

# Proofpoint Secure Email Relay — Présentation de l'API

Ce document présente l'API associée à Proofpoint Secure Email Relay (SER). Proofpoint SER permet de conférer aux emails émanant des applications le même niveau de sécurité, de protection des informations et de conformité qu'aux emails générés par des utilisateurs, tout en les maintenant séparés. Il réduit le risque de menaces en limitant l'utilisation du service aux seuls expéditeurs disposant d'identifiants de connexion. L'API Proofpoint SER est une API REST qui permet d'intégrer et d'automatiser des données via des outils de veille stratégique tels que Tableau, Splunk et PowerBI.

## Public cible

L'API Proofpoint SER et ce guide sont destinés aux ingénieurs logiciels, aux architectes système et aux concepteurs système. Pour utiliser l'API Proofpoint SER, vous devez maîtriser les éléments de base d'une API tels que les appels distants, les classes d'objet, les variables, JavaScript et le développement d'applications Web. Ces éléments permettent de créer des applications logicielles et des outils de veille stratégique. Si ces concepts ne vous sont pas familiers, faites appel à d'autres collaborateurs de votre entreprise, tels que les membres de votre équipe informatique ou des développeurs logiciels.

Hormis pour les applications Splunk et QRadar dédiées lancées début 2022, l'API Proofpoint SER n'est pas un outil prêt à l'emploi et ne possède pas de connecteurs prédéfinis. Dès lors, votre équipe d'ingénierie logicielle doit se référer aux instructions fournies par ces outils pour obtenir des informations détaillées sur l'intégration de l'API Proofpoint SER.

**Remarque :** en raison de la grande variété d'outils de veille stratégique, votre personnel technique devra réaliser toutes les tâches de programmation. Proofpoint ne propose aucune assistance à la programmation pour l'intégration de l'API Proofpoint SER avec vos outils.

## Génération de jetons

Pour garantir un accès sécurisé aux données, l'API Proofpoint SER exige une authentification par jeton. Vous devez générer ce jeton d'accès avant d'utiliser l'API. Le jeton procure aux utilisateurs de l'API et aux applications les identifiants de connexion et le niveau d'autorisation nécessaires pour accéder aux données en toute sécurité, afin que vous puissiez exécuter des demandes et des actions.

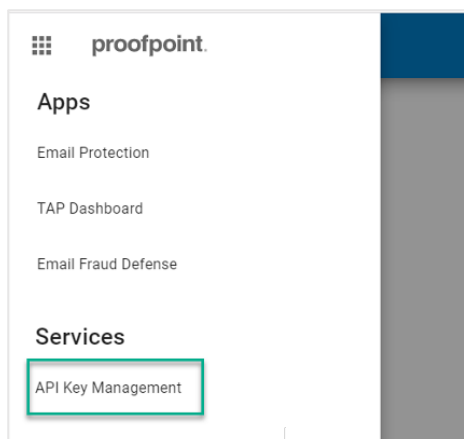
## Disponibilité des endpoints

ENDPOINT	DISPONIBILITÉ	COMMENTAIRES
Rapports	Actuellement	Fournit un accès en lecture à toute l'activité email de Proofpoint SER.
Recherche	T2 2023	Fournit un accès en lecture aux journaux de réussite/échec de distribution des emails de Proofpoint SER.
Gestion des utilisateurs	T2 2023	Fournit un accès en lecture (tous les clients) et un accès en écriture (clients Proofpoint SER Advanced uniquement) aux utilisateurs de l'authentification SMTP.

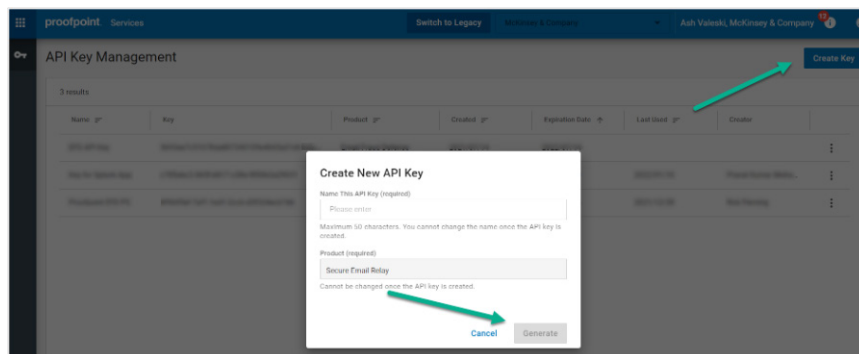
Pour générer un jeton, l'utilisateur administrateur associé à votre compte SER doit au préalable obtenir un secret et une clé auprès de l'interface d'administration Proofpoint.

Pour obtenir ce secret et cette clé :

1. Connectez-vous au site <https://admin.emaildefense.proofpoint.com>.
2. Utilisez **App Switcher** (Basculement d'applications) dans le coin supérieur gauche pour accéder à **Services > API Key Management** (Services > Gestion des clés d'API).



3. Sélectionnez **Create Key** (Créer une clé), puis **Secure Email Relay**.



### Remarques :

- Si « Secure Email Relay » ne figure pas dans la liste, cela signifie qu'un utilisateur autre que l'administrateur SER est connecté.
- Le secret et la clé expirent un an après l'activation.

Vous êtes désormais en possession du secret et de la clé.

## Demandes de jeton

Demandez un jeton à partir de l'endpoint du jeton : <https://auth.proofpoint.com/v1/token>.

### Exemple de script :

```
#!/bin/sh

#
# Procurez-vous le jeton OAUTH pour accéder à Trap Handler
#
CLIENT_ID=votreClé
CLIENT_SECRET=votreSecret
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
```

**Remarque :** les jetons expirent après 43 200 secondes (12 heures).

## Récupération de données

Vous pouvez récupérer des données de l'API Proofpoint SER à l'adresse <https://ser-api.proofpoint.com> en fournissant le jeton obtenu ci-dessus et en spécifiant une plage de dates.

Les requêtes sont formatées comme suit :

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

- Les valeurs key1 valides sont : startTimeStamp=2020-06-01T00:00:00.000Z (greaterThanEquals)
- Les valeurs key2 valides sont : endTimeStamp=2020-06-01T00:00:00.000Z (lessThan)
- Le format de startTimeStamp et de endTimeStamp doit être aaaa-MM-jj'T'HH:mm:ss.SSSZ
- Si la valeur de startTimeStamp n'est pas fournie, l'API utilise par défaut license\_start.
- Si la valeur de endTimeStamp n'est pas fournie, l'API utilise par défaut l'heure actuelle.

### Exemple de requête 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'
```

### Exemple de requête 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'
```

**Remarque :** vous pouvez effectuer jusqu'à 1 000 requêtes par minute.

## Réponse

Les données de réponse peuvent être au format JSON ou TEXT (uencode) et organisées selon deux blocs de contenu :

- **applicationUsers.** Fournit les détails des activités, ventilés par application.
- **entitlement.** Fournit le débit et la période de licence, ou la durée pendant laquelle le débit est d'application.

Toutes les dates sont au format UTC.

Le tableau ci-dessous propose une description de chaque paire balise/valeur.

### Paires balise/valeur

CATÉGORIE	BALISE	DESCRIPTION
applicationUsers	applicationName	Nom d'affichage de l'application (dans une liste dans la base de données mondiale d'applications SER) à laquelle l'utilisateur applicationUser est associé ou mappé.
	applicationUserName	Nom d'affichage de l'utilisateur SMTP AUTH. (À ne pas confondre avec l'ID utilisateur ou UID SMTP AUTH qui, avec le mot de passe SMTP AUTH, est configuré dans l'application qui envoie l'email au système.)
	fromEnvelope	Adresse Envelope/MFROM correspondant à la RFC 5321, dont l'utilisation avec l'UID SMTP AUTH est autorisée.  <b>Remarque :</b> une valeur de domaine seul correspond à {caractère_générique}@{domaine}.com.
	fromHeader	Adresse Header/HFROM (ou « visible ») correspondant à la RFC 5322, dont l'utilisation avec l'UID SMTP AUTH est autorisée.  <b>Remarque :</b> une valeur de domaine seul correspond à {caractère_générique}@{domaine}.com.
status	success	Nombre total de messages distribués dans des boîtes email.
	failure	Nombre total de messages non distribués dans des boîtes email en raison d'échecs permanents, comme dans les cas suivants : <ul style="list-style-type: none"> <li>• Proofpoint SER ne les a pas acceptés (par exemple, une adresse fromHeader non autorisée a été utilisée avec un UID).</li> <li>• Proofpoint SER n'a pas pu les livrer (par exemple, un message d'erreur 5XX a été reçu de la part d'un fournisseur de messagerie parce que la boîte email n'existait pas.)</li> <li>• Proofpoint SER n'a pas voulu les livrer (par exemple, un malware a été détecté.)</li> </ul>
	tempFailure	Nombre total de messages qui n'ont pas été distribués dans des boîtes email en raison d'erreurs 4XX temporaires reçues par des fournisseurs de messagerie.  <b>Remarque :</b> Proofpoint SER tente de distribuer ces messages pendant sept jours au maximum. Passé ce délai, ces messages sont reclassifiés en success (réussite) ou failure (échec).
	partialSuccess	Nombre total de messages qui n'ont pas été classifiés dans l'une des catégories susmentionnées (peu courant).
	inProgress	Nombre total de messages qui n'ont pas été classifiés dans l'une des catégories susmentionnées (peu courant).
	total	success + failure + tempFailure + partialSuccess + inProgress.
	recipientsTotal	Nombre total de destinataires dans les messages.
messageSizeTotal	Taille totale des messages qui ont été reçus par Proofpoint SER (en octets).  <b>Remarque :</b> cette valeur sert à calculer l'utilisation réelle du débit.	
deliveredSizeTotal	Taille totale des messages qui ont été envoyés par Proofpoint SER (en octets).	

CATÉGORIE	BALISE	DESCRIPTION
details	2.X.X	Nombre total de messages pour lesquels le résultat était un DSN 2.X.X.
	3.X.X	Nombre total de messages pour lesquels le résultat était un DSN 3.X.X.
	4.X.X	Nombre total de messages pour lesquels le résultat était un DSN 4.X.X.
	5.X.X	Nombre total de messages pour lesquels le résultat était un DSN 5.X.X.
entitlement	annual_throughput	Volume de données (débit) que vous pouvez utiliser entre les dates license_start et license_end.
	license_start	Début de la période de licence.
	license_end	Fin de la période de licence.

## Contactez le support client

Un support pour l'API Proofpoint SER est disponible à l'adresse [ser-support@proofpoint.com](mailto:ser-support@proofpoint.com).

### EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : [proofpoint.com/fr](https://www.proofpoint.com/fr).

#### À PROPOS DE PROOFPOINT

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris 75 % des entreprises de l'index Fortune 100, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur [www.proofpoint.com/fr](https://www.proofpoint.com/fr).

©Proofpoint, Inc. Proofpoint est une marque commerciale de Proofpoint, Inc. aux États-Unis et dans d'autres pays. Toutes les autres marques citées dans ce document sont la propriété de leurs détenteurs respectifs.