

Overzicht van de Cisco Advanced Malware Protection voor endpoints API

Inhoud

[Inleiding](#)

[API-Credentials genereren en verwijderen](#)

[API-versies en huidige opties](#)

[Uitsplitsing API-opdracht en voorbeeld](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de Cisco Advanced Malware Protection (AMP) voor endpoints. Cisco Advanced Malware Protection voor endpoints wordt geleverd met een API-interface (Application Programming Interface). Het stelt u in staat om gegevens uit een AMP te halen voor de toepassing van endpoints, en ze, indien nodig, te manipuleren.

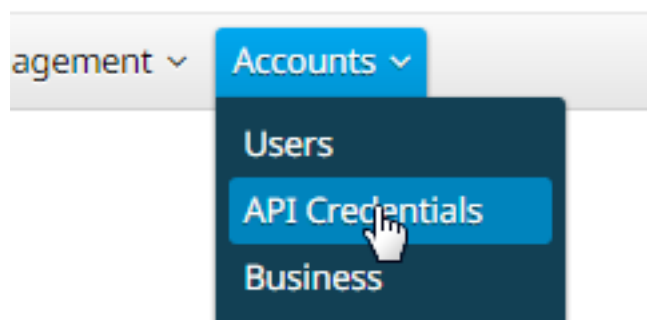
Dit artikel laat enkele basisfuncties van de API zien. De voorbeelden in dit artikel gebruiken een Windows 7-eindpunt.

Bijgedragen door Matthew Franks, Nazmul Rajib en Cisco TAC-engineers.

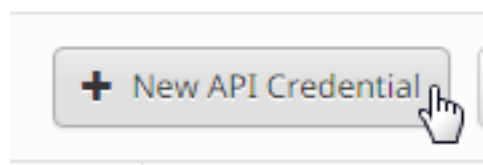
API-Credentials genereren en verwijderen

Om de AMP voor Endpoint API te kunnen gebruiken, moet u een API-gecrediteerd hebben. Volg de gegeven stappen om een gecrediteerd gebied te creëren door de AMP-console.

Stap 1: Log in op de console en navigeer naar **accounts > API**.



Stap 2: Klik op **New API Credentials** om een nieuwe set Keys te maken.



Stap 3: Geef een **toepassingsnaam** op. Selecteer het **bereik** van alleen-lezen of Lezen en schrijven.

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.

Opmerking: Een API met lees- en schrijfbereik kan wijzigingen aanbrengen in uw Cisco Advanced Malware Protection voor de configuratie van endpoints, die belangrijke problemen met uw endpoints kunnen veroorzaken. Sommige invoerbeveiliging die in Cisco Advanced Malware Protection voor Endpoints Console is niet van toepassing op API.

Stap 4: Klik op de knop **Maken**. De **API**-sleutelgegevens worden weergegeven. Bewaar deze informatie, omdat een deel ervan niet beschikbaar is nadat u het scherm hebt verlaten.

< 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


Opmerking: API-referenties (API-client-ID en API-toets) maken het mogelijk dat andere programma's uw Cisco Advanced Malware Protection voor endpoints ophalen en wijzigen. Het is functioneel equivalent aan een gebruikersnaam en wachtwoord en dient als zodanig

te worden behandeld.

Voorzichtig: Uw API-referenties worden slechts één keer weergegeven. Als je de geloofsbrieven verliest, moet je nieuwe genereren.

Verwijdert de API-referenties voor een toepassing als u vermoedt dat deze is gecompromitteerd en maak een nieuwe. Wanneer u een API-gecrediteerd verwijdert, sluit het de client af die de oude gebruikt, dus update ze met de nieuwe geloofsbrieven.

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



API-versies en huidige opties

Er zijn momenteel twee versies van de Advanced Malware Protection voor Endpoints API, versie 1 en 3. Versie 1 heeft extra functionaliteit versus versie 0. De documentatie voor versie 1 is [hier](#). U kunt deze informatie verkrijgen via het gebruik van versie 1.

- Computers
- Computer-activiteit
- Evenementen
- Incidenttypen
- Bestandslijsten
- Lijsten bestanden
- Groepen
- Beleid
- Versies

Klik op de betreffende opdracht in het document om voorbeelden van het gebruik te zien.

Uitsplitsing API-opdracht en voorbeeld

Elke API-opdracht bevat soortgelijke informatie en kan in wezen worden ingekort tot een curl-opdracht. U kunt er zo naar kijken:

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

Wanneer u de opdracht Krullen met de optie -Aan gebruikt, kunt u de uitvoer naar een bestand opslaan. In dit geval is de bestandsnaam "yourfilename.json".

Tip: Meer informatie over .json bestanden is [hier](#) te vinden.

De volgende stap in de curl opdracht is om het adres met uw geloofsbrieven in te stellen vóór het @ symbool. Wanneer u API Credentials generatie, kent u de clientID en APIKey, dus dit gedeelte

van de opdracht zal lijken op de link hieronder gegeven.

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

Voeg het versienummer toe en wat u wilt doen. Start bijvoorbeeld de opties [GET /v1/computers](#). De volledige opdracht ziet er zo uit:

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

Nadat u de opdracht hebt uitgevoerd, ziet u een **computer.json** bestand gedownload naar de folder waar u de opdracht gestart hebt.

```
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
                                 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
```

Opmerking: Curl is [online](#) beschikbaar en samengesteld voor veel platforms die Windows omvatten (meestal wilt u de Win32 - Generic versie gebruiken).

Wanneer u het bestand opent, ziet u alle gegevens in één regel. Als u dit in zijn juiste indeling wilt zien, kunt u een browser installeren plug-in om het als JSON op te maken en het bestand in een browser openen. Dit toont informatie voor uw computers die u kunt gebruiken zoals:

connector_guid, hostname, active, links, connector_version, operation_system, internal_ips, external_ip, group_guid, network_adressen, policy_guid en policy name.

```
{
  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"
}
}
```

Nu u een basisvoorbeeld in actie hebt gezien, kunt u de verschillende commando opties gebruiken om gegevens in uw omgeving te trekken en te manipuleren.

Gerelateerde informatie

- [Cisco Advanced Malware Protection voor endpoints API-documentatie](#)

Technische ondersteuning en documentatie – Cisco Systems