ThreatQuotient

A Securonix Company

AbuseIPDB Action

Version 1.0.0

July 07, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.com
Phone: 703.574.9893

Contents

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.

Support

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

Support Email: tq-support@securonix.com
Support Web: https://ts.securonix.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	1.0.0
Compatible with ThreatQ Versions	>= 5.12.1
Compatible with AbuseIPDB Versions	API v2
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The AbuseIPDB Action for ThreatQ enables users to automate reputation lookups for IP address indicators against AbuseIPDB's community-driven threat intelligence database. The action retrieves abuse reporting, categorization, and geolocation context for each IP address and ingests the results into ThreatQ to support enrichment and investigation workflows.

The integration provides the following action:

- **AbuseIPDB - Check IPs** - queries AbuseIPDB for supported IP addresses and returns reputation data, abuse reports, and related contextual information to enrich ThreatQ indicators.

The integration is compatible with IP Address type indicators

The integration returns the following enriched indicator types:

- FQDN
- IP Address

This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing IP Address indicator objects.
- An AbuseIPDB account with an API key.

> AbuseIPDB API usage is subject to the limits of your AbuseIPDB subscription. The free tier supports up to 1,000 API lookups per day, while paid subscription tiers provide higher daily request limits.

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 action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
    - Drag and drop the zip file into the dialog box
    - Select **Click to Browse** to locate the zip file on your local machine

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

You will still need to configure the action.

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 **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

   The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
API Key	Enter the AbuseIPDB API key used to authenticate requests. There is no default value.
Apply Whitelisted Status for Whitelisted IPs	Select this option to set the ThreatQ indicator status to `Whitelisted` when AbuseIPDB identifies the IP address as whitelisted. Disabled by default.
Context Filter	Select the contextual data to retrieve from AbuseIPDB and ingest into ThreatQ for each IP address. Options include: ◦ Abuse Confidence Score *(Default)* ◦ Categories *(Default)* ◦ Country Code ◦ Country *(Default)* ◦ Usage Types

PARAMETER	DESCRIPTION
	◦ ISP ◦ ISP Domain ◦ Associated Hostnames ◦ Is TOR
Add Reportings to Indicator Description	Select this option to append AbuseIPDB abuse reports to the ThreatQ indicator description when reports are available.
Set Status to Active for Selected Categories	Select the AbuseIPDB report categories that will cause the ThreatQ indicator status to be set to `Active`. If no categories are selected, the default ThreatQ indicator status is preserved. Options include: ◦ DNS Compromise *(Default)* ◦ DNS Poisoning *(Default)* ◦ Fraud Orders ◦ DDoS Attack ◦ FTP Brute-Force *(Default)* ◦ Ping of Death ◦ Phishing *(Default)* ◦ Fraud VoIP ◦ Open Proxy ◦ Web Spam ◦ Email Spam ◦ Blog Spam ◦ VPN IP ◦ Port Scan ◦ Hacking *(Default)* ◦ SQL Injection *(Default)*

PARAMETER	DESCRIPTION
	◦ Spoofing *(Default)* ◦ Brute-Force *(Default)* ◦ Bad Web Bot ◦ Exploited Host *(Default)* ◦ Web App Attack ◦ SSH ◦ IoT Targeted See AbuseIPDB's Categories topic for a description of each category.
Associated Hostname Status	Select the status to assign to associated hostname indicators. Options include: ◦ Review ◦ Indirect ◦ Active This parameter is available only when `Associated Hostnames` is selected in the **Context Filter** parameter.
Objects Per Run	Specify the maximum number of objects to process during a single execution. The default value is `1000`.

5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
AbuseIPDB - Check IPs	Performs a bulk lookup of IPs against AbuseIPDB	Indicators	IP Address

AbuseIPDB - Check IPs

The AbuseIPDB – Check IPs action enriches IP address indicators in your Threat Library by querying the AbuseIPDB Check API. The action retrieves available reputation, geolocation, categorization, and abuse reporting information for each IP address and ingests the selected context into ThreatQ. All enrichment options are configurable and can be enabled or disabled through the action settings.

```
GET https://api.abuseipdb.com/api/v2/check
```

Sample Response (truncated):


```
{
  "data": {
    "ipAddress": "82.196.3.179",
    "isPublic": true,
    "ipVersion": 4,
    "isWhitelisted": false,
    "abuseConfidenceScore": 100,
    "countryCode": "NL",
    "usageType": "Data Center/Web Hosting/Transit",
    "isp": "DigitalOcean LLC",
    "domain": "digitalocean.com",
    "hostnames": [
      "sexolviv.com"
    ],
    "isTor": false,
    "countryName": "Netherlands",
    "totalReports": 552,
    "numDistinctUsers": 287,
    "lastReportedAt": "2024-01-18T14:05:28+00:00",
    "reports": [
      {
        "reportedAt": "2024-01-18T14:05:28+00:00",
        "comment": "Automatic report: Failed SSH login [5]",
        "categories": [18, 22],
        "reporterId": 20815,
        "reporterCountryCode": "DE",
        "reporterCountryName": "Germany"
      },
      {
        "reportedAt": "2024-01-18T14:04:49+00:00",
        "comment": "SSH Bruteforce...",
```

```
        "categories": [18, 22],
        "reporterId": 96236,
        "reporterCountryCode": "DE",
        "reporterCountryName": "Germany"
      },
      {
        "reportedAt": "2024-01-18T13:53:23+00:00",
        "comment": "Jan 18 14:51:17 ... Failed password ... Invalid
user ...",
        "categories": [18, 22],
        "reporterId": 74364,
        "reporterCountryCode": "DE",
        "reporterCountryName": "Germany"
      },
      {
        "reportedAt": "2024-01-18T13:29:01+00:00",
        "comment": "Jan 18 14:22:15 ... Failed password ... Invalid
user ...",
        "categories": [18, 22],
        "reporterId": 74364,
        "reporterCountryCode": "DE",
        "reporterCountryName": "Germany"
      }
    ]
  }
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
hostnames[]	Indicator.Value	FQDN	N/A	sexolviv.com	N/A
.abuseConfidenceScore	Indicator.Attribute	Abuse Confidence Score	N/A	100	Optional; Applied to original IP. Only added if score > 0
.reports[].categories[]	Indicator.Attribute	Category	N/A	Hacking	Optional; Mapped from ID -> Name; Applied to original IP. Mapped according to values below
.isTor	Indicator.Attribute	Is TOR	N/A	true	Optional; Applied to original IP
.countryCode	Indicator.Attribute	Country Code	N/A	US	Optional; Applied to original IP & Hostnames
.countryName	Indicator.Attribute	Country	N/A	Canada	Optional; Applied to original IP & Hostnames

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.usageType	Indicator.Attribute	Usage Type	N/A	Web Hosting	Optional; Applied to original IP & Hostnames
.isp	Indicator.Attribute	ISP	N/A	DigitalOcean LLC	Optional; Applied to original IP & Hostnames
.domain	Indicator.Attribute	ISP Domain	N/A	digitalocean.com	Optional; Applied to original IP & Hostnames

Category Mapping

The following table lists the AbuseIPDB category IDs and their corresponding category names. These mappings are used by the **Set Status to Active for Selected Categories** parameter to determine which abuse categories will cause an indicator's status to be set to **Active** during enrichment.

ID	NAME
1	DNS Compromise
2	DNS Poisoning
3	Fraud Orders
4	DDoS Attack
5	FTP Brute-Force
6	Ping of Death
7	Phishing
8	Fraud VoIP
9	Open Proxy
10	Web Spam
11	Email Spam

ID	NAME
12	Blog Spam
13	VPN IP
14	Port Scan
15	Hacking
16	SQL Injection
17	Spoofing
18	Brute-Force
19	Bad Web Bot
20	Exploited Host
21	Web App Attack
22	SSH
23	IoT Targeted

Enriched Data

Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

METRIC	RESULT
Run Time	2 minutes
Indicators	12
Indicator Attributes	84

Use Case Example

1. A Threat Analyst creates a ThreatQ data collection containing IP Address indicators that require additional reputation and contextual enrichment.
2. The analyst adds the **AbuseIPDB – Check IPs** action to a workflow and configures the desired enrichment options.
3. The workflow submits each IP address to the AbuseIPDB **Check** API and retrieves the selected reputation, categorization, geolocation, ISP, usage type, TOR, whitelist, hostname, and abuse reporting information.
4. The action enriches the original IP Address indicators with the selected AbuseIPDB context and optionally creates related FQDN indicators from associated hostnames.
5. If configured, AbuseIPDB report details are appended to the ThreatQ indicator descriptions, providing analysts with additional context for investigation and prioritization.

Known Issues / Limitations

- AbuseIPDB API usage is subject to the limits of your AbuseIPDB subscription. The free tier supports up to **1,000 API lookups per day**, while paid subscription tiers provide higher daily request limits. Be aware of your API rate limits and configure the **Objects Per Run** setting accordingly.

Change Log

- **Version 1.0.0**
  - Initial release