エンドポイント API のための Cisco AMP の外観

目次

概要

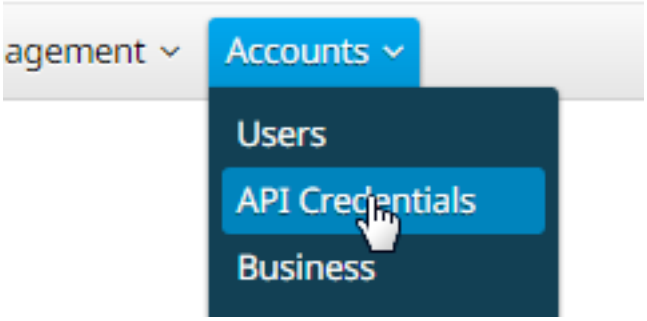
エンドポイントのための Cisco AMP は API が付いています。 それは必要なときエンドポイント配備のための AMP からのデータを引っ張ることを可能にしそれらを処理します。

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。

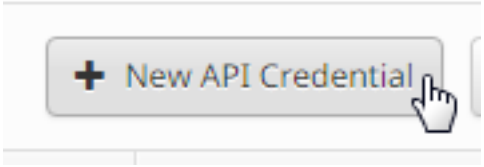
API 資格情報を生成し、削除します

AMP をエンドポイント API のために使用するために、API 資格情報を設定しなければなりません。 AMP コンソールによって資格情報を作成するために下記のステップに従って下さい。

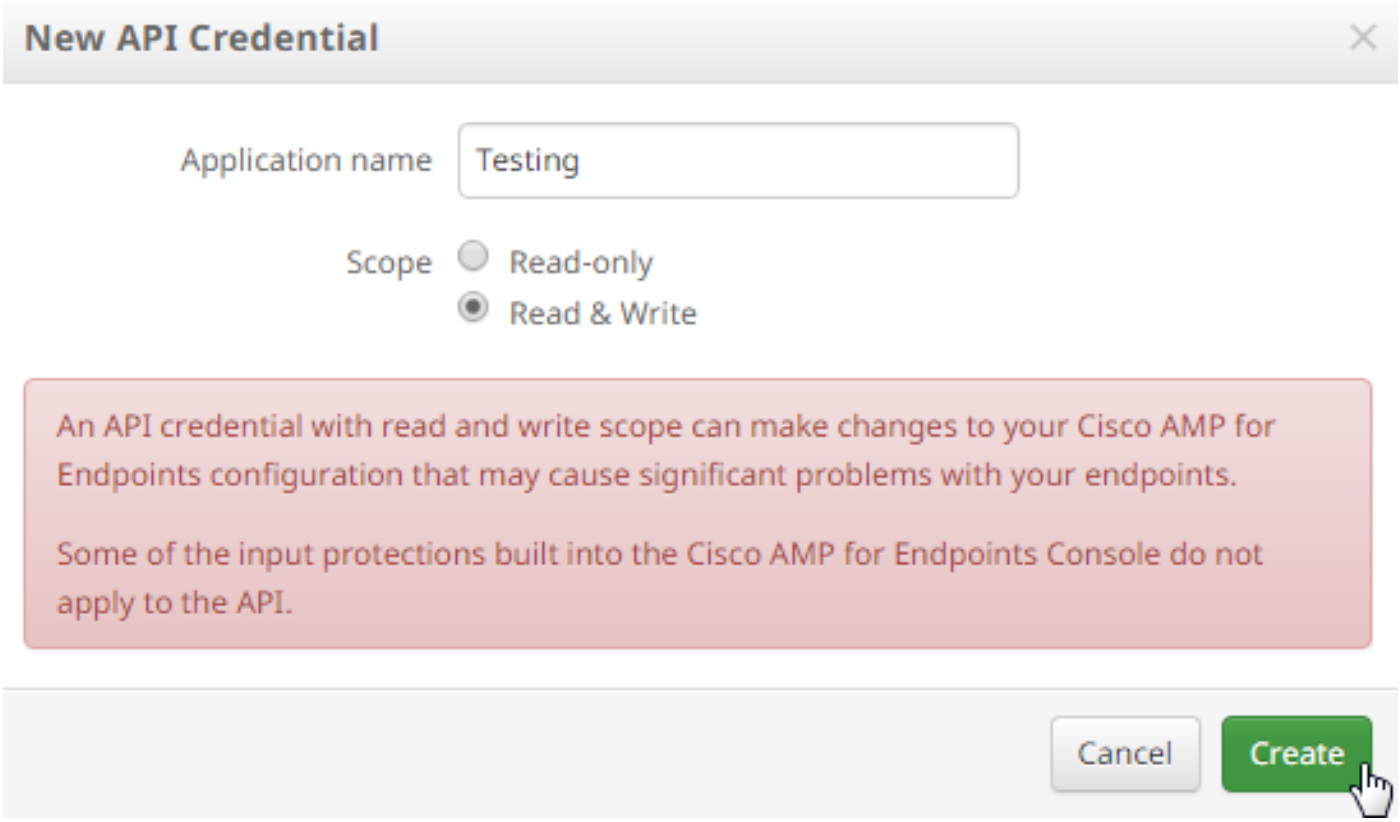
ステップ 1： コンソールにログイン し、**アカウント > API 資格情報**にナビゲート して下さい:



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:

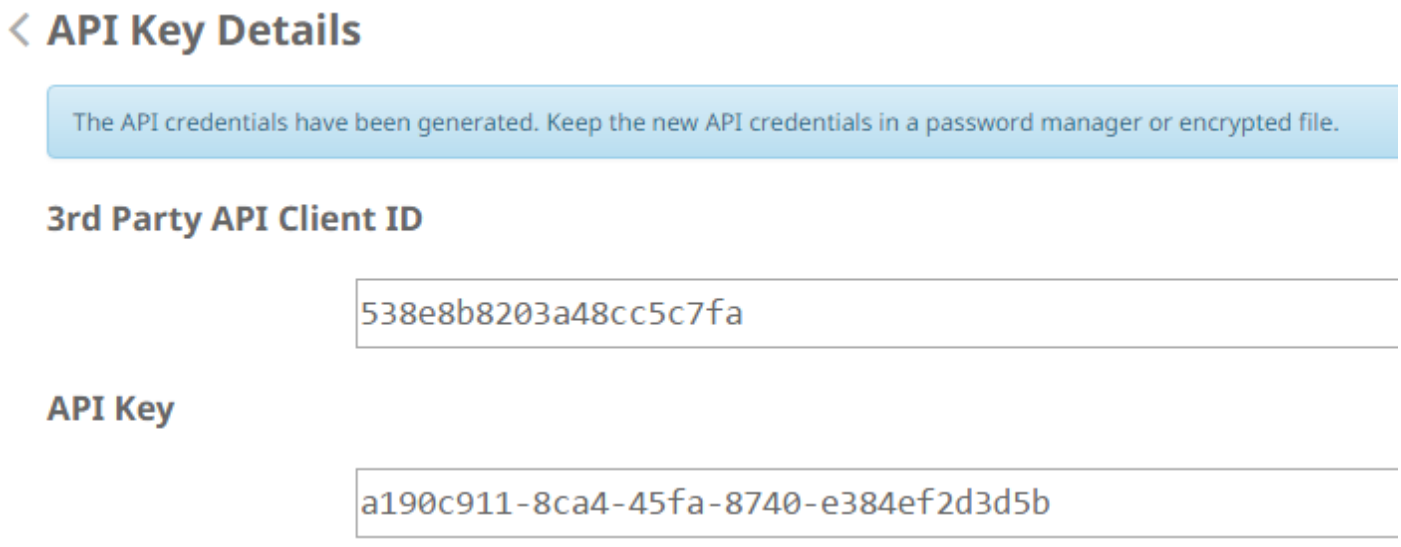


手順 3： **アプリケーション 名を**つけて下さい。 *読み取り専用の***スコープを**選択するか、または *読んで下さい及び書いて下さい。*



注: 読まれるを用いる API 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エンドポイント 設定のための Cisco AMP 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 AMP 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。 それのいくつかがこの画面を残した後利用可能ではないのでこの情報を保存することを忘れないでいて下さい。

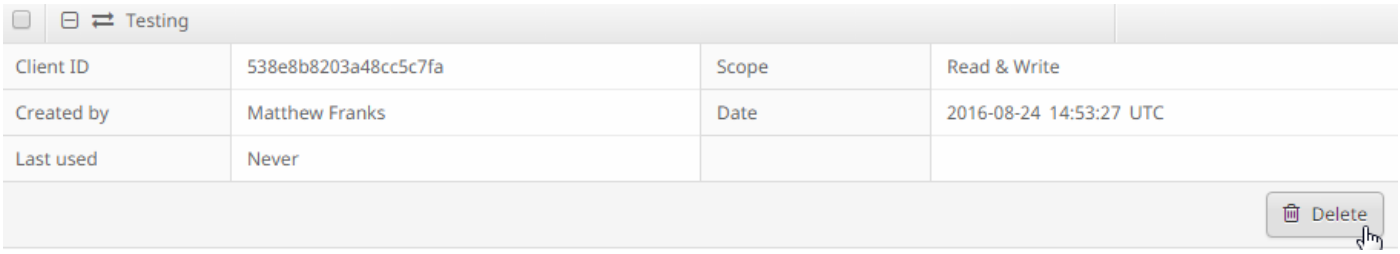


注: API 資格情報は（API クライアントID 及び API キー）他のプログラムがエンドポイントデータのための Cisco AMP を取得し、修正するようにします。 それはユーザ名 および パスワードと機能的に類似して、そのように扱う必要があります。

注意： API 資格情報は表示する一度ただ。 資格情報を失う場合、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 資格情報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 資格情報を削除することは古い物を使用する、従って新しい資格情報とそれらをアップデートすることを確かめます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 AMP の 2 バージョン-バージョン 0 およびバージョン 1 があります。 追加機能性が vs バージョン 0 あるバージョン 1。 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 を使用して次の情報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ドキュメントの相当するコマンドをクリックして下さい。

API コマンド故障および例

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:

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

のカール コマンドの使用- o オプションは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。

コマンドの次 の ステップは@記号の前に資格情報とのアドレスを設定 することです。 生成 API 資格情報 セクションの情報から、clientID および APIKey を知っています、従ってコマンドのこのセクションは類似しています:

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

次に望むか何をすることを、バージョン番号を追加し。 この例に関しては GET /v1/computers オプションを実行します。 下記にのように fullコマンド見え:

```
curl -o computers.json https://538e8b8203a48cc5c7fa:a190c911-8ca4-45fa-8740-e384ef2d3d5b@api.amp.sourcefire.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` 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:** カールは Windows を含む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: （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）。

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.sourcefire.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.sourcefire.com/v1/computers/abcdef-1234-5678-9abc-def123456789",
trajectory: "https://api.amp.sourcefire.com/v1/computers/abcdef-1234-5678-9abc-def123456789/trajectory",
group: "https://api.amp.sourcefire.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。

関連資料

- エンドポイント API シスコのドキュメントのための Cisco AMP