

ThreatQuotient

A Securonix Company



Cisco Umbrella Popularity List CDF

Version 1.0.0

October 05, 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..... 3

Support..... 4

Integration Details..... 5

Introduction 6

Installation 7

Configuration 8

ThreatQ Mapping.....10

 Cisco Umbrella Popularity List10

 Normalized Rank Mapping11

Average Feed Run.....12

Change Log13

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 © 2026 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: 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	>= 5.5.0
Support Tier	ThreatQ Supported

Introduction

The Cisco Umbrella Popularity List CDF ingests a configurable subset of highly queried domains from the Cisco Umbrella global network into ThreatQ as whitelisted FQDN indicators. These indicators help prevent commonly used domains from being identified as malicious by later intelligence imports, blocklists, or detection workflows.

The Cisco Umbrella Popularity List ranks the one million domains most frequently queried across the Cisco Umbrella global network. The ranking reflects DNS activity and includes root domains and subdomains, rather than relying only on web-browser traffic. More information is available on the [Cisco Umbrella Popularity List page](#).

The integration provides the following feed:

- **Cisco Umbrella Popularity List** - ingests up to the first 10,000 entries from the current or a historical Cisco Umbrella Popularity List snapshot.

The integration ingests indicator and indicator attribute objects into the ThreatQ platform.

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



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

The feed(s) will be added to the integrations page. You will still need to [configure and then enable](#) the feed.

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 **OSINT** option from the *Category* dropdown (optional).



If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Domains to Ingest	Select the number of highest-ranked domains to ingest. Options include: ◦ Top 10 ◦ Top 100 (<i>default</i>) ◦ Top 1,000 ◦ Top 10,000
Rank Attribute Format	Select how the Cisco rank is stored for each indicator. Options include: ◦ Normalized Rank Bands (<i>default</i>) - stores Top 10, Top 100, Top 1,000, or Top 10,000. This option reduces update churn when a domain's exact rank changes slightly between daily lists. ◦ Exact Numeric Rank - stores the numeric rank supplied by Cisco. This can cause substantially more indicator updates between runs. ◦ Do Not Ingest Rank - does not add or update the Cisco Umbrella Popularity Rank attribute.

PARAMETER	DESCRIPTION
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.

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.

ThreatQ Mapping

Cisco Umbrella Popularity List

The Cisco Umbrella Popularity List feed imports commonly queried domains into ThreatQ as whitelisted FQDN indicators to reduce false positives in threat intelligence and detection workflows.

Scheduled Run

Scheduled runs download the current list.

```
GET https://s3-us-west-1.amazonaws.com/umbrella-static/top-1m.csv.zip
```

Manual Run

Manual runs use the run's start date to request a historical snapshot.

```
GET https://s3-us-west-1.amazonaws.com/umbrella-static/top-1m-<YYYY-MM-DD>.csv.zip
```

Sample Response:

```
1,google.com
2,gstatic.com
3,www.google.com
4,microsoft.com
5,data.microsoft.com
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
0 (first token)	Indicator.Attribute	Cisco Umbrella Popularity Rank	N/A	Top 10	Included when Rank Attribute Format is Normalized Rank Bands. Updated at ingestion.
0 (first token)	Indicator.Attribute	Cisco Umbrella Popularity Rank	N/A	1	Included when Rank Attribute Format is Exact Numeric Rank. Updated at ingestion.
1 (second token)	Indicator.Value	FQDN	N/A	google.com	The indicator status is set to Whitelisted.

Normalized Rank Mapping

Normalized rank values are assigned as follows:

SOURCE RANK	ATTRIBUTE VALUE
1-10	Top 10
11-100	Top 100
101-1,000	Top 1,000
1,001-10,000	Top 10,000

Average Feed Run



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

METRIC	RESULT
Run Time	N/A
Indicators	100
Indicator Attributes	100

Change Log

- **Version 1.0.0**
 - Initial release