Proofpoint Secure Email Relay-API – Überblick

In diesem Dokument erhalten Sie einen Überblick über die API für Proofpoint Secure Email Relay (SER). Mit Proofpoint SER können Sie für App-E-Mails den gleichen Grad an Sicherheit, Informationsschutz und Compliance gewährleisten wie für Anwender-E-Mails. Gleichzeitig werden diese E-Mail-Typen weiterhin voneinander getrennt. Dadurch verringert sich das Bedrohungsrisiko, da nur autorisierte Versender den Service nutzen dürfen. Bei der SER-API handelt es sich um eine REST-API, mit der Sie Daten mithilfe von Business Intelligence-Tools wie Tableau, Splunk und PowerBI integrieren und automatisieren können.

Angesprochene Zielgruppe

Die Proofpoint SER-API und dieser Leitfaden richten sich an Softwareentwickler, Systemarchitekten und Systemdesigner. Wenn Sie die SER-API verwenden möchten, müssen Sie mit API-Bausteinen wie Remote-Aufrufen, Objektklassen, Variablen, JavaScript und Web-Anwendungsentwicklung vertraut sein, mit denen Sie die Ausgaben von Software-Anwendungen und Business Intelligence-Tools generieren können. Wenn Sie mit diesen Konzepten nicht vertraut sind, beziehen Sie andere Bereiche Ihres Unternehmens, z. B. Ihr IT- oder Softwareentwicklungs-Team, mit ein.

Mit Ausnahme der dedizierten Splunk- und QRadar-Apps, die Anfang 2022 veröffentlicht wurden, ist die SER-API kein vorkonfiguriertes Tool und enthält keine vordefinierten Konnektoren. Die Anleitungen zu diesen Tools enthalten Details dazu, wie Ihr Softwareentwicklungs-Team die SER-API integrieren kann.

Hinweis: Aufgrund der großen Vielfalt an Business Intelligence-Tools ist Ihr technisches Personal für die Programmierung verantwortlich. Proofpoint bietet bei der Integration der SER-API in Ihre Tools keinerlei Unterstützung bei der Programmierung.

Token-Generierung

Zur Gewährleistung sicherer Datenzugriffe setzt die SER-API auf Token-basierte Authentifizierung. Bevor Sie die API verwenden können, müssen Sie ein Zugriffs-Token generieren. Das Token stellt Ihren API-Anwendern und -Anwendungen die Anmeldedaten und Autorisierung zur Verfügung, die für den sicheren Datenzugriff und Anfragen sowie Aktionen erforderlich sind.

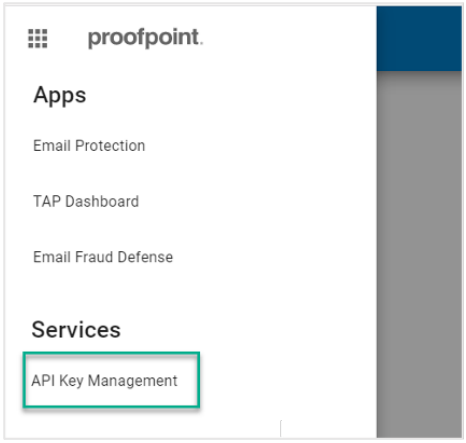
Endpunktverfügbarkeit

ENDPUNKT	VERFÜGBARKEIT	KOMMENTARE
Berichte	Jetzt	Bietet schreibgeschützten Zugriff auf alle E-Mail-Aktivitäten von SER.
Suche	2. Q. 2023	Bietet schreibgeschützten Zugriff auf Erfolg/Fehler-Protokolle für E-Mails, die von SER verarbeitet wurden.
Anwenderverwaltung	2. Q. 2023	Bietet allen Kunden schreibgeschützten und SER Advanced-Kunden Vollzugriff auf SMTP-Authentifizierungsnutzer.

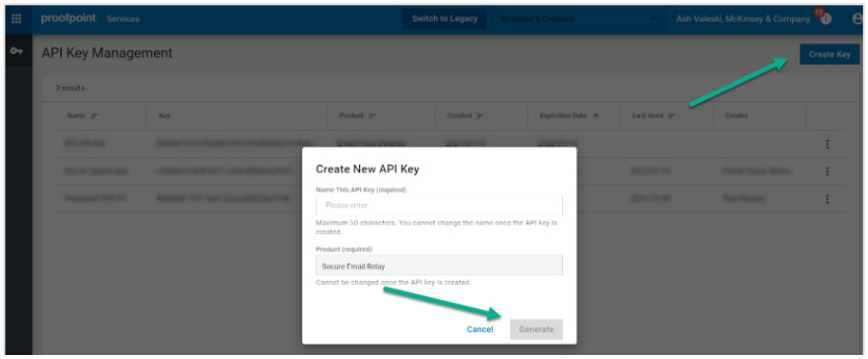
Der Ihrem SER-Konto zugewiesene Administrator muss zuerst ein Kennwort (Secret) und einen Schlüssel (Key) von der Proofpoint-Administrationswebsite abrufen, um ein Token zu generieren.

So rufen Sie Kennwort und Schlüssel ab:

1. Melden Sie sich bei **https://admin.emaildefense.proofpoint.com** an.
2. Klicken Sie oben links auf den **App Switcher** und dann auf **Services** > **API Key Management** (API-Schlüsselverwaltung).



3. Klicken Sie auf **Create Key** (Schlüssel erstellen) und wählen Sie **Secure Email Relay** aus.



Hinweise:

- Wenn „Secure Email Relay“ nicht in der Liste enthalten ist, sind Sie nicht als SER-Administrator angemeldet.
- Das Kennwort und der Schlüssel laufen ein Jahr nach Aktivierung ab.

Sie haben Kennwort und Schlüssel erhalten.

Token-Anfragen

Fordern Sie ein Token vom Token-Endpunkt an: **https://auth.proofpoint.com/v1/token**.

Beispiel-Skript:

```
#!/bin/sh

#

# Abrufen des OAUTH-Tokens für den Trap Handler-Zugriff

#

CLIENT_ID=IhrSchlüssel

CLIENT_SECRET=IhrKennwort

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
```

Hinweis: Das Token läuft nach 43.200 Sekunden (12 Stunden) ab.

Datenabruf

Sie können Reporting-Daten von der SER-API unter **https://ser-api.proofpoint.com** abrufen. Geben Sie dazu das erhaltene Token und einen Datumsbereich an.

Anfragen sind wie folgt formatiert:

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

- Gültige key1-Werte sind: startTimeStamp=2020-06-01T00:00:00.000Z (greaterThanEquals)
- Gültige key2-Werte sind: endTimeStamp=2020-06-01T00:00:00.000Z (lessThan)
- Der Wert für „startTimeStamp“ und „endTimeStamp“ muss im Format „JJJJ-MM-TT’T’HH:mm:ss.SSSZ“ angegeben werden.
- Wenn für „startTimeStamp“ kein Wert angegeben wird, verwendet die API standardmäßig den Beginn der Lizenz („license_start“).
- Wenn für „endTimeStamp“ kein Wert angegeben wird, verwendet die API standardmäßig den aktuellen Zeitpunkt.

Beispiel-Anfrage 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'
```

Beispiel-Anfrage 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'
```

Hinweis: Pro Minute können bis zu 1.000 Anfragen durchgeführt werden.

Datenantwort

Die Antwortdaten können als JSON oder TEXT (uuencode) formatiert und in zwei Inhaltsblöcken organisiert sein:

- **applicationUsers:** Liefert Details zu Aktivitäten, aufgeschlüsselt nach Anwendung
- **entitlement:** Gibt das Datenaufkommen (Durchsatz) und die Lizenzdauer bzw. den Zeitraum zurück, in dem dieses Datenaufkommen aufgetreten ist

Alle Datumsangaben werden in UTC (MEZ +1 Stunde) angegeben.

In der nachfolgenden Tabelle finden Sie eine Beschreibung für jedes Tag-Wert-Paar.

Tag-Wert-Paare

KATEGORIE	TAG	BESCHREIBUNG
applicationUsers	applicationName	Der Anzeigename der Anwendung (entsprechend einer Liste in der globalen Anwendungsdatenbank von SER), welcher der applicationUser zugewiesen bzw. zugeordnet ist.
	applicationUserName	Der Anzeigename des SMTP AUTH-Benutzernamen (nicht zu verwechseln mit der SMTP AUTH UID, die – zusammen mit dem SMTP AUTH-Kennwort – in der Anwendung konfiguriert wurde, die E-Mails an das System sendet).
	fromEnvelope	Die RFC.5321 Envelope/MFROM-Adresse, die für die Verwendung mit SMTP AUTH UID autorisiert wurde. **Hinweis:** Nur-Domain-Wert bedeutet {Platzhalter}@{Domain}.com.
	fromHeader	Die RFC.5322 Header/HFROM-Adresse (oder „sichtbare“ Adresse), die für die Verwendung mit SMTP AUTH UID autorisiert wurde. **Hinweis:** Nur-Domain-Wert bedeutet {Platzhalter}@{Domain}.com.
status	success	Die Gesamtzahl der Nachrichten, die an Postfächer gesendet wurden.
	failure	Die Gesamtzahl der Nachrichten, die aufgrund permanenter Fehler nicht an Postfächer gesendet wurden. Zu diesen Fehlern gehören: • SER hat sie nicht akzeptiert (z. B. wenn eine nicht autorisierte fromHeader-Adresse mit einer UID verwendet wurde). • SER konnte sie nicht zustellen (z. B. wenn ein 5XX-Fehler vom E-Mail-Anbieter zurückgegeben wurde, weil ein Postfach nicht existiert). • SER wollte sie nicht zustellen (z. B. wenn Malware erkannt wurde).
	tempFailure	Die Gesamtzahl der Nachrichten, die aufgrund eines temporären 4XX-Fehlers vom E-Mail-Anbieter nicht an Postfächer gesendet wurden. **Hinweis:** SER versucht über einen Zeitraum von bis zu sieben Tagen immer wieder, diese Nachrichten zuzustellen. Bei erfolgreicher Zustellung werden diese Nachrichten als Erfolg (success) reklassifiziert; andernfalls erfolgt nach sieben Tagen die Reklassifizierung als Fehler (failure).
	partialSuccess	Die Gesamtzahl der Nachrichten, die nicht mit einem der beiden Status-Tags klassifiziert wurden (ungewöhnlich).
	inProgress	Die Gesamtzahl der Nachrichten, die nicht mit einem der beiden Status-Tags klassifiziert wurden (ungewöhnlich).
	total	success + failure + tempFailure + partialSuccess + inProgress.
	recipientsTotal	Die Gesamtzahl der Nachrichtenempfänger.
	messageSizeTotal	Die Gesamtgröße der Nachrichten, wenn sie bei SER eingehen (in Bytes). **Hinweis:** Mit diesem Wert wird das tatsächliche Datenaufkommen berechnet.
	deliveredSizeTotal	Die Gesamtgröße der Nachrichten, wenn sie von SER gesendet werden (in Bytes).

KATEGORIE	TAG	BESCHREIBUNG
details	2.X.X	Die Gesamtzahl der Nachrichten mit dem Ergebnis DSN 2.X.X.
	3.X.X	Die Gesamtzahl der Nachrichten mit dem Ergebnis DSN 3.X.X.
	4.X.X	Die Gesamtzahl der Nachrichten mit dem Ergebnis DSN 4.X.X.
	5.X.X	Die Gesamtzahl der Nachrichten mit dem Ergebnis DSN 5.X.X.
entitlement	annual_throughput	Das Gesamtdatenaufkommen (Durchsatz), das während des Lizenzzeitraums (zwischen license_start und license_end) von Ihrer Lizenz abgedeckt ist.
	license_start	Der Beginn des Lizenzzeitraums.
	license_end	Das Ende des Lizenzzeitraums.

Kunden-Support kontaktieren

Support für die SER-API erhalten Sie unter **ser-support@proofpoint.com**.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **proofpoint.com/de**.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter 75 Prozent der Fortune-100-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.

proofpoint.