

# エンドポイント API のための Cisco AMP の外観

## 目次

### [概要](#)

[API 資格情報を生成し、削除します](#)

[API バージョンおよび現在のオプション](#)

[API コマンド故障および例](#)

[関連資料](#)

## 概要

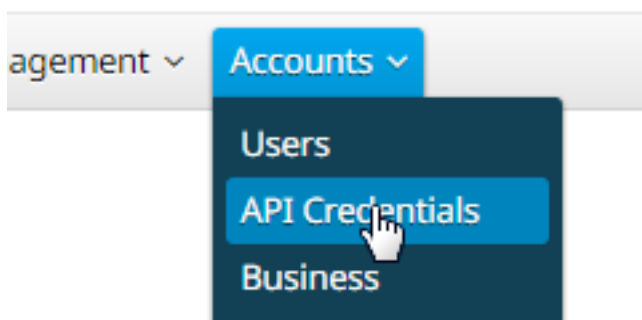
エンドポイントのための Cisco AMP は API が付いています。それは必要なときエンドポイント配備のための AMP からのデータを引っ張ることを可能にしそれら进行处理します。

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。

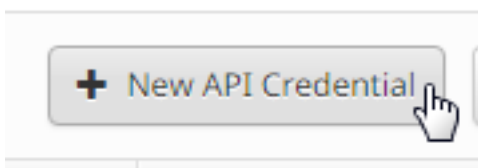
## API 資格情報を生成し、削除します

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。

## 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.

Cancel

Create



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。

## < 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

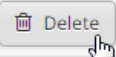
注: API 資格情報は ( API クライアントID 及び API キー ) 他のプログラムがエンドポイント データのための Cisco AMP を取得し、修正するようにします。 それはユーザ名 および パスワードと機能的に類似して、そのように扱う必要があります。

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更新することを確かめますロックしますクライアントを。

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



## 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
```

のカーン 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:

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

次に望むか何をするを、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:a190c911-8ca4-45fa-8740-e384ef2d3d5b@api.amp.sourcefire.com/v1/computers
 % Total    % Received % Xferd  Average Speed   Time    Time       Time  Current
           %         0         0             0             0      0:00:02  --:--:--   0
```

```
C:\Users\mafranks>dir | findstr computers
09/06/2016  02:37 PM                128 computers.json
```

注: カーネルは 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](#)