Proofpoint Secure Email Relay — Presentazione dell'API

Questo documento presenta l'API associata a Proofpoint Secure Email Relay (SER). Proofpoint SER offre alle email applicative lo stesso livello di sicurezza, protezione delle informazioni e conformità delle email inviate dagli utenti, pur mantenendo le due cose separate. Riduce anche il rischio di minacce limitando l'uso del servizio ai mittenti autorizzati. L'API di SER è una API REST che puoi utilizzare per integrare e automatizzare i dati attraverso strumenti di business intelligence come Tableau, Splunk e PowerBI.

Pubblico di riferimento

L'API Proofpoint SER e questa guida sono rivolte a ingegneri del software, architetti di sistema e progettisti di sistemi. Per utilizzare l'API di SER è necessario conoscere i componenti dell'API, come le chiamate remote, le classi di oggetti, le variabili, JavaScript e lo sviluppo di applicazioni web. Tali componenti permettono di creare applicazioni software e informazioni di business intelligence. Se non hai familiarità con questi concetti, coinvolgi altri collaboratori della tua azienda, come il team IT o di sviluppo software.

Ad eccezione delle applicazioni dedicate Splunk e QRadar, rilasciate all'inizio del 2022, l'API SER non è uno strumento pronto all'uso e non dispone di connettori predefiniti. Pertanto, il gruppo di ingegneria del software deve fare riferimento alle istruzioni fornite da tali strumenti per maggiori dettagli sull'integrazione dell'API SER.

Nota: data l'ampia varietà di strumenti di business intelligence, il tuo personale tecnico deve eseguire tutte le attività di programmazione. Proofpoint non offre alcuna assistenza alla programmazione per l'integrazione dell'API SER con i tuoi strumenti.

Generazione di token

L'API di SER richiede un'autenticazione basata su token per l'accesso ai dati in modo sicuro. Devi generare un token d'accesso prima di utilizzare l'API. Il token fornisce ai tuoi utenti di API e alle applicazioni le credenziali e il livello di autorizzazione necessari per accedere ai dati in modo sicuro, così da eseguire le richieste e le azioni.

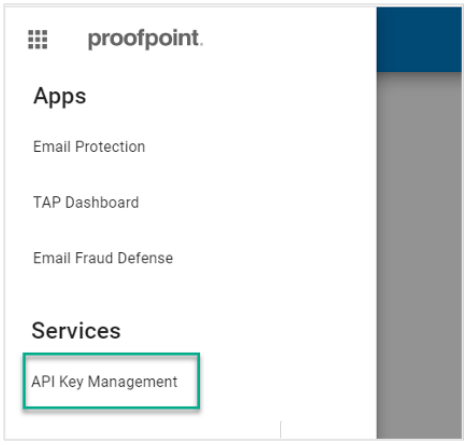
Disponibilità degli endpoint

ENDPOINT	DISPONIBILITÀ	COMMENTI
Report	Ora	Fornisce accesso in lettura a tutte le attività email SER.
Ricerca	Q2 2023	Fornisce accesso in lettura ai log di email recapitate/non recapitate SER.
Gestione degli utenti	Q2 2023	Fornisce accesso in lettura (tutti i clienti) e in scrittura (solo clienti SER Advanced) agli utenti dell'autenticazione SMTP.

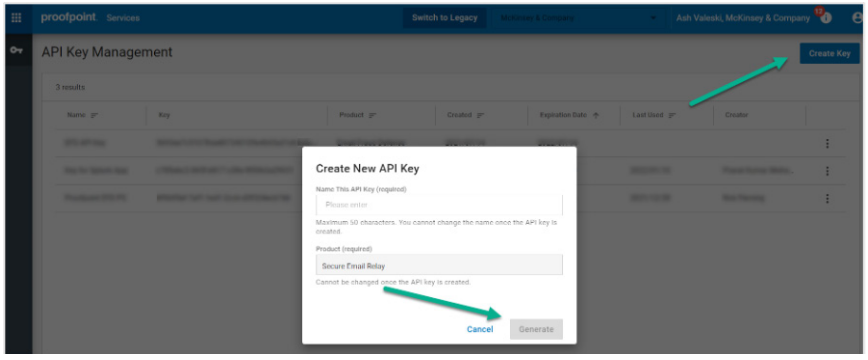
L'utente di amministrazione associato al tuo account SER deve prima acquisire un segreto e una chiave dall'interfaccia di amministrazione Proofpoint per generare un token.

Per ottenere il segreto e la chiave:

1. Collegati all'indirizzo **https://admin.emaildefense.proofpoint.com.**
2. Utilizza **App Switcher** (Commutatore di applicazioni) nell'angolo in alto a sinistra per accedere a **Services** > **API Key Management** (Servizi > Gestione delle chiavi API)**.**



3. Seleziona **Create Key** (Crea una chiave) e quindi **Secure Email Relay**.



Note:

- Se l'opzione "Secure Email Relay" non è nell'elenco, significa che un utente che non è l'amministratore SER è collegato.
- Il segreto e la chiave scadono dopo un anno dall'attivazione.

Hai ottenuto il segreto e la chiave.

Richieste di token

Richiedi un token dall'endpoint dei token: **https://auth.proofpoint.com/v1/token**.

Esempio di script:

```
#!/bin/sh

#

# Ottenere il token OAUTH per accedere alla funzione Trap Handler

#

CLIENT_ID=laChiave

CLIENT_SECRET=ilSegreto

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
```

Nota: i token scadono dopo 43.200 secondi (12 ore).

Recupero dei dati

Puoi recuperare i dati dall'API SER all'indirizzo **https://ser-api.proofpoint.com** fornendo il token ottenuto sopra e un intervallo di date.

Le richieste vengono formattate come segue:

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

- I valori key1 validi sono: startTimeStamp=2020-06-01T00:00:00.000Z (greaterThanEquals)
- I valori key2 validi sono: endTimeStamp=2020-06-01T00:00:00.000Z (lessThan)
- Il formato di startTimeStamp e di endTimeStamp deve essere aaaa-MM-gg'T'HH:mm:ss.SSSZ
- Se il valore di startTimeStamp non viene fornito, l'API utilizza di default license_start.
- Se il valore endTimeStamp non viene fornito, l'API utilizza di default l'ora attuale.

Esempio di richiesta 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'
```

Esempio di richiesta 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'
```

Nota: puoi effettuare fino a 1.000 richieste al minuto.

Risposta

I dati di risposta possono essere in formato JSON o TEXT (uuencode) e organizzati in due blocchi di contenuti:

- **applicationUsers.** Fornisce i dettagli delle attività, suddivisi per applicazione.
- **entitlement.** Fornisce il throughput e la durata della licenza, ovvero il periodo di tempo in cui si applica il throughput.

Tutte le date sono in formato UTC.

La tabella seguente fornisce una descrizione di ogni coppia tag/valore.

Coppie Tag/valore

CATEGORIA	TAG	DESCRIZIONE
applicationUsers	applicationName	Il nome visualizzato dell'applicazione (in un elenco del database mondiale di applicazioni SER) a cui l'utente applicationUser è associato/mappato.
	applicationUserName	Il nome utente visualizzato SMTP AUTH (da non confondere con l'ID utente o UID SMTP AUTH che, insieme alla password SMTP AUTH, è configurato nell'applicazione che invia l'email al sistema).
	fromEnvelope	L'indirizzo Envelope/MFROM corrispondente a RFC 5321, il cui utilizzo è autorizzato con l'UID SMTP AUTH. **Nota:** un valore di solo dominio corrisponde a {carattere_generico}@{dominio}.com.
	fromHeader	L'indirizzo Header/MFROM corrispondente a RFC 5323, il cui utilizzo è autorizzato con l'UID SMTP AUTH. **Nota:** un valore di solo dominio corrisponde a {carattere_generico}@{dominio}.com.
status	success	Il numero totale di messaggi consegnati alle caselle email.
	failure	Il numero totale di messaggi non recapitati alle caselle email a causa di errori permanenti, come nei casi seguenti: • SER non li ha accettati (ad esempio, un indirizzo fromHeader non autorizzato è stato utilizzato con un UID). • SER non è stato in grado di recapitarli (ad esempio, è stato ricevuto un messaggio di errore 5XX da un provider email perché la casella email non esisteva). • SER si è rifiutato di recapitarli (ad esempio, è stato rilevato un malware).
	tempFailure	Il numero totale di messaggi non recapitati alle caselle email a causa di errori 4XX temporanei ricevuti dai provider email. **Nota:** SER tenterà nuovamente il recapito di questi messaggi per un massimo di sette giorni. Dopo questo periodo di sette giorni, saranno riclassificati come "success" (recapitato) e "failure" (non recapitato).
	partialSuccess	Il numero totale di messaggi che non sono stati classificati secondo una delle categorie menzionate (non comune).
	inProgress	Il numero totale di messaggi che non sono stati classificati secondo una delle categorie menzionate (non comune).
	total	success + failure + tempFailure + partialSuccess + inProgress.
	recipientsTotal	Il numero totale di destinatari nei messaggi.
	messageSizeTotal	La dimensione totale dei messaggi che sono stati ricevuti da SER (in byte). **Nota:** questo valore serve per calcolare l'utilizzo del throughput reale.
	deliveredSizeTotal	La dimensione totale dei messaggi inviati da SER (in byte).

CATEGORIA	TAG	DESCRIZIONE
details	2.X.X	Il numero complessivo di messaggi per i quali il risultato è stato un DSN 2.X.X.
	3.X.X	Il numero complessivo di messaggi per i quali il risultato è stato un DSN 3.X.X.
	4.X.X	Il numero complessivo di messaggi per i quali il risultato è stato un DSN 4.X.X.
	5.X.X	Il numero complessivo di messaggi per i quali il risultato è stato un DSN 5.X.X.
entitlement.	annual_throughput	Il volume di dati (throughput) che puoi utilizzare tra le date license_start e license_end.
	license_start	L'inizio del periodo della licenza.
	license_end	La fine del periodo della licenza.

Per contattare l'assistenza clienti

L'assistenza per l'API di SER è disponibile all'indirizzo **ser-support@proofpoint.com**.

PER SAPERNE DI PIÙ

Per maggiori informazioni visita il sito **proofpoint.com/it**.

INFORMAZIONI SU PROOFPOINT

Proofpoint è un'azienda leader nella cybersecurity e nella conformità, che protegge dai rischi il patrimonio più importante di un'azienda: le persone. Con una suite integrata di soluzioni basate su cloud, Proofpoint aiuta le aziende di tutto il mondo a bloccare le minacce mirate, a salvaguardare i propri dati e a proteggere gli utenti dagli attacchi IT. Aziende di ogni dimensione, tra cui il 75% delle Fortune 100, si affidano alle soluzioni di sicurezza e di conformità incentrate sulle persone di Proofpoint per mitigare i rischi di sicurezza veicolati via email, cloud, social media e web. Per ulteriori informazioni: **www.proofpoint.com/it**.