

Aperçu de l'AMP de Cisco pour les points finaux API

Contenu

[Introduction](#)

[Générez et supprimez les qualifications API](#)

[Versions API et options en cours](#)

[Panne et exemple de commande API](#)

[Informations connexes](#)

Introduction

Ce document décrit au sujet de la protection de malware avancée par Cisco (AMP) pour des points finaux. L'AMP de Cisco pour des points finaux est livré avec une interface de programmation (API). Il te permet pour tirer des données d'un AMP pour le déploiement de points finaux, et les manipule, si nécessaire.

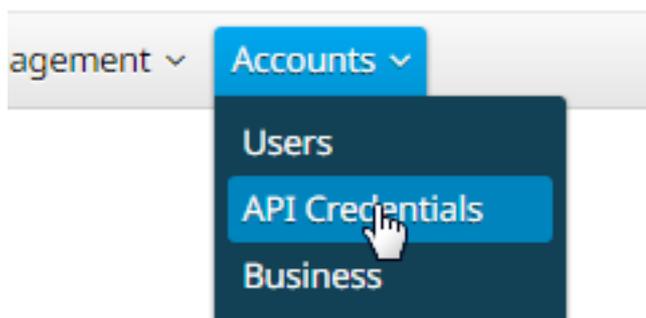
Cet article explique quelques fonctionnalités de base de l'API. Les exemples sur cet article utilise un point final de Windows 7.

Contribué par des contreseings de Matthew, Nazmul Rajib, et des ingénieurs TAC Cisco.

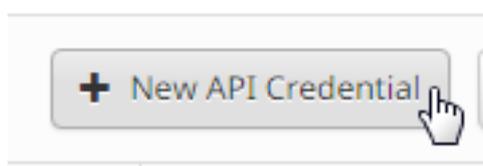
Générez et supprimez les qualifications API

Afin d'utiliser l'AMP pour le point final API, vous devez installer un laisser-passer API. Suivez les étapes données pour créer un laisser-passer par la console d'AMP.

Étape 1 : Connectez-vous dans la console, et naviguez vers des **comptes > des qualifications API**.



Étape 2 : Cliquez sur New le **laisser-passer API** pour créer un nouvel ensemble de clés.



Étape 3 : Fournissez un **nom d'application**. Sélectionnez la **portée** d'en lecture seule ou lisez et écrivez.

New API Credential ✕

Application name

Scope Read-only
 Read & Write

An API credential with read and write scope can make changes to your Cisco AMP for Endpoints configuration that may cause significant problems with your endpoints.

Some of the input protections built into the Cisco AMP for Endpoints Console do not apply to the API.

Note: Un laisser-passer API avec lu et écrivent la portée peut apporter des modifications à votre Cisco l'AMP pour la configuration de points finaux qui pourrait poser des problèmes importants avec vos points finaux. Certaines des protections d'entrée établies dans l'AMP de Cisco pour la console de points finaux ne s'appliquent pas à l'API.

Étape 4 : Cliquez sur le bouton de **création**. **Les détails de clé API** apparaît. Sauvegardez ces informations car une partie de elle ne sera pas disponible après avoir laissé l'écran.

< API Key Details

The API credentials have been generated. Keep the new API credentials in a password manager or encrypted file.

3rd Party API Client ID

538e8b8203a48cc5c7fa

API Key

a190c911-8ca4-45fa-8740-e384ef2d3d5b

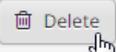
Note: Les qualifications API (clé d'ID et API d'api client) permettront à d'autres programmes pour récupérer et modifier votre AMP de Cisco pour des données de points finaux. Il est fonctionnellement équivalent à un nom d'utilisateur et mot de passe, et devrait être traité en

soi.

Attention : Vos qualifications API sont affichées une fois seulement. Si vous perdez les qualifications, vous devez générer des neufs.

Supprimez les qualifications API pour une application si vous suspectez qu'ils aient été compromis, et créez un neuf. Quand vous supprimez un laissez-passer API, il verrouille le client qui utilise les vieux, les met à jour ainsi avec les nouvelles qualifications.

Testing			
Client ID	538e8b8203a48cc5c7fa	Scope	Read & Write
Created by	Matthew Franks	Date	2016-08-24 14:53:27 UTC
Last used	Never		



Versions API et options en cours

Il y a actuellement deux versions de l'AMP pour les points finaux API - version 0 et version 1. La version 1 a la fonctionnalité supplémentaire contre la version 0. La documentation pour la version 1 est [ici](#). Vous pouvez tirer ce with de l'information l'utilisation de la version 1.

- Ordinateurs
- Activité d'ordinateur
- [Événements](#)
- Types d'événement
- Listes de fichier
- Éléments de liste de fichier
- Groupes
- Stratégies
- Versions

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

Panne et exemple de commande API

Chaque commande API contient les informations semblables et peut essentiellement décomposer à une commande de boucle et peut être regardée comme ceci :

boucle - o yourfilename.json https://clientID:APIKey@api.amp.cisco.com/v1/whatyouwanttodo

Quand vous utilisez la commande de boucle avec - option o, elle te permet de sauvegarder la sortie à un fichier. Dans ce cas le nom du fichier est « `yourfilename.json` ».

Conseil : Plus d'informations sur des fichiers .json peuvent être trouvées [ici](#).

L'étape suivante dans la commande de **boucle** est de placer l'adresse avec vos qualifications

avant @ le symbole. Quand vous des qualifications du generatie API, vous connaissez le clientID et l'APIKey, ainsi cette section de la commande ressemblera au lien donné ci-dessous.

<https://538e8b8203a48cc5c7fa:a190c911-8ca4-45fa-8740-e384ef2d3d5b@>

Ajoutez le numéro de version et ce que vous voudriez faire. Pour cet exemple, exécutez les options de [/v1/computers d'OBTENIR](#). La pleine commande ressemble à ceci :

boucle - o computers.json <https://538e8b8203a48cc5c7fa:a190c911-8ca4-45fa-8740-e384ef2d3d5b@api.amp.cisco.com/v1/computers>

Après que vous exécutiez la commande, vous devriez voir un fichier computers.json téléchargé au répertoire où vous avez initié la commande.

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

Note: La boucle est [accessible en ligne](#) et compilée pour un bon nombre de Plateformes qui inclut Windows (généralement vous voudrez utiliser Win32 – version générique).

Quand vous ouvrez le fichier vous verrez toutes les données dans une ligne simple. Si vous voudriez voir ceci dans son format approprié, vous pouvez installer un module d'extension de navigateur pour le formater comme JSON et pour ouvrir le fichier dans un navigateur. Ceci affiche que les informations pour vos ordinateurs que vous pouvez utiliser cependant vous voudraient, comme :

connector_guid, adresse Internet, active, liens, connector_version, operating_system, internal_ips, external_ip, group_guid, network_addresses, guid de stratégie, et nom de stratégie.

```
{
  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: "test.cisco.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: "1.1.1.1",
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"
}
}
```

Maintenant que vous avez vu un exemple de base dans l'action, vous pouvez utiliser les diverses options de commande de tirer et manipuler des données dans votre environnement.

[Informations connexes](#)

- [AMP de Cisco pour la documentation des points finaux API](#)

Support et documentation techniques - Cisco Systems