# ThreatQuotient

## ThreatQuotient for AbuseIPDB Operation Guide

Version 1.0.2

Monday, May 18, 2020

**ThreatQuotient**

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

### Support

Email: support@threatq.com

Web: Support.threatq.com

Phone: 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.

# Contents

# Versioning

- Integration Version: 1.0.2
- ThreatQ Version: 4.20.0 or greater

# Introduction

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

## 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.

## Audience

This document is intended for use by the following parties:

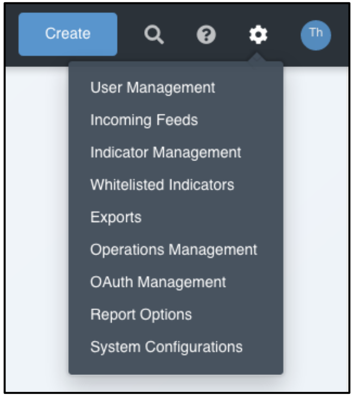
1. ThreatQ and Security Engineers.
2. ThreatQuotient Professional Services Project Team & Engineers.

# Installation

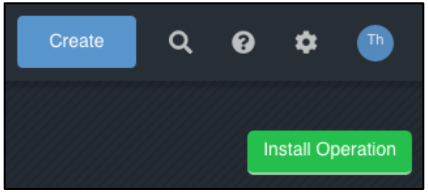
Perform the following steps to install the operation:

Note: The same steps can be used to upgrade the operation to a new version.

1. Ensure the .whl file is available on the device being used to administer the ThreatQ instance in which the ThreatQuotient for AbuseIPDB Operation is being installed/upgraded.
2. Log into your ThreatQ instance.
3. Click on the **Settings** icon and select **Operations Management**.



4. Click on the **Install Operation** button.



5. Upload the operation file using one of the following methods:

- Drag and drop the file into the dialog box.
- Select Click to Browse to locate the operation file on your local machine.

  **Note:** ThreatQ will inform you if the operation already exists on the platform and will require user confirmation before proceeding.

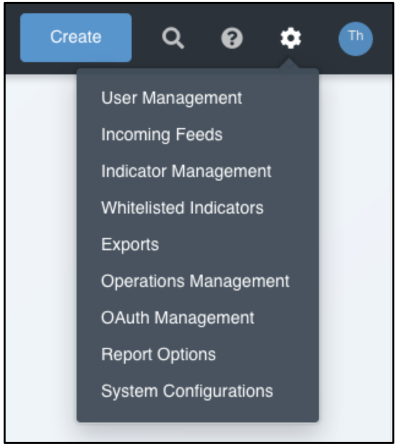
The operation will be added to your list of installed operations. You will still need to configure and enable the operation.

# Configuration

> ***Note:*** *ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other operation-related credentials.*

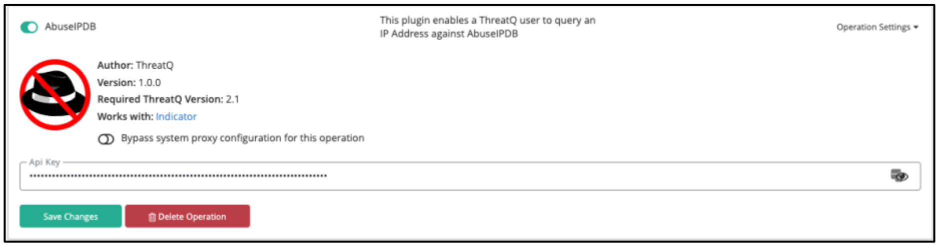
**To configure the connector:**

1. Click on the **Settings** icon and select **Operations Management**.



2. Locate the operation and click on **Operation Settings**.
3. Enter the following configuration parameter:

| Parameter | Description |
|---|---|
| API Key | Your AbuseIPDB API key. |


AbuseIPDB

This plugin enables a ThreatQ user to query an IP Address against AbuseIPDB

Operation Settings ▾

**Author:** ThreatQ
**Version:** 1.0.0
**Required ThreatQ Version:** 2.1
**Works with:** Indicator

○ Bypass system proxy configuration for this operation

Api Key
••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••

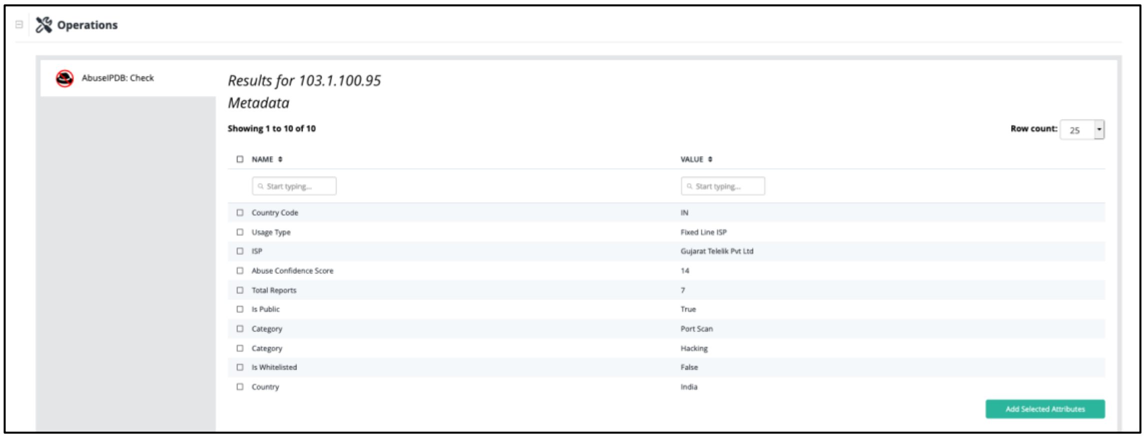
Save Changes | Delete Operation

4. Click on Save Changes.
5. Click on the toggle switch to the left of the connector name to enable the connector.

# Usage

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

The Check action will query AbuseIPDB for any IP address hits.



*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 Telelik Pvt Ltd |
| □ Abuse Confidence Score | 14 |
| □ Total Reports | 7 |
| □ Is Public | True |
| □ Category | Port Scan |
| □ Category | Hacking |
| □ Is Whitelisted | False |
| □ Country | India |

# Change Log

| Version | Details |
|---|---|
| 1.0.2 | - Added the hostname as a user specified parameters with a default value.<br>- Added a checkbox for the user to bring in reports as attributes in the UI instead of always showing them as default.<br>- Modified the operation to make it compatible with the auto-enrichment framework. |
| 1.0.0 | Initial Release |