ThreatQuotient

A Securonix Company

Proofpoint TIS CDF

Version 1.0.0

July 22, 2025

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
Support Tier	ThreatQ Supported

Introduction

The Proofpoint TIS CDF integration pulls indicators collected by the Proofpoint Threat Intelligence Services (TIS) team into the ThreatQ platform. These indicators are typically related to a specific threat actor or malware campaign.

> This integration does not ingest the full campaign details. Full campaign data can be ingested using the **Proofpoint TAP Campaigns CDF** integration.

The integration provides the following feed:

- **Proofpoint TIS Indicators -** pulls indicators collected by Proofpoint's TIS team.

The integration ingests the following object types:

- Campaigns
- Indicators

Prerequisites

The following is required to run the integration:

- Proofpoint TIS Credentials
    - Customer ID
    - Temp Key 1
    - Temp Key 2

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 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.

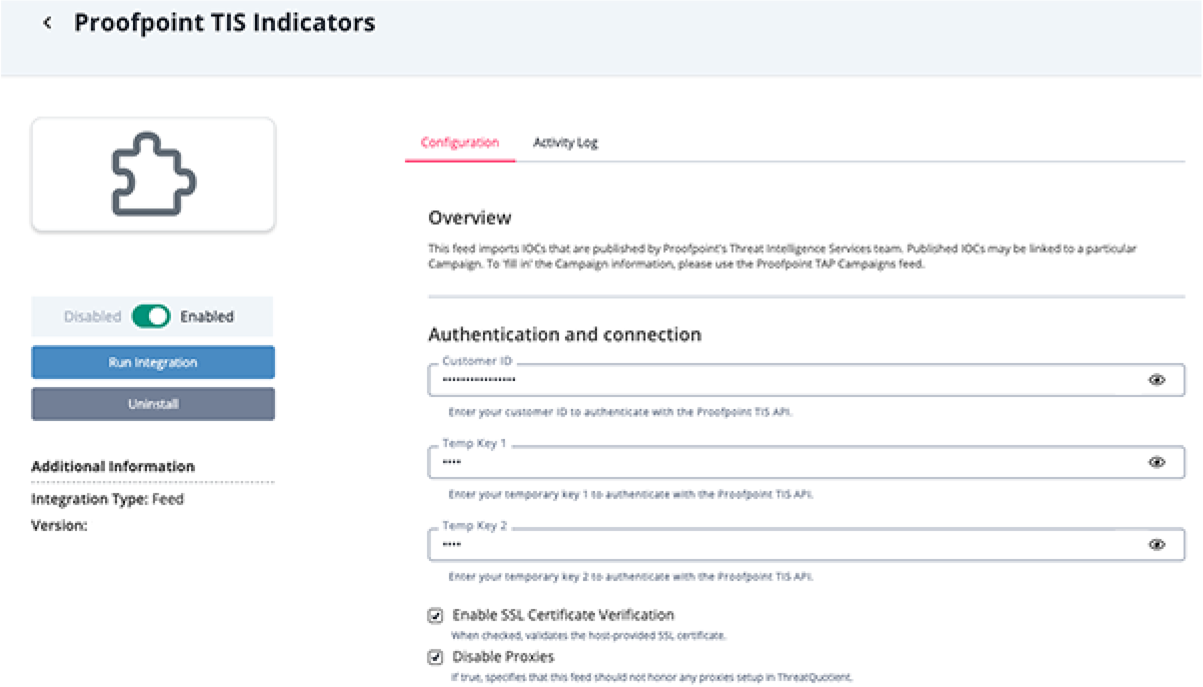
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** 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
Customer ID	Enter your customer ID to authenticate with the Proofpoint TIS API.
Temp Key 1	Enter your Temp Key 1 to authenticate with the Proofpoint TIS API.
Temp Key 2	Enter your Temp Key 2 to authenticate with the Proofpoint TIS API.
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.



‹ Proofpoint TIS Indicators

Additional Information

Integration Type: Feed

Version:

Overview

This feed imports IOCs that are published by Proofpoint's Threat Intelligence Services team. Published IOCs may be linked to a particular Campaign. To 'fill in' the Campaign information, please use the Proofpoint TAP Campaigns feed.

Authentication and connection

Customer ID: ••••••••••••••••

Enter your customer ID to authenticate with the Proofpoint TIS API.

Temp Key 1: ••••

Enter your temporary key 1 to authenticate with the Proofpoint TIS API.

Temp Key 2: ••••

Enter your temporary key 2 to authenticate with the Proofpoint TIS API.

☑ Enable SSL Certificate Verification

When checked, validates the host-provided SSL certificate.

☑ Disable Proxies

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.

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

Proofpoint TIS Indicators

The Proofpoint TIS Indicators feed automatically pulls indicators produced by the Proofpoint TIS team, into ThreatQ. Each indicator *may* be associated with a campaign.

> This feed does not provide the full campaign details. Full campaign data can be ingested using the **Proofpoint TAP Campaigns CDF** integration.

`GET https://tis-iocs.proofpoint.com`

Sample Response:

```
Date Added,Type,IOC,Campaign
29-
Feb-24,HASH,c308289f17f10ab5031acaa581f33ec42354909cbe7099225e00cacb82499576,Ac
meLocker | Compressed VBScript Attachments | acmephishstudios | 29 February
2024
29-Feb-24,URL,http://acmephishstudios.ydns.eu/sbv/wrg.txt,AcmeLocker |
Compressed VBScript Attachments | acmephishstudios | 29 February 2024
```

ThreatQ provides the following default mapping for this feed based on each column within the CSV response.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.data[2]`	Indicator Value	`.data[1]`	`.data[0]`	`c308289f17f10ab5031acaa581f33ec42354909cbe7099225e00cacb82499576`	Mapped according to `Proofpoint TIS Indicators Type Mapping`
`.data[3]`	Campaign Value	Campaign	`.data[0]`	`AcmeLocker | Compressed VBScript Attachments | acmephishstudios | 29 February 2024`	N/A

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	1 minute
Campaigns	4
Indicators	100

Known Issues / Limitations

- This feed does not provide the full campaign details. Full campaign data can be ingested using the **Proofpoint TAP Campaigns CDF** integration.

Change Log

- **Version 1.0.0**
    - Initial release