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 （ アンペア ）について記述したものです。 エンド ポイントのための Cisco アンペアは 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。

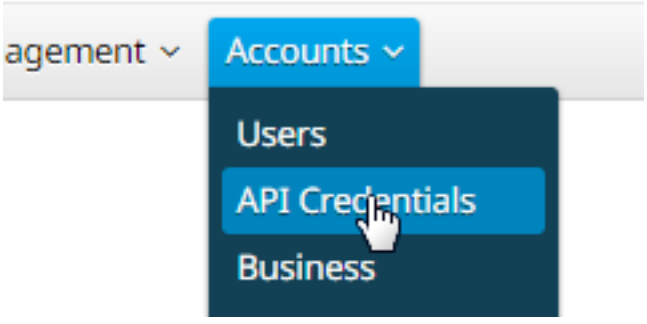
この技術情報は API のいくつかの基本的な機能性を示します。 この技術情報の例は Windows 7 エンド ポイントを使用します。

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

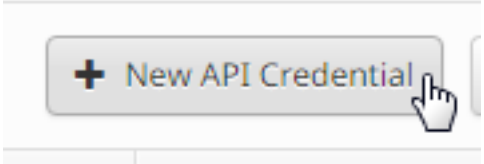
API 信任状を生成し、削除して下さい

アンペアをエンド ポイント API のために使用するために、API クレデンシャルを設定しなければなりません。 アンペア コンソールを通してクレデンシャルを作成するためにある特定のステップに従って下さい。

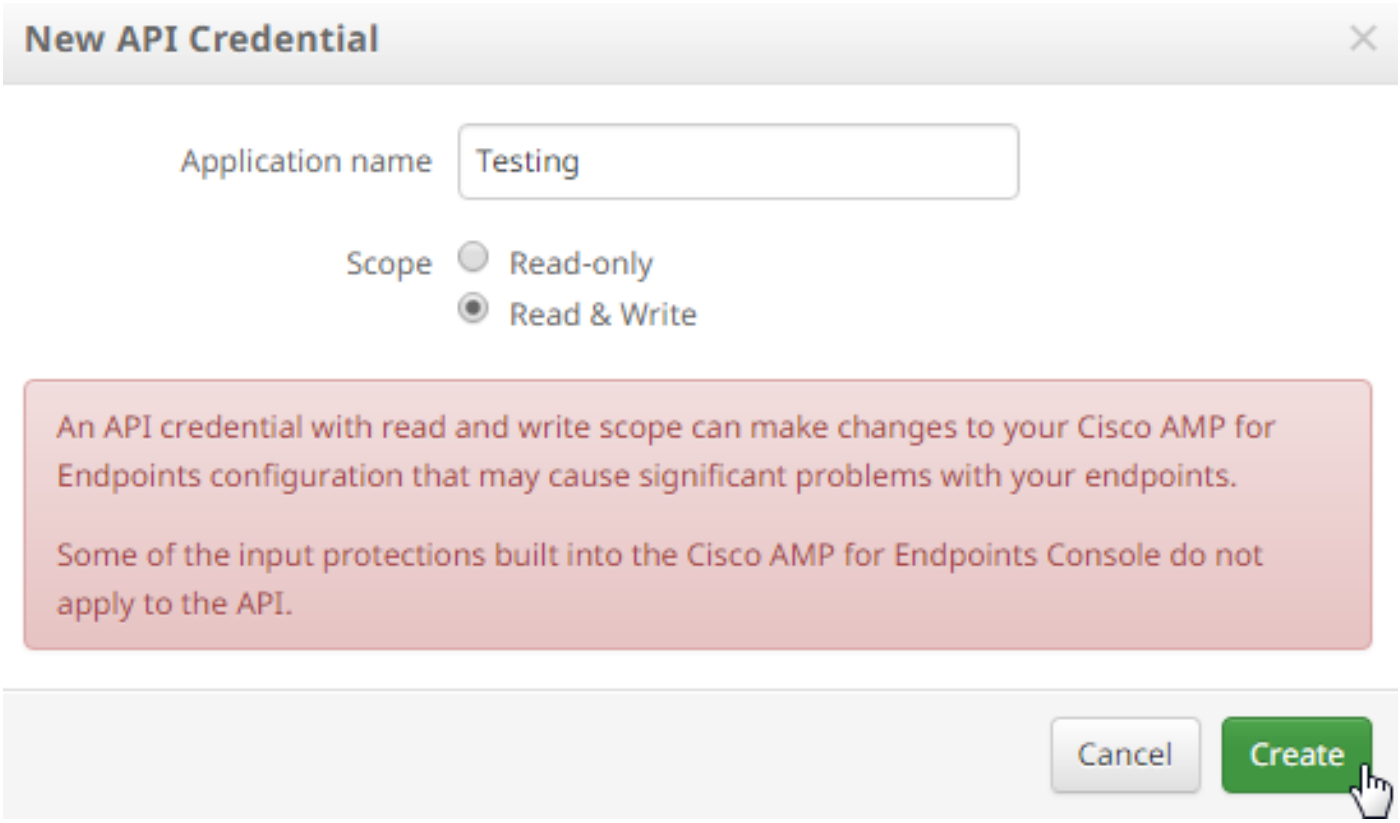
ステップ 1： コンソールにログイン し、**アカウント > API 信任状**にナビゲート して下さい。



ステップ 2： 新しい一組のキーを作成するために **API クレデンシャルを**『New』 をクリック して下さい。

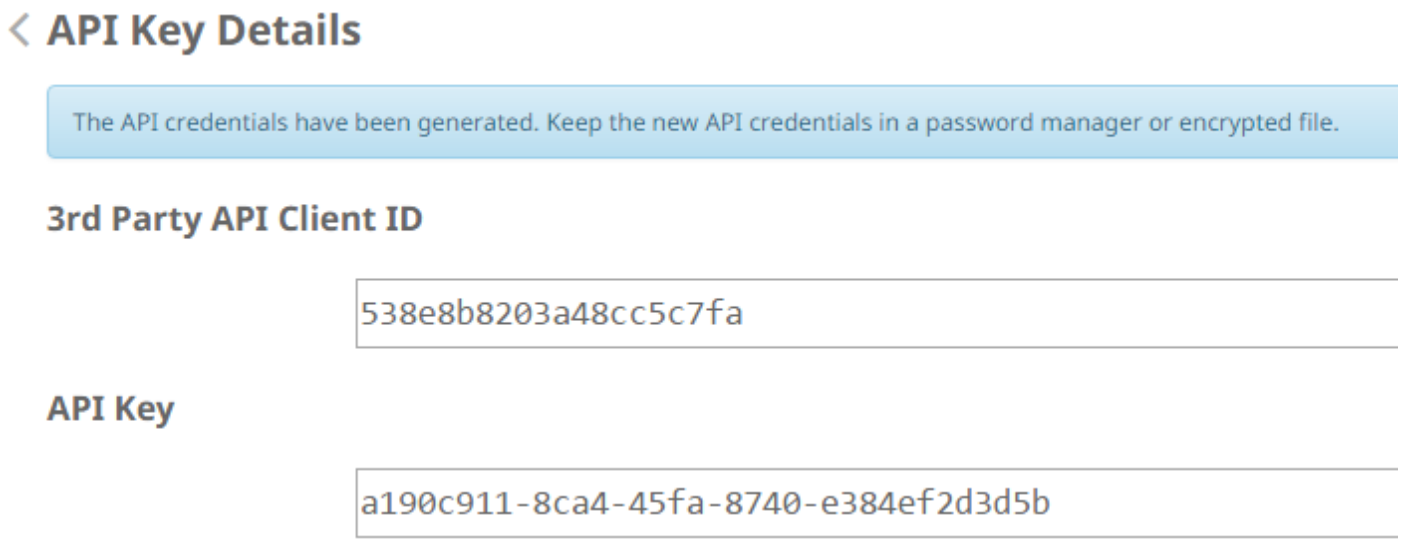


ステップ3： **アプリケーション 名を**つけて下さい。 読み取り専用の**スコープを**選択するか、または読んで下さい及び書いて下さい。



注: 読まれるを用いる API クレデンシャル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エンド ポイント設定用の Cisco アンペアへの変更を行なうことができます書き。 エンド ポイント コンソールのための Cisco アンペアに構築される API にいくつかの入力保護は適用しません。

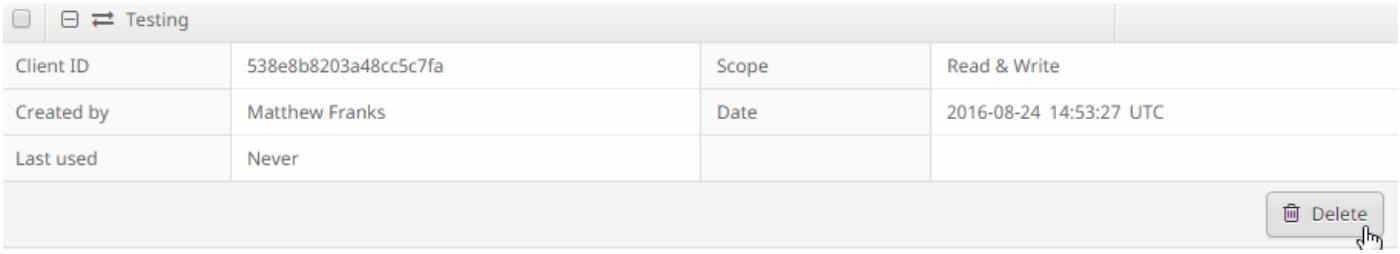
ステップ 4： [Create] ボタンをクリックします。 **API キー詳細は**現われます。 それのいくつかが画面を残した後利用可能ではないのでこの情報を保存して下さい。



注: API 信任状は（API クライアントID 及び API キー）他のプログラムがエンド ポイントデータのための Cisco アンペアを取得し、修正するようにします。 それはユーザ名 およびパスワードと機能的に類似して、そのように扱う必要があります。

> **注意**： API 信任状は表示されます一度ただ。 信任状を失う場合、新しいものを生成しなければなりません。

疑う場合アプリケーションのための API 信任状を削除して下さい妥協され、新しいものを作成することを。 API クレデンシャルを削除するとき、新しい信任状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 バージョンおよび現在のオプション

現在エンド ポイント API のためのアンペアの 2 つのバージョンが-バージョン 0 およびバージョン 1 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 のためのドキュメントはここにあります。 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 リスト
- ファイル リスト項目
- [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 は故障および例を命じます

各 API コマンドは同じような情報が含まれ、カール コマンドに本質的に破壊でき、このようになることができます:

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 ファイルに関する詳細はここに見つけることができます。

カール コマンドの次のステップは@記号の前に信任状とのアドレスを設定することです。 generatie API 信任状、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、コマンドを始めるディレクトリにダウンロードされる **computers.json ファイルを**見るはずです。

```
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。

ファイルを開く場合単一 行のデータすべてが表示されます。 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。 これはコンピュータのための情報が使用できるしかしこと、好む示します (以下を参照) :

connector_guid、ホスト名、アクティブ、リンク、connector_version、operating_system、internal_ips、external_ip、group_guid、network_addresses、ポリシー guid およびポリシー名。


```
{
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"
}
```


操作の基本的な例を参照したので、環境のデータを引っ張り、処理するさまざまなコマンドオプションを使用できます。

関連情報

- エンド ポイント API ドキュメントのための Cisco アンベア

テクニカルサポートとドキュメント - Cisco Systems