面向終端的思科AMP API概述

目錄

簡介

本檔案介紹思科終端進階惡意軟體防護(AMP)。面向終端的思科AMP附帶了一個應用程式設計介面(API)。 它允許您從面向終端的AMP部署中提取資料，並在必要時對其進行操作。

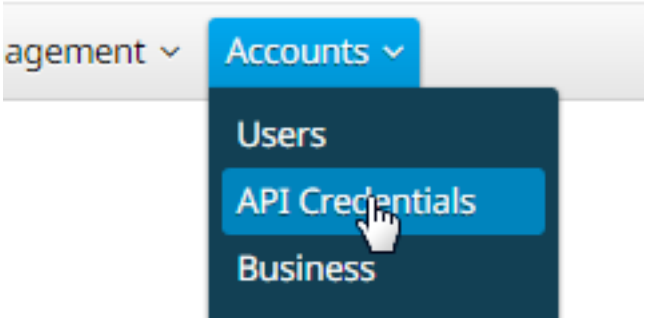
本文展示API的一些基本功能。本文中的示例使用Windows 7終結點。

作者：Matthew Franks、Nazmul Rajib和Cisco TAC工程師。

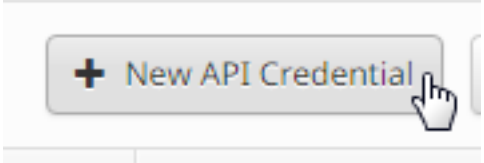
生成和刪除API憑據

為了使用面向終端API的AMP，您必須設定API憑證。 按照給定的步驟通過AMP控制檯建立憑據。

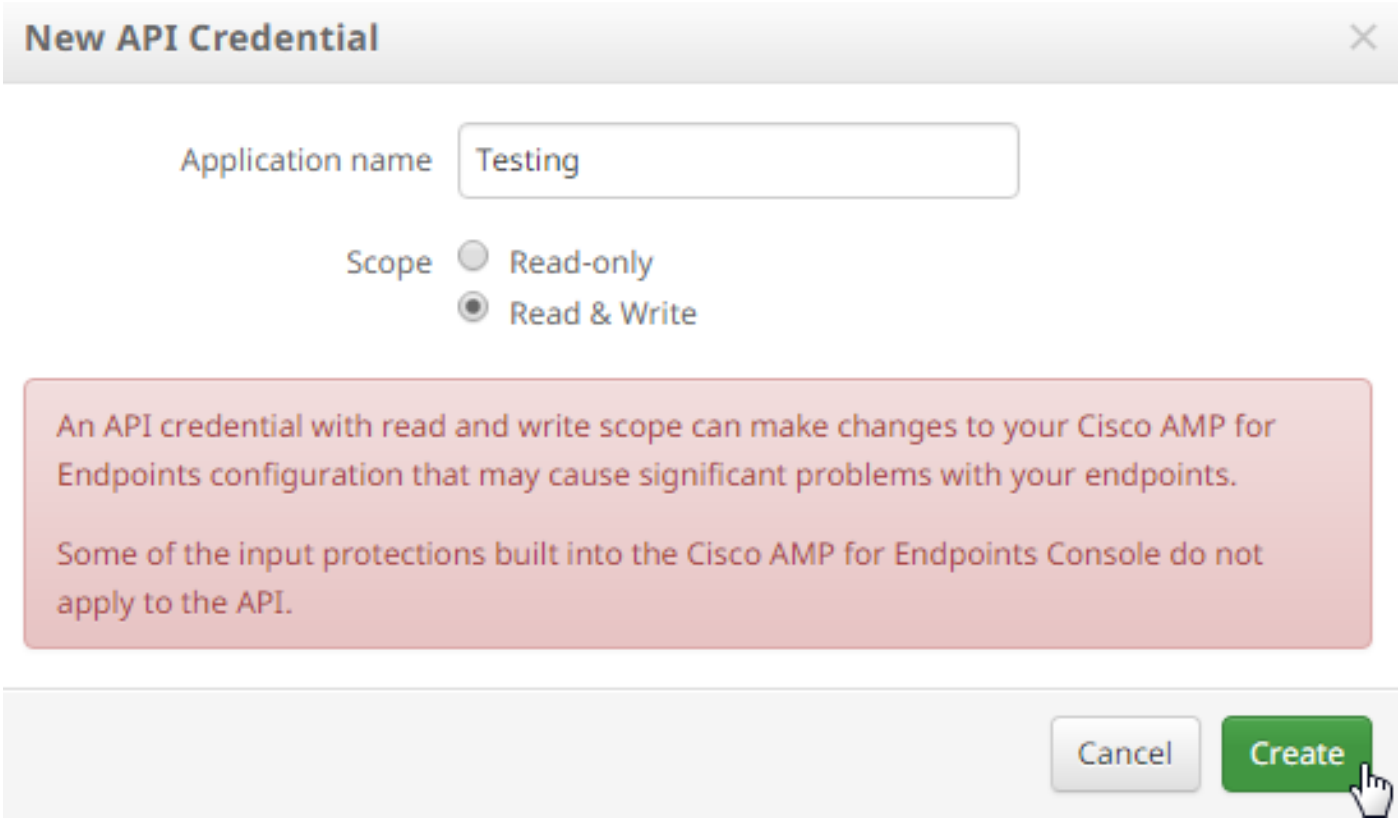
第1步：登入到Console，然後導航到**Accounts > API Credentials。**



第2步：按一下**新建API憑據**以建立新的金鑰集。

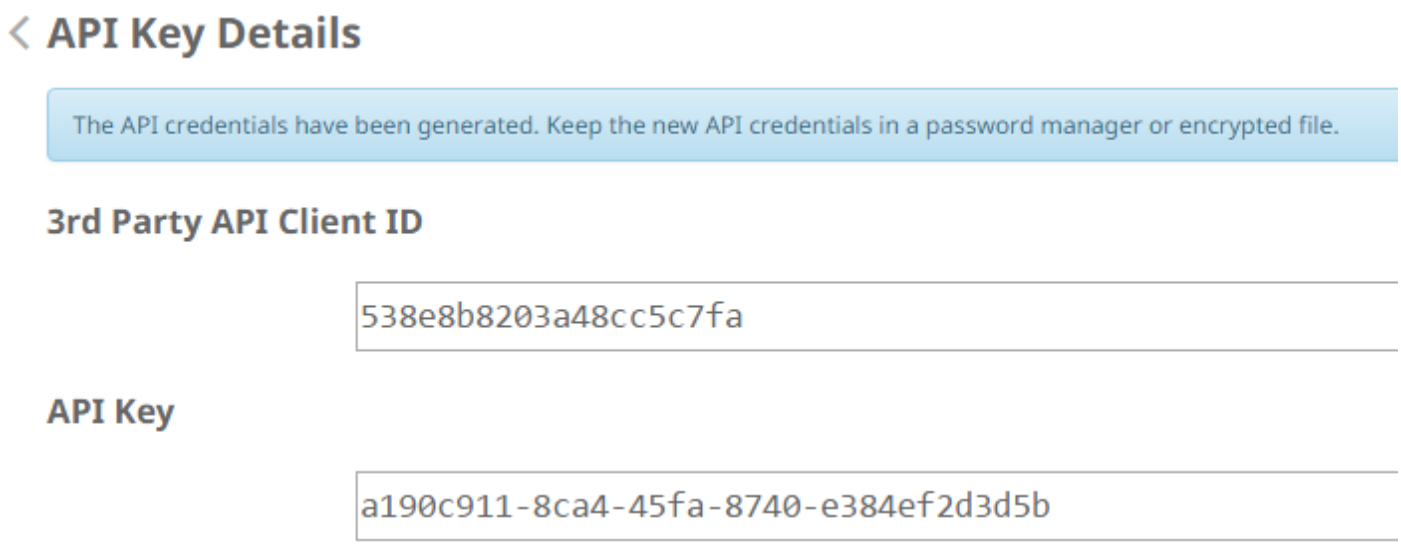


步驟3:提供應用**程式名稱**。選擇**Scope** of Read-only或Read & Write。



附註：具有讀取和寫入作用域的API憑證可以對面向終端的思科AMP配置進行更改，這可能導致您的終端出現嚴重問題。 面向終端的思科AMP控制檯內建的一些輸入保護不適用於API。

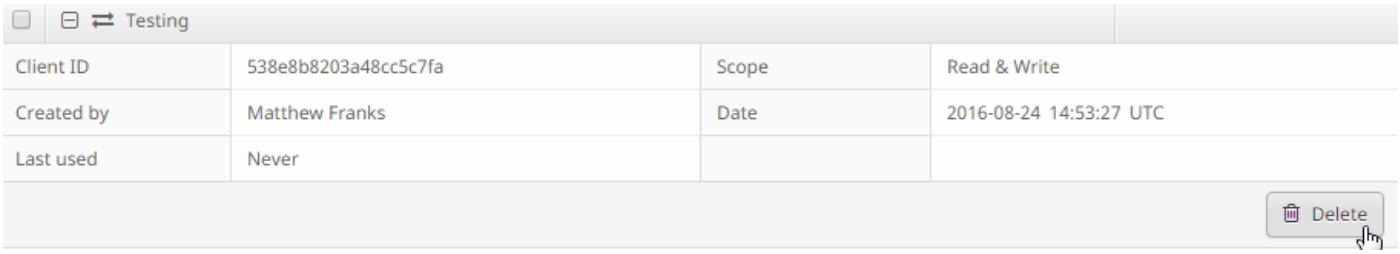
第4步： 按一下**Create**按鈕。系統將顯示**API Key Details**。儲存此資訊，因為某些資訊在離開螢幕後不可用。



附註：API憑證（API客戶端ID和API金鑰）將允許其他程式檢索和修改面向終端的思科AMP資料。它在功能上與使用者名稱和密碼等效，應視為等效。

注意：您的API憑證僅顯示一次。如果丟失憑證，您必須生成新憑證。

如果您懷疑某個應用程式的API憑證已受到危害，請將其刪除，然後建立一個新憑據。 刪除API憑據時，它會鎖定使用舊憑據的客戶端，因此使用新憑據更新它們。



API版本和當前選項

目前有兩個版本的面向終端的AMP API — 版本0和版本1。 版本1與版本0相比具有其他功能。版本1的文檔位於此處。 您可以使用版本1獲取此資訊。

- 電腦
- 電腦活動
- 活動
- 事件型別
- 檔案清單
- 檔案清單項
- 組
- 策略
- 版本

按一下文檔中的相關命令可檢視其用法示例。

API命令細分和示例

每個API命令都包含類似的資訊，並且基本上可以分解為一個curl命令，可以這樣檢視：

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

使用帶有-o選項的curl命令時，可將輸出儲存到檔案。在這種情況下，檔名是"yourfilename.json"。

> **提示：**有關.json檔案的更多資訊，請參閱此處。

curl命令的下一步是使用@符號前的憑據設定地址。生成API憑據時，您知道clientID和APIKey，因此命令的這一部分將類似於下面給出的連結。

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

新增版本號和您要執行的操作。在本示例中，運行GET /v1/computers選項。完整命令如下所示：

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

運行該命令後，您應該會看到一個computers.json檔案下載到您發起該命令的目錄中。

```
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
```

附註：Curl線上提供，針對包括Windows在內的許多平台進行編譯（通常您想要使用Win32 — 通用版本）。

開啟檔案時，您將看到一行中的所有資料。 如果您希望看到其格式正確，可以安裝一個瀏覽器外掛，將其格式化為JSON，然後在瀏覽器中開啟該檔案。這顯示您想要使用的電腦資訊，例如：

connector_guid、hostname、active、links、connector_version、operating_system、internal_ips、external_ip、group_guid、network_addresses、policy guid和策略名稱。


```
{
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"
}
```


現在已看到一個操作中的基本示例，您可以使用各種命令選項來提取和操作環境中的資料。

相關資訊

- 思科終端進階惡意軟體防護API檔案

技術支援與文件 - Cisco Systems