendations are based upon customer information provided to ThreatQuotient at the time of the services. ThreatQuotient shall not be liable for the accuracy or completeness of the customer information contained in the ThreatQuotient recommendations.

All documentation and deliverables shall be provided in the English language, unless specifically stated otherwise. or agreed before the commencement of any services in writing.

Any costs incurred by ThreatQuotient as a result of translations requested by Customer shall be Customer's responsibility.

In the event of any conflict between this English version and the translation(s), the English version will prevail.

ThreatQuotient and the ThreatQuotient Rhino Logo are trademarks of ThreatQuotient, Inc.

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.

©2019 ThreatQuotient, Inc. All rights reserved.