# ThreatQuotient

## Universal CSV Parser Action

**Version 1.0.0**

October 07, 2024

**ThreatQuotient**
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

**ThreatQ Supported**

**Support**

| | |
|---|---|
| Email: | support@threatq.com |
| Web: | support.threatq.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**: 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** | 1.0.0 |
| **Compatible with ThreatQ Versions** | >= 5.12.1 |
| **ThreatQ TQO License Required** | Yes |
| **Support Tier** | ThreatQ Supported |

# Introduction

The Universal CSV Parser Action parses selected CSV files using ThreatQ default mappings for the columns.

> ⚠ Input CSV files must have the column headers present in the file.

The action will parse the CSV file and create indicators based on the columns present in the file as well as normalize the data in the columns to the appropriate data types.

The integration provides the following action:

- **Universal CSV Parser -** parses CSV files and creates indicators, attributes, and relationships based on the columns present in the file.

The action is compatible with File object types (CSV files).

The action returns the following enriched system objects:

- Adversaries
- Attack Patterns
- Indicators
- Malware
- Tags

> 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 CSV Files.

# 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

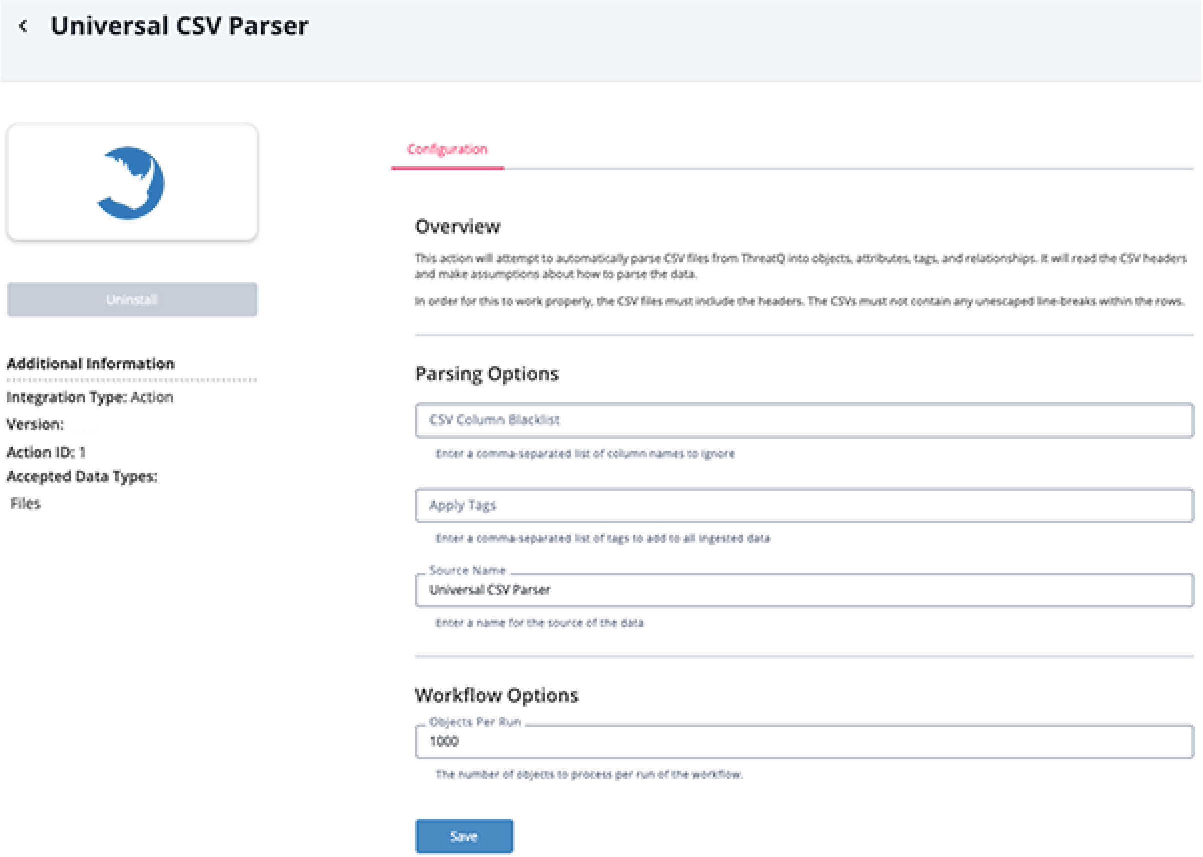
ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

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 |
|---|---|
| **CSV Column Blacklist** | Enter a comma-separated list of column names to ignore. |
| **Apply Tags** | Enter a comma-separated list of tags to add to all ingested data |
| **Source Names** | Enter a name for the source of the data. The default value is **Universal CSV Parser**. |
| **Objects Per Run** | The maximum number of objects to process per run. |



Universal CSV Parser

Additional Information

Integration Type: Action

Version:

Action ID: 1

Accepted Data Types:

Files

Overview

This action will attempt to automatically parse CSV files from ThreatQ into objects, attributes, tags, and relationships. It will read the CSV headers and make assumptions about how to parse the data.

In order for this to work properly, the CSV files must include the headers. The CSVs must not contain any unescaped line-breaks within the rows.

Parsing Options

CSV Column Blacklist

Enter a comma-separated list of column names to ignore

Apply Tags

Enter a comma-separated list of tags to add to all ingested data

Source Name: Universal CSV Parser

Enter a name for the source of the data

Workflow Options

Objects Per Run: 1000

The number of objects to process per run of the workflow.

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

# Actions

The following actions are available:

| ACTION | DESCRIPTION | OBJECT TYPE | OBJECT SUBTYPE |
|---|---|---|---|
| Universal CSV Parser | Parses IOCs and Context out of CSV files saved in ThreatQ. | Files | CSV - Generic Text |

## Universal CSV Parser

The Universal CSV Parser action takes input CSV files from the ThreatQ Threat Library and parses them for IOCs, relationships, attributes, and other context.

> This action uses sensible default mappings for columns in the CSV file. CSVs without column headers will not be parsed correctly, and likely ignored. If you are not seeing data being mapped properly, please ensure that the column headers are present in the CSV first.

### API Mapping

The following is a list of the default mappings for the columns in the CSV file to the ThreatQ API objects.

| COLUMN NAME | OBJECT TYPE | OBJECT SUBTYPE |
|---|---|---|
| title | Report | |
| report | Report | |
| type | Subtype | |
| ioc_type | Subtype | |
| entity_type | Subtype | |

| COLUMN NAME | OBJECT TYPE | OBJECT SUBTYPE |
|---|---|---|
| indicator_type | Subtype | |
| indicatortype | Subtype | |
| value | Indicator | |
| data | Indicator | |
| indvalue | Indicator | |
| indval | Indicator | |
| ind_value | Indicator | |
| indicator_value | Indicator | |
| ind_val | Indicator | |
| ind | Indicator | |
| ioc | Indicator | |
| indicator | Indicator | |
| observable | Indicator | |
| hash | Indicator | |
| sample | Indicator | |
| file | Indicator | |
| c2 | Indicator | IP Address |

| COLUMN NAME | OBJECT TYPE | OBJECT SUBTYPE |
|---|---|---|
| c2_server | Indicator | IP Address |
| ip_dst | Indicator | IP Address |
| ip_src | Indicator | IP Address |
| source_ip | Indicator | IP Address |
| destination_ip | Indicator | IP Address |
| ip_source | Indicator | IP Address |
| ip_destination | Indicator | IP Address |
| dst_ip | Indicator | IP Address |
| src_ip | Indicator | IP Address |
| ip | Indicator | IP Address |
| ip_address | Indicator | IP Address |
| ipv4 | Indicator | IP Address |
| address | Indicator | IP Address |
| ip_attacker | Indicator | IP Address |
| ipv6 | Indicator | IPv6 Address |
| url | Indicator | URL |
| asn | Indicator | ASN |

| COLUMN NAME | OBJECT TYPE | OBJECT SUBTYPE |
|---|---|---|
| domain | Indicator | FQDN |
| fqdn | Indicator | FQDN |
| host | Indicator | FQDN |
| dns | Indicator | FQDN |
| md5 | Indicator | MD5 |
| md5_hash | Indicator | MD5 |
| sha1 | Indicator | SHA-1 |
| sha1_hash | Indicator | SHA-1 |
| sha_1 | Indicator | SHA-1 |
| sha256 | Indicator | SHA-256 |
| sha256_hash | Indicator | SHA-256 |
| sha_256 | Indicator | SHA-256 |
| sha512 | Indicator | SHA-512 |
| sha512_hash | Indicator | SHA-512 |
| sha_512 | Indicator | SHA-512 |
| sha384 | Indicator | SHA-384 |
| sha384_hash | Indicator | SHA-384 |

| COLUMN NAME | OBJECT TYPE | OBJECT SUBTYPE |
|---|---|---|
| sha_384 | Indicator | SHA-384 |
| hash_md5 | Indicator | MD5 |
| hash_sha1 | Indicator | SHA-1 |
| hash_sha256 | Indicator | SHA-256 |
| hash_sha512 | Indicator | SHA-512 |
| hash_sha384 | Indicator | SHA-384 |
| filehash_md5 | Indicator | MD5 |
| filehash_sha1 | Indicator | SHA-1 |
| filehash_sha256 | Indicator | SHA-256 |
| filehash_sha512 | Indicator | SHA-512 |
| filehash_sha384 | Indicator | SHA-384 |
| mutex | Indicator | Mutex |
| cve | Indicator | CVE |
| vulnerability | Indicator | CVE |
| email | Indicator | Email Address |
| email_address | Indicator | Email Address |
| file_name | Indicator | Filename |

| COLUMN NAME | OBJECT TYPE | OBJECT SUBTYPE |
|---|---|---|
| filename | Indicator | Filename |
| campaign | Campaign | |
| adversary | Adversaries | |
| adversaries | Adversaries | |
| threat_actor | Adversaries | |
| actor | Adversaries | |
| handle | Adversaries | |
| malware | Malware | |
| family | Malware | |
| families | Malware | |
| malware_family | Malware | |
| malware_families | Malware | |
| malware_class | Malware | |
| signature | Malware | |
| tag | Tag | |
| tags | Tag | |
| date | Published At | |

| COLUMN NAME | OBJECT TYPE | OBJECT SUBTYPE |
|---|---|---|
| dateins | Published At | |
| date_discovered | Published At | |
| timestamp | Published At | |
| dateadded | Published At | |
| published | Published At | |
| created | Published At | |
| last_seen | Published At | |
| first_seen | Published At | |
| date_discovered | Published At | |
| discovered_at | Published At | |
| published_at | Published At | |
| created_at | Published At | |
| first_seen_utc | Published At | |
| description | Description | |
| descriptions | Description | |
| short_description | Description | |
| long_description | Description | |

| COLUMN NAME | OBJECT TYPE | OBJECT SUBTYPE |
|---|---|---|
| overview | Description | |
| summary | Description | |
| tlp | TLP | |
| country | Attribute | Country |
| country_code | Attribute | Country Code |
| status | Status | |
| status_name | Status | |
| attack_pattern | Attack Pattern | |
| attack_patterns | Attack Pattern | |

# 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** | 24 minutes |
| **Indicators** | 10 |
| **Indicator Attributes** | 30 |

# Use Case Example

- I receive Threat Intelligence via a CSV file from a third-party vendor. I need the data to be parsed and converted into ThreatQ objects for further analysis. I also want to maintain the supporting context from the columns in the CSV file, to the corresponding indicator/object.
- I have an intelligence mailbox setup to receive Threat Intelligence reports from third-party vendors. I want to automatically have those files parsed and converted into ThreatQ objects for further analysis.

# Known Issues / Limitations

- Input CSV files *must* have the column headers present in the file in order for the action to work.

# Change Log

- **Version 1.0.0**
  - Initial release