Cisco AMP for Endpoints API 개요

목차

소개

이 문서에서는 Cisco AMP(Advanced Malware Protection) for Endpoints에 대해 설명합니다.Cisco AMP for Endpoints는 API(Application Programming Interface)와 함께 제공됩니다. 이를 통해 AMP for Endpoints 구축에서 데이터를 가져오고 필요한 경우 조작할 수 있습니다.

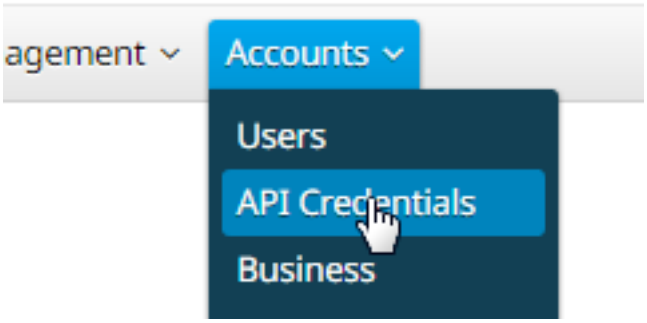
이 문서에서는 API의 몇 가지 기본 기능에 대해 설명합니다.이 문서의 예제에서는 Windows 7 끝점을 사용합니다.

기고자: Matthew Frankes, Nazmul Rajib, Cisco TAC 엔지니어

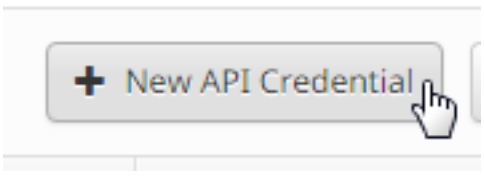
API 자격 증명 생성 및 삭제

AMP for Endpoint API를 사용하려면 API 자격 증명을 설정해야 합니다. 지정된 단계에 따라 AMP 콘솔을 통해 자격 증명을 생성합니다.

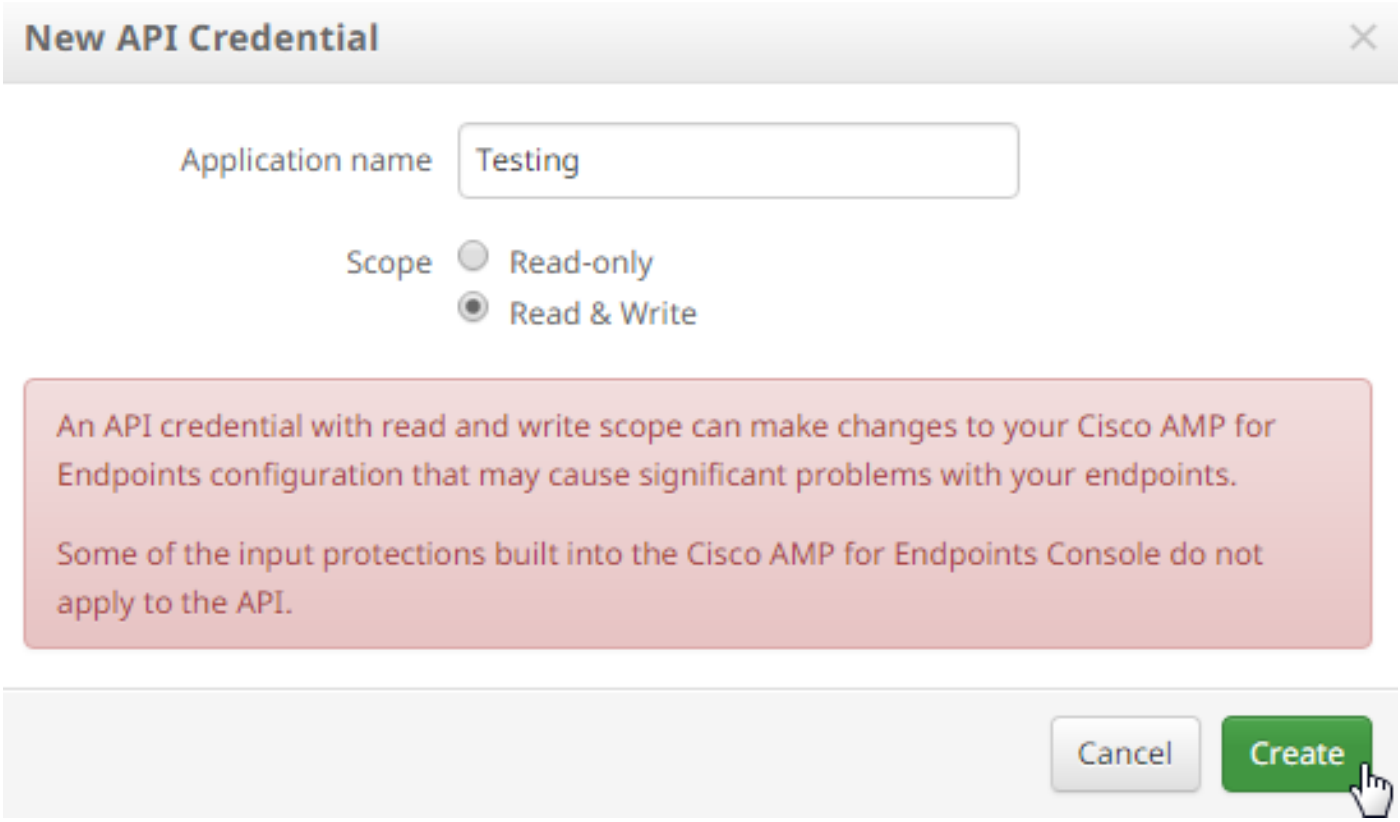
1단계:Console에 로그인하고 Accounts(계정) **> API Credentials(API 자격 증명)로 이동합니다.**



2단계:New **API Credential**을 클릭하여 새 키 집합을 생성합니다.

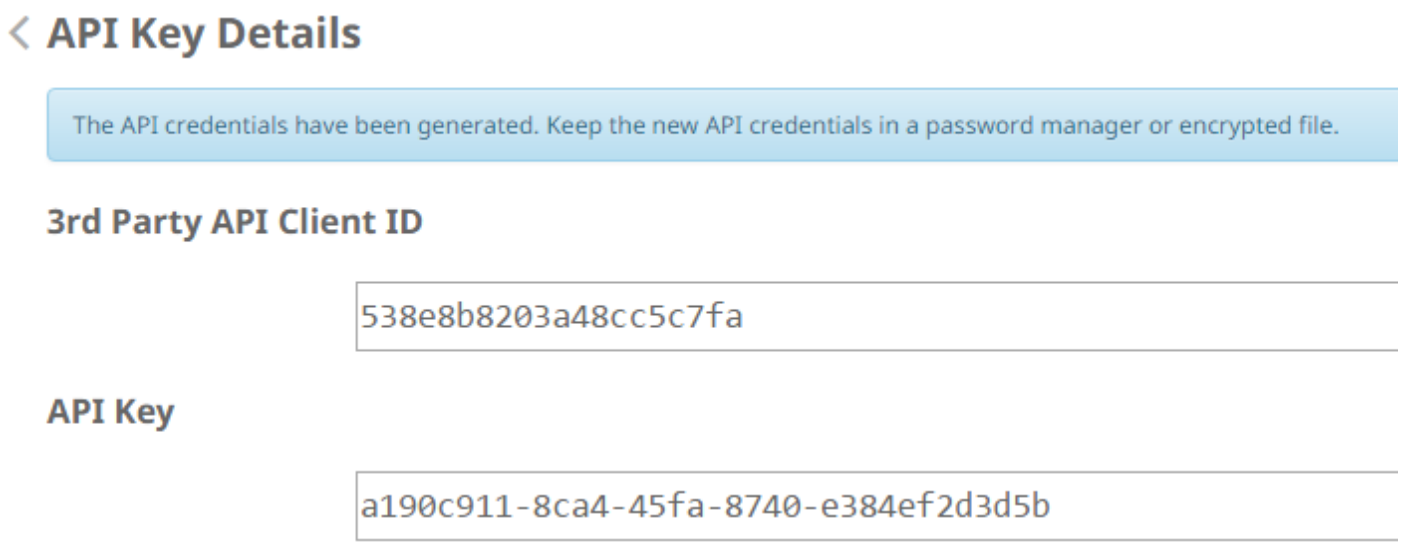


3단계:애플리케이션 **이름**을 **제공합니다**.읽기 전용 또는 읽기 및 쓰기 범위를 선택합니다.



참고:읽기 및 쓰기 범위가 있는 API 자격 증명은 Cisco AMP for Endpoints 컨피그레이션을 변경하여 엔드포인트에 심각한 문제를 일으킬 수 있습니다. Cisco AMP for Endpoints Console에 내장된 일부 입력 보호는 API에 적용되지 않습니다.

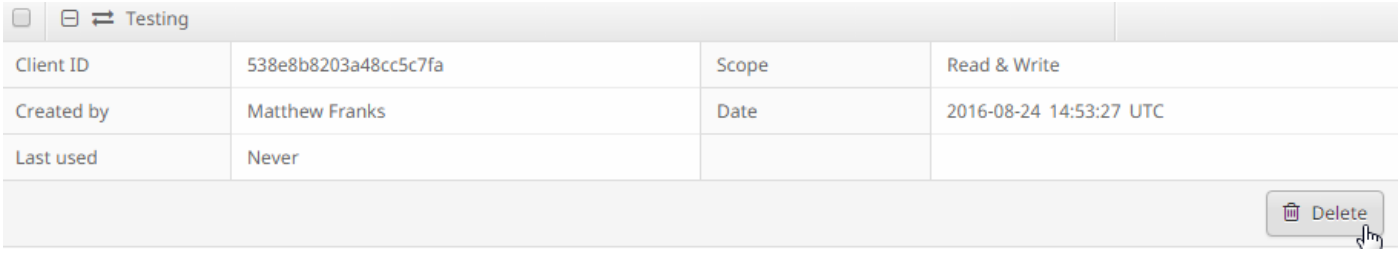
4단계: Create(생성) 버튼을 클릭합니다.API **Key Details가** 나타납니다.이 정보를 저장하면 화면을 떠난 후에는 일부 정보를 사용할 수 없습니다.



참고:API 자격 증명(API Client ID & API Key)을 사용하면 다른 프로그램에서 Cisco AMP for Endpoints 데이터를 검색하고 수정할 수 있습니다.사용자 이름 및 비밀번호와 기능적으로 동일하며, 그렇게 취급해야 합니다.

주의:API 자격 증명은 한 번만 표시됩니다.자격 증명이 손실되면 새 자격 증명을 생성해야 합니다.

보안이 침해되었다고 의심되는 애플리케이션의 API 자격 증명을 삭제하고 새 자격 증명을 생성합니다. API 자격 증명을 삭제하면 이전 자격 증명을 사용하는 클라이언트가 잠기므로 새 자격 증명으로 업데이트합니다.



API 버전 및 현재 옵션

현재 AMP for Endpoints API의 두 가지 버전(버전 0 및 버전 1)이 있습니다. 버전 1에는 버전 0과 다른 추가 기능이 있습니다. 버전 1에 대한 설명서가 여기에 있습니다. 버전 1을 사용하여 이 정보를 가져올 수 있습니다.

- 컴퓨터
- 컴퓨터 활동
- 이벤트
- 이벤트 유형
- 파일 목록
- 파일 목록 항목
- 그룹
- 정책
- 버전

문서의 관련 명령을 클릭하면 사용 예가 표시됩니다.

API 명령 분리 및 예

각 API 명령에는 유사한 정보가 포함되어 있으며 기본적으로 curl 명령으로 분류할 수 있으며 다음과 같이 볼 수 있습니다.

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

curl 명령을 -o 옵션과 함께 사용하면 출력을 파일에 저장할 수 있습니다.이 경우 파일 이름은 "yourfilename.json"입니다.

> **팁**:.json 파일에 대한 자세한 내용은 여기에서 확인할 수 있습니다.

curl 명령의 다음 단계는 @ 기호 앞에 자격 증명으로 주소를 설정하는 것입니다.API 자격 증명을 생성할 때 clientID와 APIKey를 알고 있으므로 이 명령 섹션은 아래에 지정된 링크와 유사합니다.

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

버전 번호와 원하는 작업을 추가합니다.이 예에서는 GET /v1/computers 옵션을 실행합니다.전체 명령은 다음과 같습니다.

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

명령을 실행한 후 명령을 시작한 디렉토리**에** 다운로드한 computers.json 파일이 표시됩니다.

```
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
```

> **참고:**Curl은 온라인으로 제공되며 Windows를 포함하는 여러 플랫폼에 대해 컴파일됩니다(일반적으로 Win32 - 일반 버전 사용).

파일을 열면 모든 데이터가 한 줄로 표시됩니다. 적절한 형식으로 보려면 브라우저 플러그인을 설치하여 JSON으로 포맷하고 브라우저에서 파일을 열 수 있습니다.다음과 같이 원하는 대로 사용할 수 있는 컴퓨터에 대한 정보를 표시합니다.

connector_guid, hostname, active, links, connector_version, operating_system, internal_ips, external_ip, group_guid, network_addresses, policy guid 및 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"
}
```


이제 기본적인 예제가 확인되었으므로 다양한 명령 옵션을 사용하여 사용자 환경의 데이터를 끌어와 조작할 수 있습니다.

관련 정보

- Cisco AMP for Endpoints API 설명서

기술 지원 및 문서 – Cisco Systems