

ThreatQuotient



ThreatQuotient for AbuseIPDB Operation

Version 1.0.0

August 21, 2019

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: 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, August 21, 2019

Contents

WARNING AND DISCLAIMER.....	2
CONTENTS	4
LIST OF FIGURES AND TABLES	5
1 INTRODUCTION.....	6
1.1 APPLICATION FUNCTION	6
1.2 PREFACE	6
1.3 AUDIENCE	6
1.4 SCOPE	6
2 THREATQUOTIENT FOR ABUSEIPDB OPERATION INSTALLATION	7
2.1 SETTING UP THE INTEGRATION	7
2.2 CONFIGURING THE OPERATION	9
2.3 USING THE OPERATION	10
2.3.1 Check	10
TRADEMARKS AND DISCLAIMERS	11

List of Figures and Tables

FIGURE 1: OPERATIONS MANAGEMENT – INSTALL7

FIGURE 2: INSTALL OPERATION7

FIGURE 3: ADD OPERATION8

FIGURE 4: OPERATIONS MANAGEMENT – CONFIGURATION9

FIGURE 5: OPERATION CONFIGURATION.....9

FIGURE 6: ABUSEIPDB OPERATION SUBMIT EXAMPLE.....10

TABLE 1: THREATQUOTIENT SOFTWARE & APP VERSION INFORMATION6

1 Introduction

1.1 Application Function

The ThreatQuotient for AbuseIPDB Operation enables a ThreatQ user to query AbuseIPDB for enrichment metadata.

1.2 Preface

This guide provides the information necessary to implement the ThreatQuotient for AbuseIPDB 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 the 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 ThreatQuotient for AbuseIPDB Operation only.

Table 1: ThreatQuotient Software & App Version Information

Software/App Name	File Name	Version
ThreatQ	Version 4.20.x or greater	
ThreatQuotient for AbuseIPDB Operation	1.0.0	

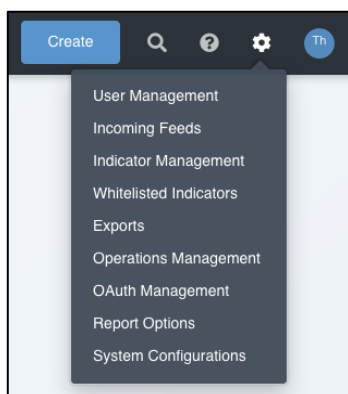
2 ThreatQuotient for AbuseIPDB Operation Installation

2.1 Setting up the Integration

Ensure the file `tq_op_abuse_ip_db-1.0.0-py3-none-any.whl` is available on the device being used to administer the ThreatQ instance in which the ThreatQuotient for AbuseIPDB Operation is being installed/upgraded.

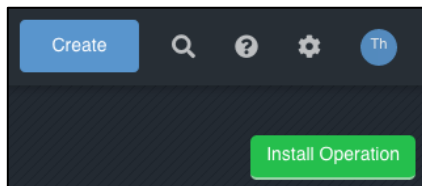
1. Navigate to the **Settings icon > Operations Management**.

Figure 1: Operations Management – Install



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

Figure 2: Install Operation

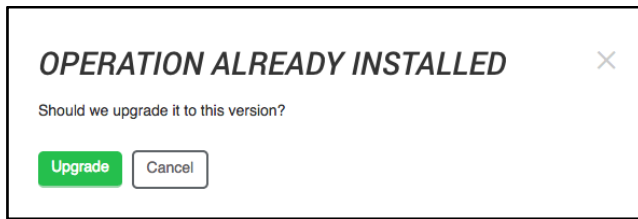


3. Drag the `tq_op_abuse_ip_db-1.0.0-py3-none-any.whl` to the Add Operation Popup or Click to Browse to the required file.
4. Click **Install** or **Upgrade**.



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

Figure 3: Add Operation



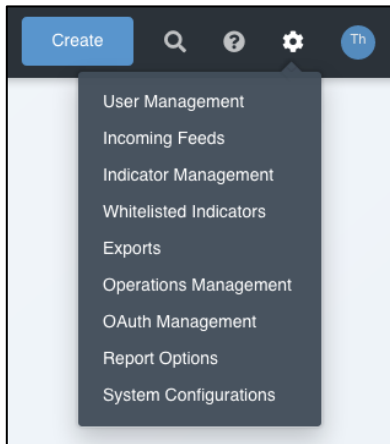
Installation/upgrade is now complete.

2.2 Configuring the Operation

The following section covers the configuration of the ThreatQuotient for AbuseIPDB Operation.

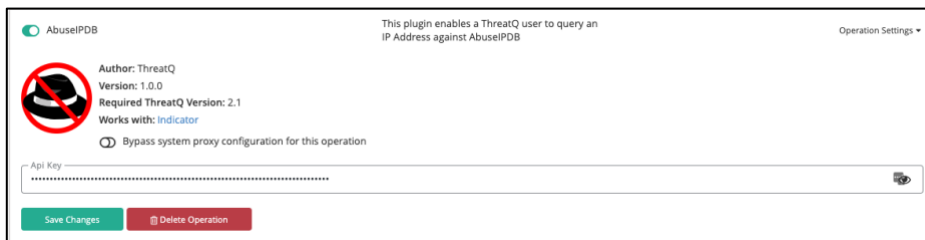
1. Navigate to the **Settings icons > Operations Management**.

Figure 4: Operations Management – Configuration



2. Expand the **AbuseIPDB** Operation Settings configuration.

Figure 5: Operation Configuration



3. Enter your **AbuseIPDB API Key** into the **API Key** field.
4. Click **Save Changes**.
5. Click the toggle in next to the **AbuseIPDB** name to enable the operation.

2.3 Using the Operation

The following section covers the use of the ThreatQuotient for AbuseIPDB Operation.

2.3.1 Check

This action will query AbuseIPDB for any IP address hits.

Applies to: IP Address

Figure 6: AbuseIPDB Operation Submit Example

Operations

AbuseIPDB: Check

Results for 103.1.100.95

Metadata

Showing 1 to 10 of 10

Row count: 25

NAME	VALUE
Country Code	IN
Usage Type	Fixed Line ISP
ISP	Gujarat Telelink Pvt Ltd
Abuse Confidence Score	14
Total Reports	7
Is Public	True
Category	Port Scan
Category	Hacking
Is Whitelisted	False
Country	India

Add Selected Attributes

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.