Cisco AMP for Endpoints API の概要

目次

概要

この資料はエンドポイントのための Cisco Advanced Malware Protection （ AMP ）について記述したものです。 Cisco AMP for Endpoints は Application Programming Interface （ API; アプリケーション プログラミング インターフェイス ）が付いています。 これにより、必要に応じて、導入されている AMP for Endpoints からデータを取得し、それらのデータを操作できます。

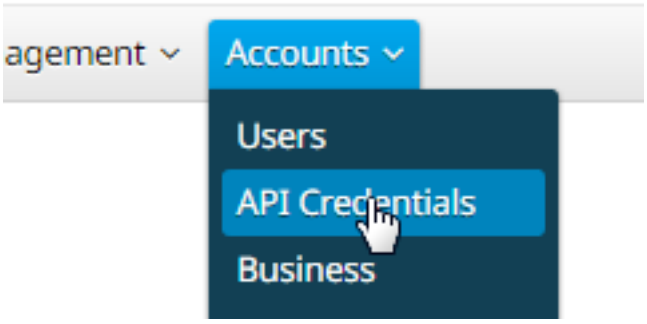
この記事では、API の基本機能について説明します。 この記事の例では Windows 7 エンドポイントが使用されています。

Matthew Franks、Nazmul Rajib、および Cisco TAC エンジニアによって貢献される。

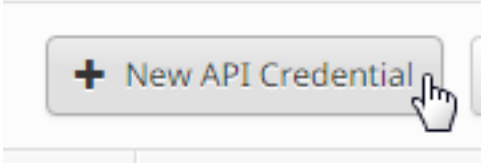
生成するおよび削除 API 資格情報

AMP for Endpoint API を使用するには、API クレデンシャルを設定する必要があります。 AMP コンソールによって資格情報を作成するためにある特定のステップに従って下さい。

ステップ 1： コンソールにログイン し、**アカウント > API 資格情報**にナビゲート して下さい。

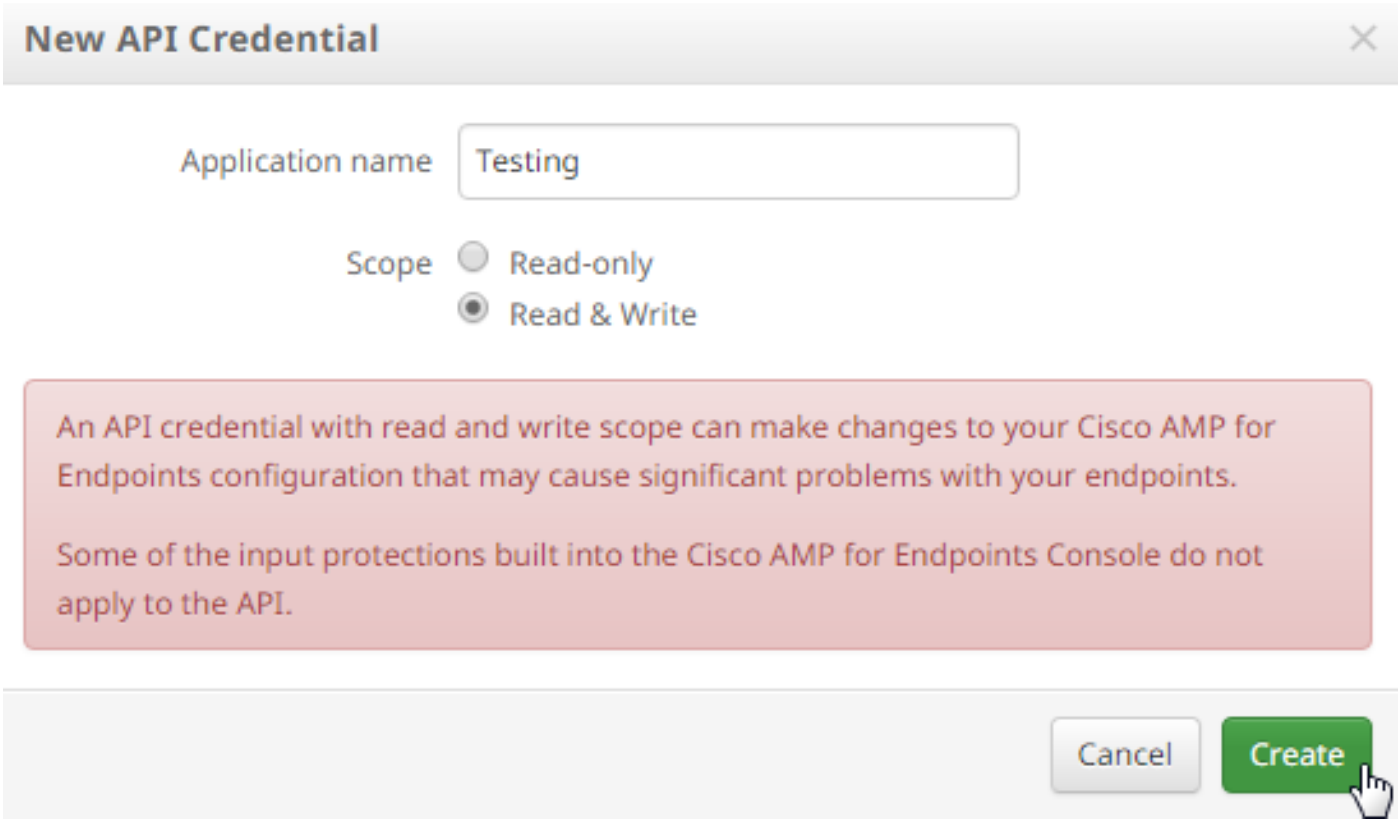


ステップ 2： 新しい一組のキーを作成するために **API 資格情報を**『New』 をクリック して下さい。



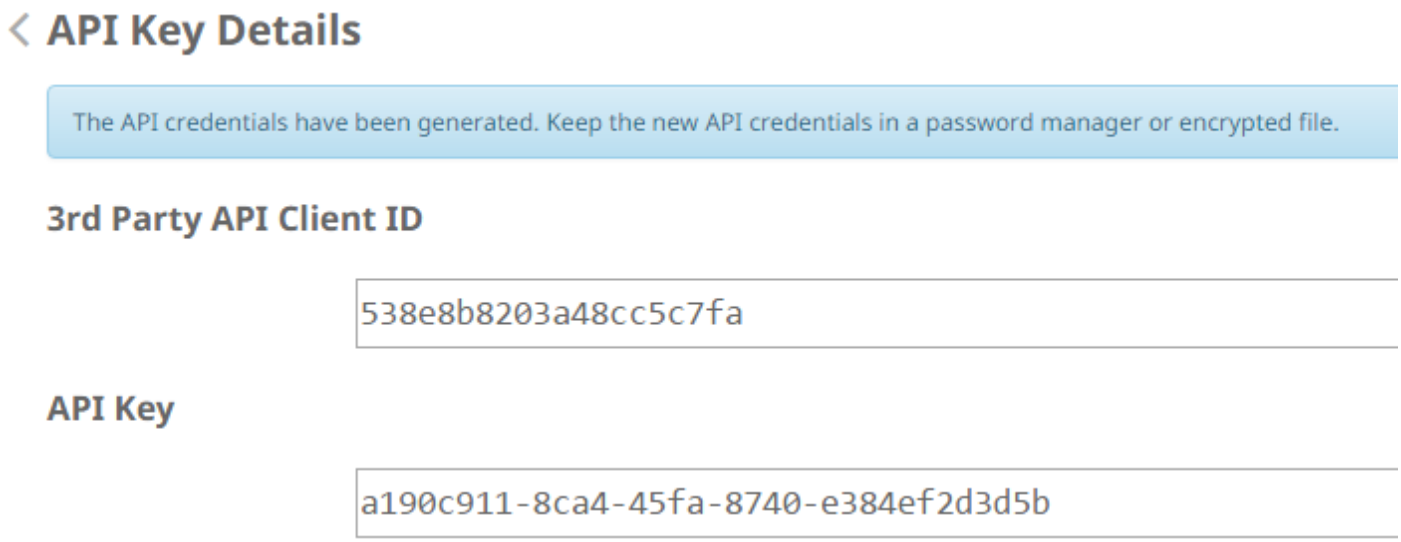
ステップ3： [Application name] を指定します。 [Scope] で [Read-only] または [Read & Write] を

選択します。



注: 読まれるを用いる API 資格情報はスコープをエンドポイントに重要な問題を引き起こすかもしれない Cisco AMP for Endpoints 設定への変更を行なうことができます書き。 Cisco AMP for Endpoints コンソールに組み込まれている一部の入力保護は、API には適用されません。

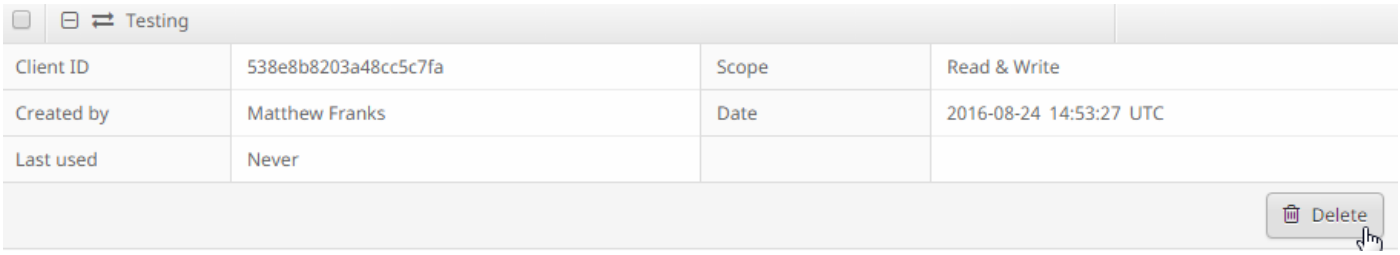
ステップ 4： [Create] ボタンをクリックします。 [API Key Details] が表示されます。 それのいくつかが画面を残した後利用可能ではないのでこの情報を保存して下さい。



注: API クレデンシャル（ API クライアント ID および API キー ）により、他のプログラムで Cisco AMP for Endpoints データを取得および変更できます。 これは、ユーザ名およびパスワードと機能的には同等であるため、そのように取り扱う必要があります。

注意： API クレデンシャルが表示されるのは 1 回のみです。 クレデンシャルが不明になった場合、新しいクレデンシャルを作成する必要があります。

アプリケーションの API クレデンシャルが漏えいした疑いがある場合、その API クレデンシャルを削除し、新しい API クレデンシャルを作成します。 API 資格情報を削除するとき、新しい資格情報と古い物を使用する、従ってアップデートしますそれらをロックしますクライアントを。



API のバージョンおよび現在のオプション

AMP for Endpoints API には、現在 2 つのバージョン (バージョン 0 とバージョン 1) があります。 バージョン 1 に追加機能性が vs バージョン 0 あります。 バージョン 1 のドキュメンテーションは、ここにあります。 バージョン 1 の使用この情報 witn を引っ張ることができます。

- コンピュータ
- コンピュータ アクティビティ
- イベント
- イベント タイプ
- ファイル一覧
- ファイル一覧項目
- [グループ (Groups)]
- ポリシー
- バージョン

使用方法の例を参照する資料の相当するコマンドをクリックして下さい。

API コマンドの詳細および例

各 API コマンドには類似する情報が含まれます。各 API コマンドは、curl コマンドに基本的に分解できます。

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

とカール コマンドを使用するとき - o オプション、ファイルに出力を保存することを可能にします。 この場合、ファイル名は「yourfilename.json」です。

ヒント： .json ファイルの詳細については、ここを参照してください。

curl コマンドでの次の手順は、@ 記号の前にクレデンシャルがあるアドレスを設定することです。 generatie API 資格情報、コマンドの clientID および APIKey、従って知っている場合このセクションを下記に与えられたリンクに類似しています。

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

望むか何をすることをバージョン番号を追加すれば。 この例に関しては、GET /v1/computers オプションを実行して下さい。このように fullコマンドな:

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

コマンドを実行した後、コマンドを開始したディレクトリに computers.json ファイルがダウンロードされたことが分かるはずです。

```
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
```

> **注:** Windows（一般に–ジェネリック バージョン Win32 を使用したいと思います）が含まれているカールは多くのプラットフォームのためにオンラインで手続きでき、コンパイルされて。

ファイルを開くと、すべてのデータが 1 行で表示されます。 適切な形式でこれを見ることを望んだ場合それを JSON としてフォーマットし、ブラウザのファイルを開くためにブラウザ プラグインをインストールできます。 これにより、使用できるコンピュータの情報が表示されますが、以下のようなデータが有用です。

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


ここまで実際の基本例を見てきました。各種コマンド オプションを使用して、環境のデータを取得および操作できます。

関連情報

- Cisco AMP for Endpoints API のドキュメンテーション

テクニカルサポートとドキュメント - Cisco Systems