Proofpoint Secure Email Relay — Visão geral da API

Este documento oferece uma visão geral da API do Proofpoint Secure Email Relay (SER). O Proofpoint SER proporciona uma maneira dos e-mails de aplicativo terem o mesmo nível de segurança, proteção de informações e conformidade que os e-mails baseados em usuário e, ao mesmo tempo, mantê-los separados. Ele também reduz o risco de ameaça permitindo que apenas remetentes credenciados utilizem o serviço. O SER tem uma API REST que você pode utilizar para integrar e automatizar dados por meio de ferramentas de inteligência empresarial (BI), como Tableau, Splunk e PowerBI.

Público-alvo

Tanto a API do Proofpoint SER quanto este guia são indicados para engenheiros de software, arquitetos de sistemas e designers de sistemas. Para utilizar a API do SER, você precisa estar familiarizado com os blocos constituintes de uma API, como chamadas remotas, classes de objetos, variáveis, JavaScript e desenvolvimento de aplicativos Web. Você pode criar aplicativos de software e gerar saídas de inteligência empresarial (BI) utilizando esses blocos constituintes. Se você não está familiarizado com os conceitos, envolva outras pessoas da sua organização, como a sua equipe de TI ou de desenvolvimento de software.

Com exceção dos aplicativos dedicados Splunk e QRadar, lançados no início de 2022, a API do SER não é uma ferramenta pronta e não tem conectores predefinidos. Portanto, o seu grupo de engenharia de software precisa consultar as instruções fornecidas por essas ferramentas para obter detalhes sobre como integrar a API do SER.

Nota: devido à grande variedade de ferramentas de BI existentes, o seu pessoal técnico precisa se encarregar de toda a programação. A Proofpoint não oferece assistência alguma de programação para integrar a API do SER com as suas ferramentas.

Geração de tokens

A API do SER exige autenticação baseada em token para proteger o acesso aos dados. Você precisa gerar um token de acesso antes de utilizar a API. O token proporciona aos usuários e aplicativos da API as credenciais e a autorização necessárias para acessar os dados com segurança, para que você possa realizar solicitações e ações.

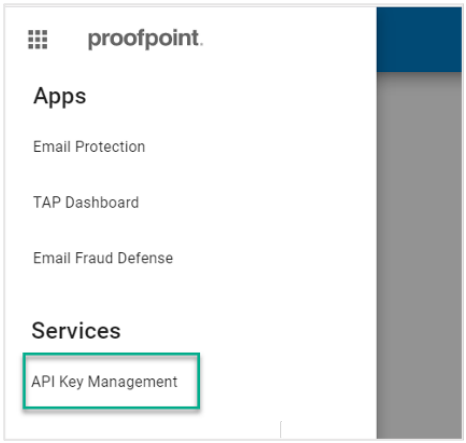
Disponibilidade de endpoints

ENDPOINT	DISPONIBILIDADE	COMENTÁRIOS
Geração de relatórios	Já disponível	Oferece acesso somente de leitura a todas as atividades de e-mail do SER.
Pesquisa	T2 2023	Oferece acesso somente de leitura a logs de sucesso/falha de e-mails do SER.
Gerenciamento de usuários	T2 2023	Oferece acesso de leitura (para todos os clientes) / gravação (somente para clientes do SER Advanced) a usuários com autenticação SMTP.

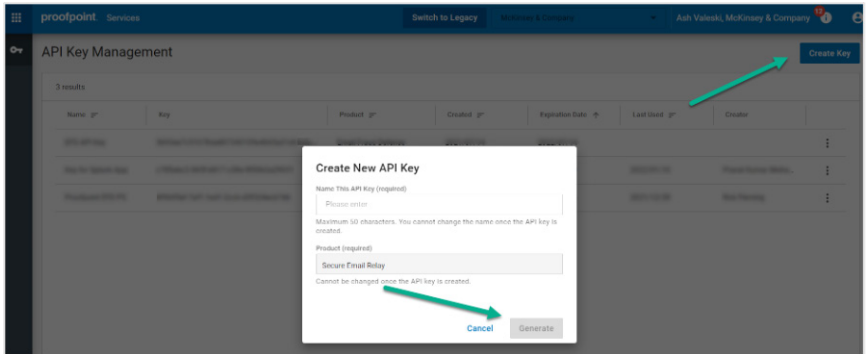
O usuário administrativo associado à conta do SER precisa primeiro obter um “segredo” e uma “chave” da interface de administração da Proofpoint para gerar um token.

Para gerar o segredo e a chave:

1. Efetue login em **https://admin.emaildefense.proofpoint.com.**
2. Use o **App Switcher** (Seletor de aplicativos) do canto superior esquerdo e vá para **Services** (Serviços) > **API Key Management** (Gerenciamento de chaves da API).



3. Selecione **Create Key** (Criar chave) e, em seguida, **Secure Email Relay**.



Notas:

- Se “Secure Email Relay” não aparecer, isso significa que alguém mais, que não o usuário administrador do SER, está conectado.
- O segredo e a chave expiram um ano após a ativação.

Você obteve o segredo e a chave.

Solicitações de token

Solicite um token do endpoint de tokens: **https://auth.proofpoint.com/v1/token**.

Exemplo de script:

```
#!/bin/sh

#

# Obtém token OAUTH para acessar o Trap Handler

#

CLIENT_ID=suaChave

CLIENT_SECRET=seuSegredo

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: os tokens expiram após 43.200 segundos (12 horas).

Recuperação de dados

Você pode recuperar dados de relatório da API do SER em **https://ser-api.proofpoint.com** fornecendo o token obtido acima, juntamente com um intervalo de datas.

O formato das solicitações é o seguinte:

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

- Os valores válidos de key1 são: startTimeStamp=2020-06-01T00:00:00.000Z (greaterThanEquals)
- Os valores válidos de key2 são: endTimeStamp=2020-06-01T00:00:00.000Z (lessThan)
- O formato de startTimeStamp e endTimeStamp deve ser aaaa-MM-dd'T'HH:mm:ss.SSSZ
- Se startTimeStamp não for informado, a API utilizará como padrão license_start.
- Se endTimeStamp não for informado, a API utilizará como padrão a hora atual.

Exemplo de solicitação 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'
```

Exemplo de solicitação 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: é possível fazer até 1.000 solicitações por minuto.

Resposta de dados

Os dados da resposta podem ser formatados como JSON ou TEXT (uuencode) e organizados em dois blocos de conteúdo:

- **applicationUsers.** Fornece detalhes da atividade, categorizados por aplicativo
- **entitlement.** Informa a capacidade de saída e o prazo da licença, ou seja, o período durante o qual a capacidade se aplica.

Todas as datas são UTC.

A tabela abaixo contém uma descrição de cada par tag/valor.

Pares tag/valor

CATEGORIA	TAG	DESCRIÇÃO
applicationUsers	applicationName	O nome de exibição do aplicativo (em uma lista no banco de dados global de aplicativos do SER) ao qual applicationUser está associado/mapeado.
	applicationUserName	O nome de exibição de usuário SMTP AUTH (não confundir com SMTP AUTH UID que, juntamente com a senha SMTP AUTH, é configurado no aplicativo que está enviando o e-mail ao sistema).
	fromEnvelope	Endereço RFC.5321 Envelope/MFROM autorizado para uso com SMTP AUTH UID. **Nota:** um valor só com domínio significa {curinga}@{domínio}.com.
	fromHeader	Endereço RFC.5322 Header/HFROM (ou “vísivel”) autorizado para uso com SMTP AUTH UID. **Nota:** um valor só com domínio significa {curinga}@{domínio}.com.
status	success	O número total de mensagens que foram entregues em caixas de correio.
	failure	O número total de mensagens que não foram entregues em caixas de correio devido a falhas permanentes, como: • O SER não as aceitou (por exemplo, um endereço fromHeader não autorizado foi utilizado com um UID). • O SER não pôde entregá-las (por exemplo, um erro 5XX foi recebido de um provedor de caixa de correio porque a caixa de correio não existia). • O SER não quis enviá-las (por exemplo, devido a uma detecção de malware).
	tempFailure	O número total de mensagens que não foram entregues em caixas de correio devido a erros temporários 4XX recebidos por provedores de caixa de correio. **Nota:** o SER fará novas tentativas de entrega dessas mensagens durante até sete dias. Após sete dias, elas serão reclassificadas como falhas (failure) ou sucessos (success).
	partialSuccess	O número total de mensagens que não foram classificadas em uma das categorias acima (incomum).
	inProgress	O número total de mensagens que não foram classificadas em uma das categorias acima (incomum).
	total	success + failure + tempFailure + partialSuccess + inProgress.
	recipientsTotal	O número total de destinatários das mensagens.
	messageSizeTotal	O tamanho total das mensagens quando estas foram recebidas pelo SER (medido em bytes). **Nota:** esse valor é utilizado para calcular o uso real da capacidade.
	deliveredSizeTotal	O tamanho total das mensagens quando estas foram enviadas pelo SER (medido em bytes).

CATEGORIA	TAG	DESCRIÇÃO
details	2.X.X	O número total de mensagens para as quais o resultado foi DSN 2.X.X.
	3.X.X	O número total de mensagens para as quais o resultado foi DSN 3.X.X.
	4.X.X	O número total de mensagens para as quais o resultado foi DSN 4.X.X.
	5.X.X	O número total de mensagens para as quais o resultado foi DSN 5.X.X.
entitlement	annual_throughput	A quantidade de capacidade (dados) que você tem direito de utilizar entre as datas license_start e license_end.
	license_start	O início do período da licença.
	license_end	O término do período da licença.

Entre em contato com o atendimento ao cliente

O suporte da API do SER está disponível em **ser-support@proofpoint.com**.

SAIBA MAIS

Para obter mais informações, visite **proofpoint.com/br**.

SOBRE A PROOFPOINT

A Proofpoint, Inc. é uma empresa líder em cibersegurança que protege as organizações em seus maiores riscos e seus ativos mais valiosos: sua equipe. Com um pacote integrado de soluções baseadas em nuvem, a Proofpoint ajuda empresas do mundo todo a deter ameaças direcionadas, proteger seus dados e tornar seus usuários mais resilientes contra ataques cibernéticos. Organizações líderes de todos os portes, incluindo 75% das empresas da Fortune 100, contam com a Proofpoint para obter soluções de segurança e conformidade centradas nas pessoas e que minimizem seus riscos mais críticos em e-mail, nuvem, redes sociais e Web. Mais informações estão disponíveis em **www.proofpoint.com/br**.