

# ThreatQuotient



## ThreatQuotient for AbuseIPDB Operation User Guide

Version 1.0.3

October 23, 2023

**ThreatQuotient**

20130 Lakeview Center Plaza Suite 400  
Ashburn, VA 20147

 **ThreatQ Supported**

### Support

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

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

Phone: 703.574.9893

# Contents

Warning and Disclaimer ..... 3

Support ..... 4

Integration Details..... 5

Introduction ..... 6

Installation..... 7

Configuration ..... 8

Actions ..... 9

Change Log ..... 10

# 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 © 2023 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.

# Support

This integration is designated as **ThreatQ Supported**.

**Support Email:** [support@threatq.com](mailto: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.

# Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.3
Compatible with ThreatQ Versions	>= 4.20.0
Support Tier	ThreatQ Supported

# Introduction

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

The operation provides the following action:

- **Check** - queries AbuseIPDB for any IP Address hits.

The operation is compatible with IP Address Indicator types.

# Installation

Perform the following steps to install the integration:



The same steps can be used to upgrade the integration to a new version.

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
  - Drag and drop the file into the dialog box
  - Select **Click to Browse** to locate the integration file on your local machine



ThreatQ will inform you if the operation already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the operation contains changes to the user configuration. The new user configurations will overwrite the existing ones for the operation and will require user confirmation before proceeding.

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to [configure](#) and then [enable](#) the operation.

# Configuration



ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Hostname	The Hostname or IP Address of AbuseIPDB API.
API Key	Your AbuseIPDB API Key.
Show AbuseIPDB Reports in Output	Show user reports of abusive activity in the output. This allows you to decide if they want to see all the user reports from AbuseIPDB.

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.





# Change Log

- **Version 1.0.3**
  - Fixed a timeout error.
- **Version 1.0.2**
  - Added the hostname as a user specified parameters with a default value.
  - Added a checkbox for the user to bring in reports as attributes in the UI instead of always showing them as default.
  - Modified the operation to make it compatible with the auto-enrichment framework.
- **Version 1.0.0**
  - Initial release