ThreatQuotient

A Securonix Company

Proofpoint EFD CDF

Version 1.0.0

November 17, 2025

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	>= 5.29.0
Support Tier	ThreatQ Supported

Introduction

The Proofpoint Email Fraud Defense (EFD) integration ingests lookalike domains detected by Proofpoint’s Email Fraud Defense solution into ThreatQ.

The integration provides the following feed:

- **Proofpoint EFD Lookalike Domains –** Periodically retrieves lookalike domains identified by Proofpoint’s Email Fraud Defense system to detect possible impersonation attempts or phishing campaigns.

The integration ingests indicators and indicator attributes.

Prerequisites

The following is required in order to install and run the integration:

- Proofpoint EFD API Client ID
- Proofpoint EFD API Client Secret

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 for Proofpoint EFD.
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.

6. The feed will be added to the integrations page. You will still need to configure and then enable the feed.

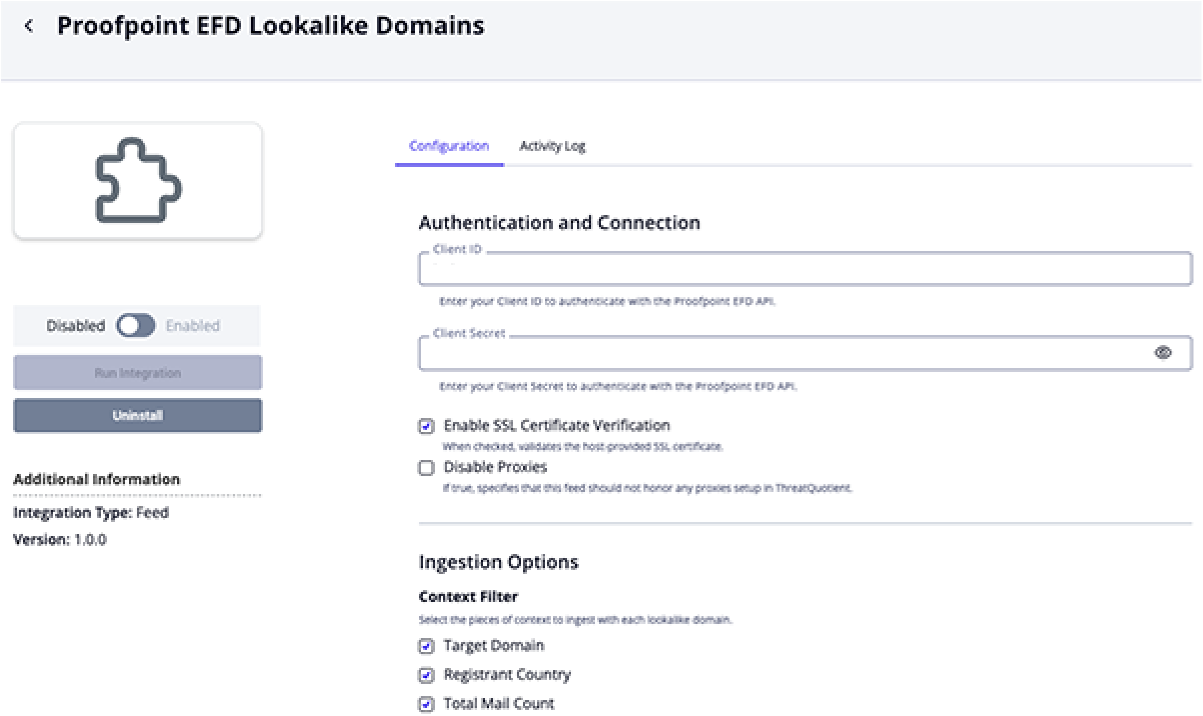
Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact Proofpoint to obtain API credentials.

To configure the integration:

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

PARAMETER	DESCRIPTION
Client ID	Enter your Proofpoint EFD API Client ID for authentication.
Client Secret	Enter your Proofpoint EFD API Client Secret for authentication.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Context Filter	Select context to ingest into the ThreatQ platform. Options include: ◦ Target Domain *(default)* ◦ Registrant Country *(default)* ◦ Total Mail Count



Proofpoint EFD Lookalike Domains

Additional Information

Integration Type: Feed

Version: 1.0.0

Authentication and Connection

Client ID

Enter your Client ID to authenticate with the Proofpoint EFD API.

Client Secret

Enter your Client Secret to authenticate with the Proofpoint EFD 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.

Ingestion Options

Context Filter

Select the pieces of context to ingest with each lookalike domain.

☑ Target Domain

☑ Registrant Country

☑ Total Mail Count

5. Review and adjust settings as needed, then click **Save**.
6. Click the toggle switch to enable the feed.

ThreatQ Mapping

Proofpoint EFD Lookalike Domains

This feed periodically ingests lookalike domains detected by Proofpoint's Email Fraud Defense solution. The parameter `previous_days` is dynamically calculated and supports values of 7, 30, 90, 180, and 365 days.

```
GET https://api.emaildefense.proofpoint.com/dmarc/v1/metrics/domain-lookalikes/details?previous_days=7
```

Sample Response:

```
{
  "data": {
    "results": [
      {
        "lookalikeDomain": "mykplan.click",
        "domain": "mykplan.com",
        "createdDate": "2025-04-03T00:00:00.000Z",
        "registrantCountry": "USA",
        "totalMailCount": 0
      }
    ]
  }
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.lookalikeDomain	Indicator.Value	FQDN	.createdDate	mykplan.click	N/A
.domain	Indicator.Attribute	Target Domain	.createdDate	mykplan.com	User-configurable
.registrantCountry	Indicator.Attribute	Country	.createdDate	USA	User-configurable
.totalMailCount	Indicator.Attribute	Total Mail Count	.createdDate	0	User-configurable, updatable

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
Indicators	3
Report Attributes	4

Change Log

- **Version 1.0.0**
  - Initial release