Proofpoint Secure Email Relay— API Overview

This document provides an overview to the Proofpoint Secure Email Relay (SER) API. Proofpoint SER provides a way for application email to have the same level of security, information protection and compliance as user-based emails while at the same time keeping the two separate. And it reduces threat risk by letting only credentialed senders use the service. The SER API is a REST API that you can use to integrate and automate data through business intelligence (BI) tools such as Tableau, Splunk and PowerBI.

Intended Audience

Both the Proofpoint SER API and this guide are meant for software engineers, system architects and system designers. To use the SER API, you must be familiar with API building blocks such as remote calls, object classes, variables, JavaScript and web application development. You can build software applications and business intelligence (BI) outputs using these building blocks. If you are not familiar with the concepts, engage others in your organization, such as your IT or software development team.

With the exception of dedicated Splunk and QRadar apps that were released in early 2022, the SER API is not an out-of-the-box tool and does not have predefined connectors. Therefore, your software engineering group must refer to the instructions provided by those tools for details on how to integrate the SER API.

Note: Because of the large variety of BI tools, your technical personnel must perform all programming. Proofpoint does not offer any programming assistance with integrating the SER API with your tools.

Token Generation

The SER API requires token-based authentication for secure access to data. You must generate an access token before using the API. The token provides your API users and applications with the credentials and authorization you need to securely access the data so you can perform requests and actions.
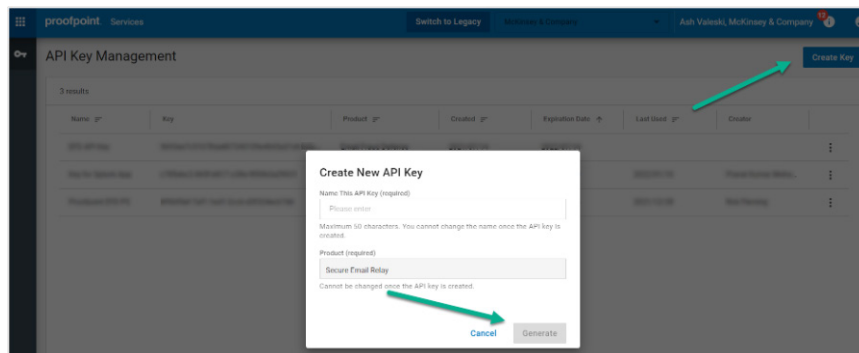
The administrative user associated with your SER account must first acquire a "secret" and "key" from the Proofpoint Admin Interface to generate a token.

To get the secret and key:

1. Login to **https://admin.emaildefense.proofpoint.com.**
2. Use the **App Switcher** in the top-left corner to go to **Services** > **API Key Management.**
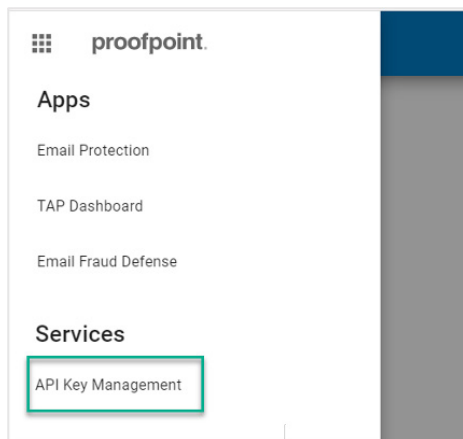
3. Select **Create Key** then **Secure Email Relay.**

Notes:

- If "Secure Email Relay" is not listed, then someone other than the SER Admin user is logged in.
- The secret and key expire one year after activation.

You have obtained the secret and key.

Token Requests

Request a token from the token endpoint: **https://auth.proofpoint.com/v1/token**.

Example script:

```
#!/bin/sh
#
# Obtain OAUTH token to access Trap Handler
#
CLIENT_ID=yourKey
CLIENT_SECRET=yourSecret
OAUTH_URL=https://auth.proofpoint.com/v1/token
function gettoken() {
TOKEN=`curl -s -v -X POST ${OAUTH _ URL} -H "Cache-Control: no-cache" -d "grant_type=client_
credentials"' & '"client_id=${CLIENT_ID}"' & '"client_secret=${CLIENT_SECRET}" | cut -f 1 -d "," | cut -f
2 -d ":" | sed -e "s/^\"//g" | sed -e "s/\"$//g"`
echo $TOKEN
}
token=$(gettoken)
echo $token
```

Note: Tokens expire after 43,200 seconds (12 hours).

Data Retrieval

You can retrieve reporting data from the SER API at **https://ser-api.proofpoint.com** by providing the token obtained above along with a date range.

Requests are formatted as follows:

```
GET /v1/sercustomer/report/summary?key1=<>&key2=<>..
```

• Valid key1 values are: startTimeStamp=2020-06-01T00:00:00.000Z (greaterThanEquals)
• Valid key2 values are: endTimeStamp=2020-06-01T00:00:00.000Z (lessThan)
• The startTimeStamp,endTimeStamp format must be yyyy-MM-dd'T'HH:mm:ss.SSSZ
• If startTimeStamp is not provided, the API defaults to license_start.
• If endTimeStamp is not provided, the API defaults to the current time.

Example request 1

```
curl --location --request GET 'https://ser-api.proofpoint.com/v1/sercustomer/report/
summary?startTimeStamp=2019-02-10T12:34:00.016Z&endTimeStamp=2019-09-10T12:36:00.016Z' \
--header 'Authorization: Bearer TokenYouGet'
```

Example request 2

```
curl --location --request GET 'https://ser-api.proofpoint.com/v1/sercustomer/report/
summary?startTimeStamp=2019-02-10T12:34:00.016Z' \
--header 'Authorization: Bearer TokenYouGet'
```

Note: Up to 1,000 requests can be made per minute.

Data Response

Response data can be formatted as JSON or TEXT (uuencode) and organized into two blocks of content:

- **applicationUsers.** Provides activity detail broken down by application
- **entitlement.** Provides the throughput amount and license term, or the period of time in which the throughput applies.

All dates are UTC.

The table below provides a description for each tag/value pair.

Tag/Value Pairs

CATEGORY	TAG	DESCRIPTION
applicationUsers	applicationName	The display-friendly name of the application (among a list in the SER Global Application Database) to which the applicationUser is associated/mapped.
	applicationUserName	The display-friendly SMTP AUTH user name (not to be confused with the SMTP AUTH UID, which, along with the SMTP AUTH password, is configured on the application that's submitting email to the system).
	fromEnvelope	The RFC.5321 Envelope/MFROM address authorized for use with the SMTP AUTH UID. Note: a domain-only value means {wildcard}@{domain}.com.
	fromHeader	The RFC.5322 Header/HFROM (or "visible") address authorized for use with the SMTP AUTH UID. **Note:** a domain-only value means {wildcard}@{domain}.com.
status	success	The total number of messages that were delivered to mailboxes.
	failure	The total number of messages that weren't delivered to mailboxes due to permanent failures, such as: • SER didn't accept them (for example, an unauthorized fromHeader address was used with an UID). • SER was unable to deliver them (for example, a 5XX error was received from a mailbox provider because a mailbox didn't exist). • SER was unwilling to deliver them (for example, malware was detected).
	tempFailure	The total number of messages that weren't delivered to mailboxes due to temporary 4XX errors received by mailbox providers. **Note:** SER will re-attempt delivery of these messages for up to seven days. Up to (or at) seven days, they'll be reclassified as either failures or successes.
	partialSuccess	The total number of messages that haven't been classified with one of the above (uncommon).
	inProgress	The total number of messages that haven't been classified with one of the above (uncommon).
	total	success + failure + tempFailure + partialSuccess + inProgress.
	recipientsTotal	The total number of recipients in the messages.
	messageSizeTotal	The total size of the messages when they were received by SER (measured in bytes). **Note:** This value is used to calculate actual throughput usage
	deliveredSizeTotal	The total size of the messages when they were sent by SER (measured in bytes).

CATEGORY	TAG	DESCRIPTION
details	2.X.X	The total number of messages for which a DSN 2.X.X was the result.
	3.X.X	The total number of messages for which a DSN 3.X.X was the result.
	4.X.X	The total number of messages for which a DSN 4.X.X was the result.
	5.X.X	The total number of messages for which a DSN 5.X.X was the result.
entitlement	annual_throughput	The amount of throughput (data) you're entitled to use between the license_start and license_end date.
	license_start	The start of the license period.
	license_end	The end of the license period.

Contact Customer Support

Support for the SER API is available at **ser-support@proofpoint.com**.

LEARN MORE
For more information, visit **proofpoint.com**.

proofpoint.