ةجمرب ةهجاول Cisco AMP ىلع ةماع ةرظن تاقيبطت نقاط الناية

المحتويات

المقدمة

يوضح هذا المستند الحماية المتقدمة من البرامج الضارة (AMP) من Cisco لنقاط النهاية. تأتي الحماية المتقدمة لنقاط النهاية من Cisco بواجهة برمجة التطبيقات (API). يسمح لك بسحب البيانات من AMP لنشر نقاط النهاية ومعالجتها عند الضرورة.

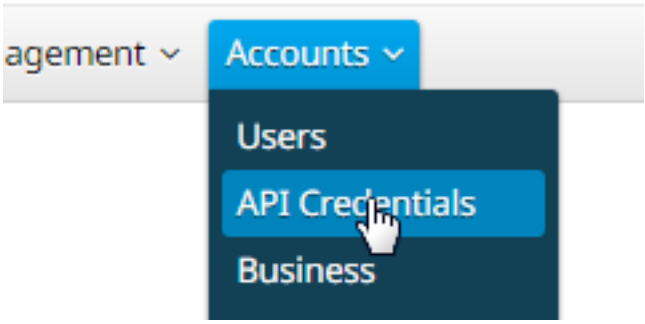
يوضح هذا المقال بعض الوظائف الأساسية ل API. تستخدم الأمثلة الواردة في هذه المقالة نقطة نهاية لنظام التشغيل Windows 7.

تمت المساهمة من قبل مهندسي ماثيو فرانكس ونزول رجب و Cisco TAC.

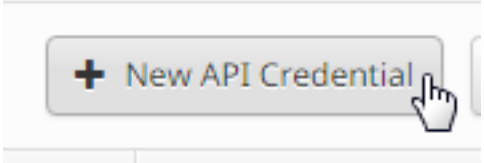
إنشاء بيانات اعتماد API وحذفها

من أجل إستخدام AMP لواجهة برمجة تطبيقات Endpoint API، يجب عليك إعداد بيانات اعتماد API. اتبع الخطوات المحددة لإنشاء بيانات اعتماد من خلال وحدة تحكم AMP.

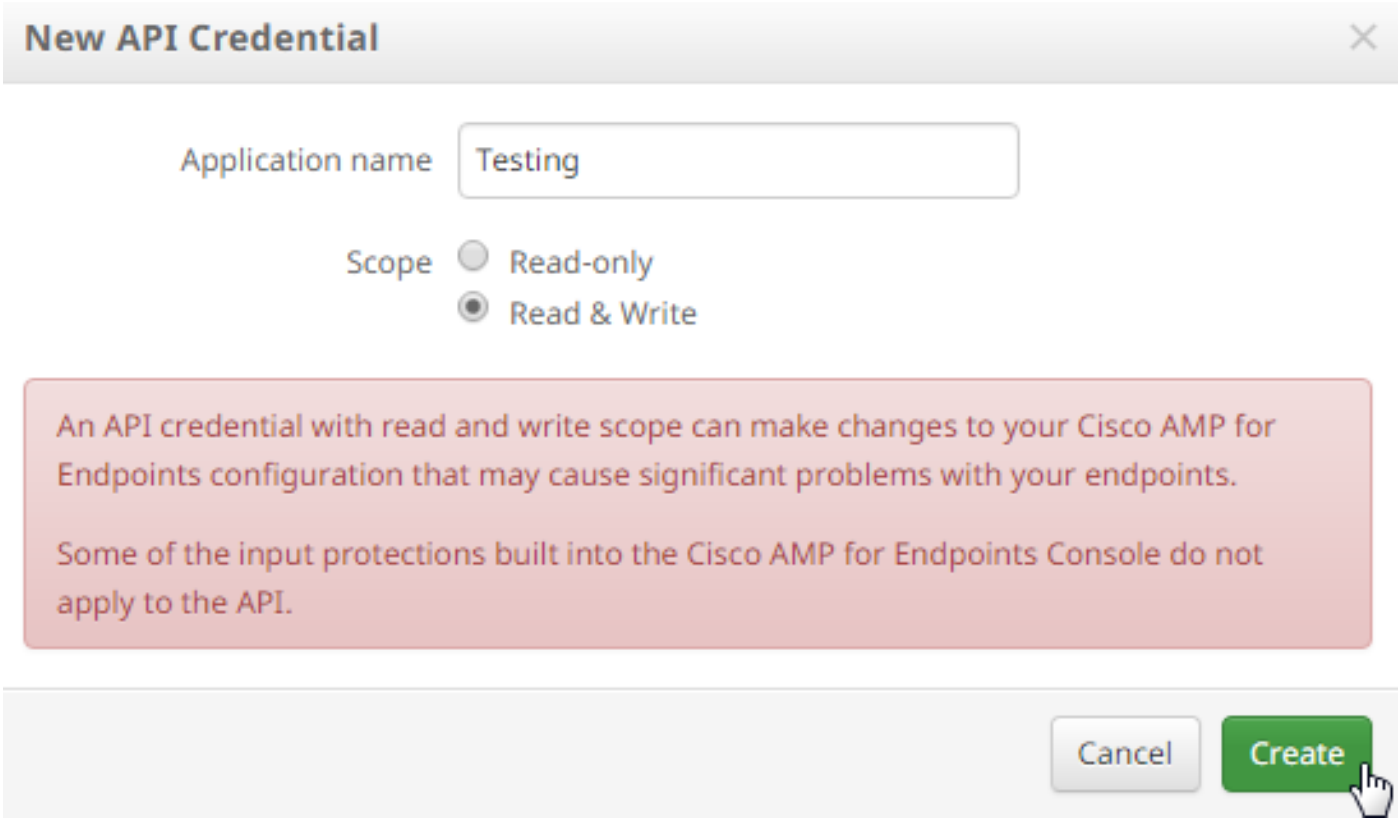
الخطوة 1: سجل الدخول إلى وحدة التحكم، وانتقل إلى **الحسابات > بيانات اعتماد واجهة برمجة التطبيقات (API).**



الخطوة 2: انقر فوق **بيانات اعتماد واجهة برمجة تطبيقات جديدة** لإنشاء مجموعة جديدة من المفاتيح.

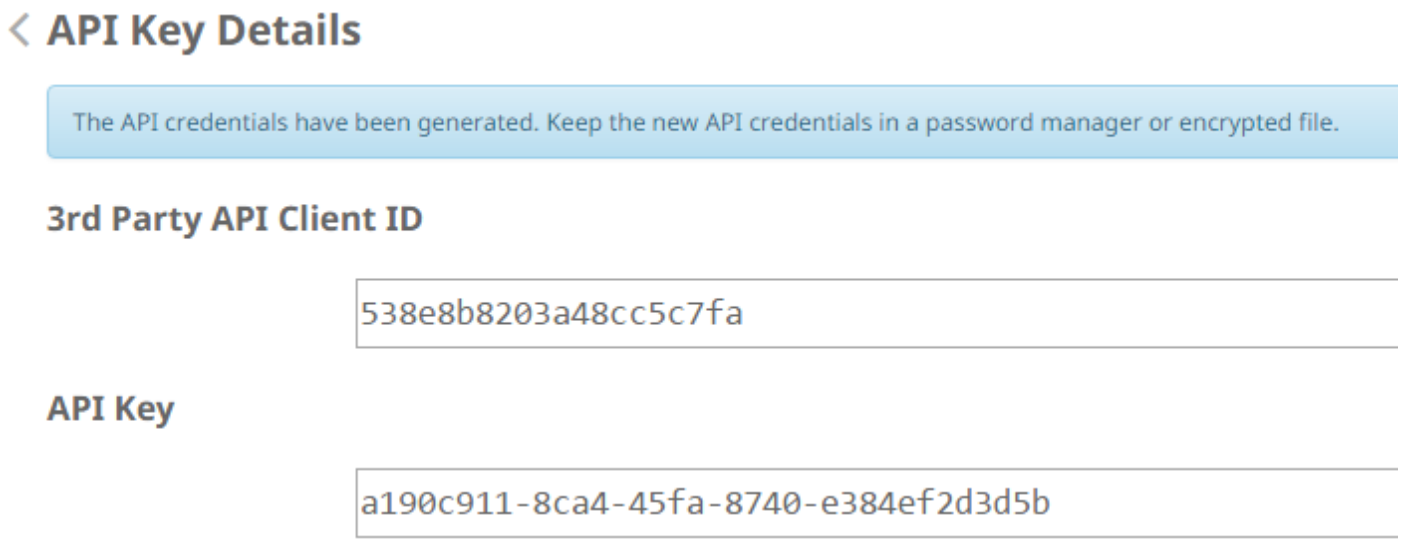


الخطوة 3: أدخل **اسم التطبيق**. حدد **نطاق** القراءة فقط أو القراءة والكتابة.



ملاحظة: يمكن أن تقوم بيانات اعتماد واجهة برمجة تطبيقات مزودة بنطاق قراءة وكتابة بإجراء تغييرات على تكوين نقاط النهاية من Cisco AMP الخاص بك قد يؤدي إلى حدوث مشاكل كبيرة في نقاط النهاية الخاصة بك. لا تنطبق بعض أوجه حماية الإدخال المضمنة في Cisco AMP لوحدة تحكم نقاط النهاية على واجهة برمجة التطبيقات.

الخطوة 4: انقر فوق الزر **إنشاء**. تظهر تفاصيل **مفتاح API**. احفظ هذه المعلومات لأن بعضها لن يكون متوفرا بعد مغادرة الشاشة.

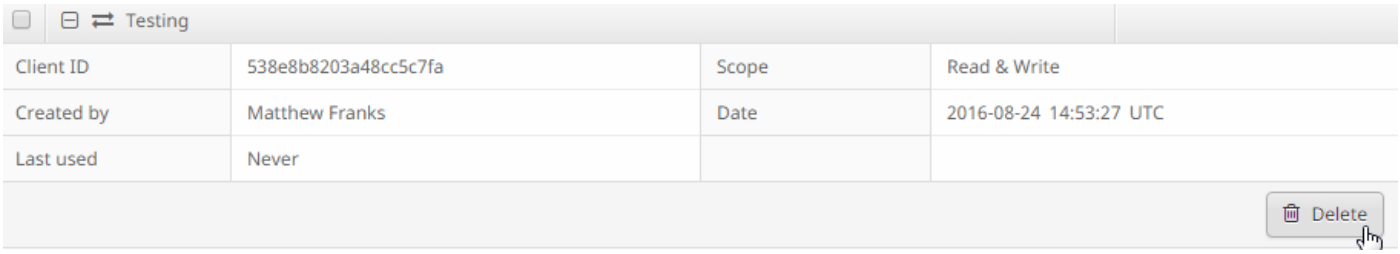


ملاحظة: ستتيح بيانات اعتماد واجهة برمجة التطبيقات (معرف عميل واجهة برمجة التطبيقات (API) ومفتاح واجهة برمجة التطبيقات (API)) للبرامج الأخرى إسترداد وتعديل AMP الخاص بك من Cisco لبيانات نقاط النهاية. وهو يعادل وظيفيا اسم مستخدم وكلمة مرور، ويجب التعامل معه على هذا النحو.

تحذير: يتم عرض بيانات اعتماد API مرة واحدة فقط. إذا فقدت بيانات الاعتماد، فعليك إنشاء بيانات اعتماد

جديدة.

قم بحذف بيانات اعتماد واجهة برمجة التطبيقات للتطبيق إذا كنت تشك في أنه قد تم أختراق بيانات الاعتماد هذه، ثم قم بإنشاء بيانات اعتماد جديدة. عند حذف بيانات اعتماد واجهة برمجة تطبيقات (API)، يتم قفل العميل الذي يستخدم البيانات القديمة، لذا قم بتحديثها باستخدام بيانات الاعتماد الجديدة.



إصدارات واجهة برمجة التطبيقات (API) والخيارات الحالية

هناك حاليا إصداران من AMP لواجهة برمجة تطبيقات Endpoints - الإصدار 0 والإصدار 1. يحتوي الإصدار 1 على وظائف إضافية مقابل الإصدار 0. هنا وثائق الإصدار 1. يمكنك سحب هذه المعلومات باستخدام الإصدار 1.

- حواسيب
- نشاط حاسوبي
- الأحداث
- أنواع الأحداث
- قوائم الملفات
- عناصر قائمة الملفات
- مجموعات
- السياسات
- الإصدارات

انقر فوق الأمر ذي الصلة في الوثيقة لترى أمثلة على إستخدامه.

نموذج وانهيار أمر API

يحتوي كل أمر API على معلومات مماثلة ويمكن أن ينقسم أساسا إلى أمر curl ويمكن أن ينظر إليه مثل هذا:

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

عندما تستخدم أمر التجعد مع خيار -o، فإنه يسمح لك بحفظ المخرجات في ملف. في هذه الحالة يكون اسم الملف هو اسم الملف filename.json "you.

تلميح: يمكن العثور على مزيد من المعلومات حول ملفات .json هنا.

الخطوة التالية في الأمر **curl** هي تعيين العنوان باستخدام بيانات اعتمادك قبل رمز @. عندما تقوم بإنشاء بيانات اعتماد واجهة برمجة التطبيقات، فأنت تعرف معرف العميل و APIKey، وبالتالي فإن هذا القسم من الأمر سيشبه الارتباط المعطى أدناه.

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

قم بإضافة رقم الإصدار وما تريد القيام به. على سبيل المثال، قم بتشغيل خيارات GET /v1/computers.يبدو الأمر الكامل كما يلي:

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

بعد تشغيل الأمر، يجب أن ترى ملف **computers.json** الذي تم تنزيله إلى الدليل حيث بدأت الأمر.

```
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
```

ملاحظة: يتوفر Curl [عبر الإنترنت]() ويتم تجميعه للعديد من الأنظمة الأساسية التي تتضمن نظام التشغيل Windows (بشكل عام سترغب في إستخدام Win32 - الإصدار العام).

عندما تقوم بفتح الملف سترى كل البيانات في سطر واحد. إذا كنت ترغب في رؤية هذا بالتنسيق المناسب، يمكنك تثبيت ملحق مستعرض لتكوينه ك JSON وفتح الملف في مستعرض. يعرض هذا معلومات لأجهزة الكمبيوتر التي يمكنك إستخدامها كيفما تشاء، مثل:

hostname، connector_guid، نشط، إرتباطات، internal_ips، operating_system، connector_version، guid، network_address، group_guid، external_ip، النهج، واسم النهج.


```
{
"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
{
```


الآن وقد رأيت مثالا أساسيا في العمل، يمكنك إستخدام خيارات الأوامر المختلفة لسحب ومعالجة البيانات في بيئتك.

معلومات ذات صلة

- وثائق واجهة برمجة التطبيقات (API) لنقاط النهاية من Cisco AMP
الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).