Présentation de l'API Secure Endpoints

Table des matières

[Problème](#)

[Résolution](#)

[Environnement](#)

[Exemple de répartition des commandes API](#)

[Autres informations utiles](#)

Problème

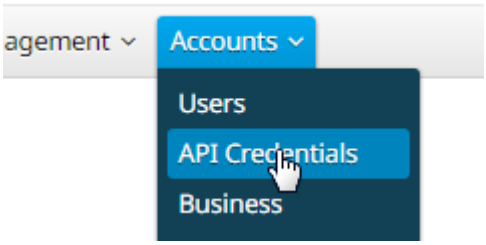
Ce document décrit l'utilisation de l'API Cisco Secure Endpoints (SE).

Résolution

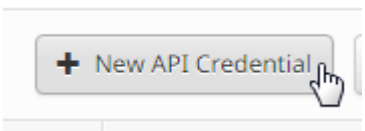
Pour utiliser l'API SE, créez des informations d'identification d'API dans la console SE.

Les exemples de cet article utilisent un point de terminaison Windows 7.

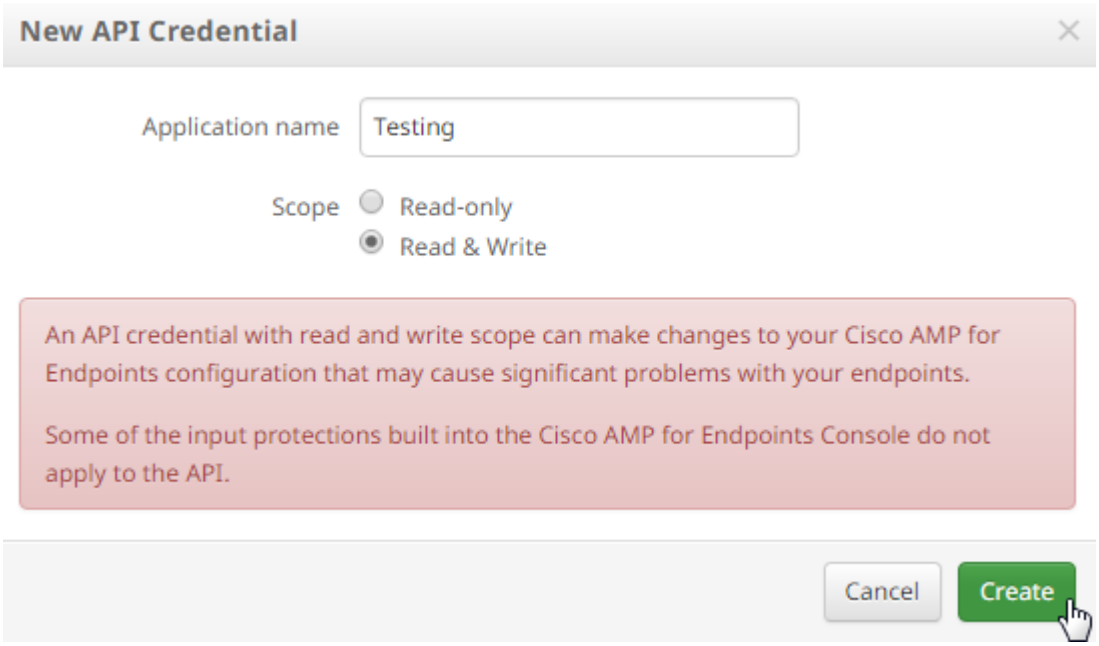
1. Connectez-vous à la console et accédez à Comptes > Informations d'identification de l'API.



1. Cliquez sur New API Credential pour créer un nouvel ensemble de clés.

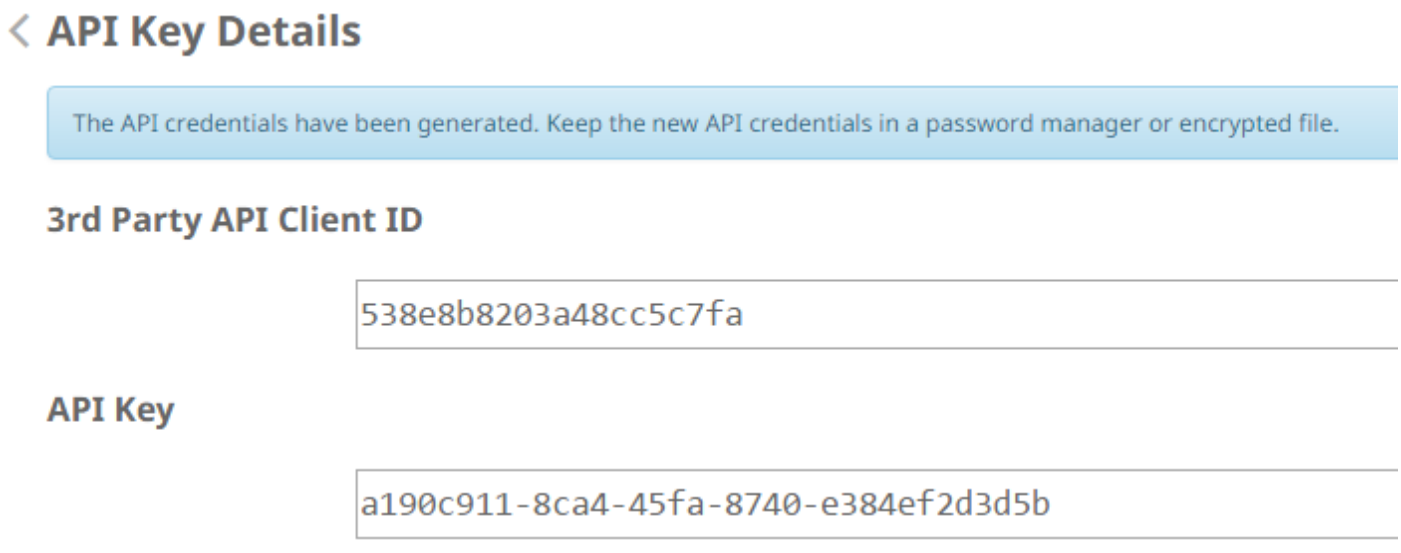


2. Entrez un nom d'application. Sélectionnez l'étendue de Lecture seule ou Lecture et écriture.



Remarque : Les informations d'identification d'API en lecture et en écriture peuvent apporter des modifications à votre configuration Cisco SE, ce qui peut entraîner des problèmes importants au niveau de vos terminaux. Certaines des protections d'entrée intégrées à la console Cisco SE ne s'appliquent pas à l'API.

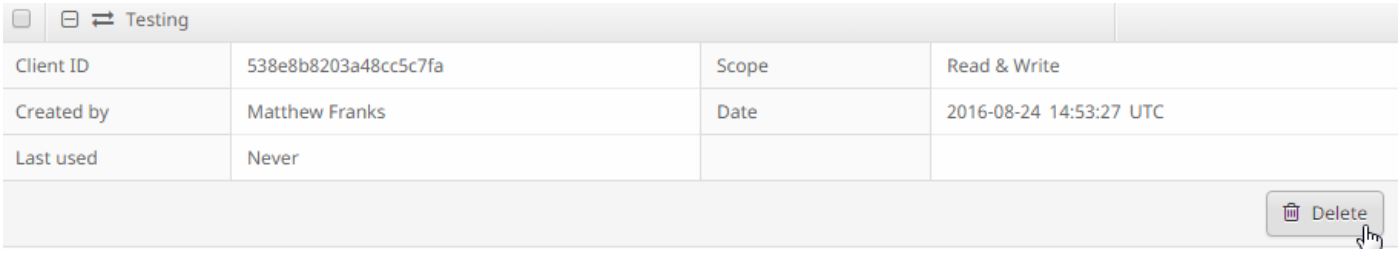
3. Cliquez sur le bouton Créer. La page API Key Details s'affiche. Enregistrez ces informations car certaines ne sont plus disponibles après avoir quitté l'écran.



Remarque : Les identifiants API (ID client API et clé API) permettent à d'autres programmes de récupérer et de modifier vos données Cisco SE. Il est fonctionnellement équivalent à un nom d'utilisateur et à un mot de passe et doit être traité comme tel.

⚠ Mise en garde : Vos informations d'identification API sont affichées une seule fois. Si vous perdez les informations d'identification, vous devez en générer de nouvelles.

Supprimez les informations d'identification API d'une application si vous pensez qu'elles ont été compromises, puis créez-en une nouvelle. Lorsque vous supprimez des informations d'identification d'API, le client qui utilise les anciennes est verrouillé. Vous devez donc les mettre à jour avec les nouvelles informations d'identification.



Environnement

- Terminal testé : Terminal Windows 7.
- Produit : Cisco SE
- Accès : Accès à la console avec autorisation de créer et supprimer des informations d'identification API.
- API : SE API version 3, version 1 et version 0 (exemples utilisant la version 1).
- Outil client : curl installé sur le système utilisé pour exécuter les requêtes API.

Il existe actuellement trois versions de l'API SE : Version 3 , version 1 et version 0. La version 3 offre des fonctionnalités supplémentaires par rapport aux versions 1 et 0. La documentation de l'API de version 3 est disponible sur ce lien. Utilisez la version 3 pour récupérer ces informations :

- Journaux d'audit
- Contrôle des périphériques
- Périphériques
- Exclusions
- Pare-feu hôte
- CIO
- MSSP
- Organisations
- Politiques
- Ordinateurs
- Vulnérabilités

Cliquez sur la commande appropriée dans le document pour voir des exemples de son utilisation.

Exemple de répartition des commandes API

Chaque commande API contient des informations similaires et se décompose en une commande curl comme ceci :

```
curl -o yourfilename.json https://client_id:api_key@api.example.com/v1/whatyouwanttodo
```

Lorsque vous utilisez la commande curl avec l'option -o, elle vous permet d'enregistrer la sortie dans un fichier. Dans ce cas, le nom du fichier est « votrenom_fichier.json ».

Conseil : Pour plus d'informations sur les fichiers .json, consultez le site Web de JSON.

La partie suivante de la commande curl spécifie les informations d'identification avant le symbole @. Après avoir généré les informations d'identification API, utilisez l'ID client API et la clé API dans cette partie de l'URL.

```
https://client_id:api_key@
```

Ajoutez le numéro de version et l'action à effectuer. Pour cet exemple, exécutez GET /v1/computers. La commande complète ressemble à ceci :

```
curl -o computers.json https://client_id:api_key@api.example.com/v1/computers
```

Après avoir exécuté la commande, un fichier computers.json apparaît dans le répertoire où vous avez lancé la commande.

```
C:\Users\mafranks>curl -o computers.json https://538e8b8203a48cc5c7fa:a190c911-8
ca4-45fa-8740-e384ef2d3d5b@api.amp.sourcefire.com/v1/computers
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:--  0:00:02 --:--:--     0
```

```
C:\Users\mafranks>dir | findstr computers
09/06/2016  02:37 PM               128 computers.json
```

Remarque : Curl est disponible en ligne et compilé pour de nombreuses plates-formes, y compris Windows (généralement, vous voulez utiliser la version Win32 - Générique).

Lorsque vous ouvrez le fichier, toutes les données apparaissent sur une seule ligne. Pour l'afficher dans une mise en page formatée, installez un plug-in de navigateur qui formate JSON et ouvrez le fichier dans un navigateur. Cette sortie affiche des informations pour vos ordinateurs, telles que :

connector_guid, hostname, active, links, connector_version, operating_system, internal_ips, external_ip, group_guid, network_addresses, policy guid et policy name.

<#root>

```
{
version: "v1.0.0",
metadata: {
links: {
self: "https://api.amp.cisco.com/v1/computers"
},
results: {
total: 4,
current_item_count: 4,
index: 0,
items_per_page: 500
}
},
data: [
{
```

connector_guid

```
: "abcdef-1234-5678-9abc-def123456789",
```

hostname

```
: "host.example.com",
```

active

```
: true,
```

links

```
: {
computer: "https://api.amp.cisco.com/v1/computers/abcdef-1234-5678-9abc-def123456789",
trajectory: "https://api.amp.cisco.com/v1/computers/abcdef-1234-5678-9abc-def123456789/trajectory",
group: "https://api.amp.cisco.com/v1/groups/abcdef-1234-5678-9abc-def123456789"
},
```

connector_version

```
: "4.4.2.10200",
```

operating_system

: "Windows 7, SP 1.0",

internal_ips

: [
"10.1.1.2",
" 192.168.1.2",
" 192.168.2.2",
" 169.254.245.1"
],

external_ip

: "192.0.2.10",

group_guid

: "abcdef-1234-5678-9abc-def123456789",

network_addresses

: [
{
mac: "ab:cd:ef:01:23:45",
ip: "10.1.1.2"
},
{
mac: "bc:de:f0:12:34:56",
ip: "192.168.1.2"
},
{
mac: "cd:ef:01:23:45:67",
ip: "192.168.2.2"
},
{
mac: "de:f0:12:34:56:78",
ip: "169.254.245.1"
}
],
policy: {

guid

: "abcdef-1234-5678-9abc-def123456789",

name

: "Protect Policy"
}
}
]
}

Cet exemple montre une demande d'API de base. Vous pouvez maintenant utiliser d'autres options de commande pour récupérer et modifier des données dans votre environnement.

Autres informations utiles

- Documentation de l'API Cisco AMP for Endpoints
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.