

终端API的Cisco AMP概述

Contents

[Introduction](#)

[生成并且删除API证件](#)

[API版本和当前选项](#)

[API命令细分和示例](#)

[Related Information](#)

简介

本文描述关于Cisco提前Malware保护(AMP)终端的。终端的Cisco AMP附有Application Programming Interface (API)。它允许您拉从一AMP的数据终端配置的，并且操作他们，当必要时。

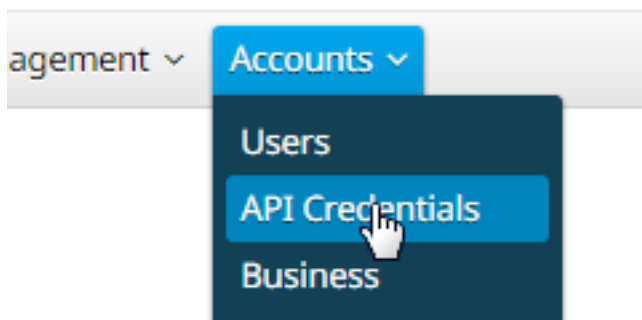
此条款展示API的一些基本功能。在此条款的示例使用Windows 7终端。

贡献由马修直率、Nazmul Rajib和Cisco TAC工程师。

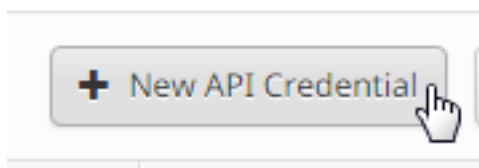
生成并且删除API证件

为了使用AMP终端API，您必须设置API凭证。遵从特定步骤通过AMP控制台创建凭证。

步骤 1：日志到控制台里，和连接对帐户> API证件。



步骤 2：点击新的API凭证创建新的一套键。



步骤 3：提供一个应用程序名称。选择范围只读或读&写道。

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.

Note:与读的一API凭证和写范围能做对您的Cisco AMP的变动也许引起严重问题由于您的终端的终端配置的。某些输入保护被建立到终端控制台的Cisco AMP不适用于API。

步骤 4 : 点击**创建按钮**。API键详细资料出现。请保存此信息，因为一些它在留下屏幕以后不会是可用的。

< 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

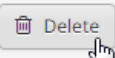
API Key

Note:API证件(Api client ID & API键)将允许其他程序检索和修改您的终端数据的Cisco AMP。它是功能上相同的与用户名和密码，并且应该同样地对待。

警告 : 您的API证件一次只显示。如果丢失证件，您必须生成新的。

请删除应用程序的API证件，如果怀疑他们折衷了，并且创建新的。当您删除API凭证时，锁定使用老部分的客户端，如此更新他们与新的证件。

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



API版本和当前选项

当前有AMP的两个版本终端API的-版本0和版本1。版本1有其他功能与版本0。版本1的文档[在这里](#)。您能拉此信息withn使用版本1。

- 计算机
- 计算机活动
- [事件](#)
- 事件类型
- 文件列表
- 文件列表项目
- 组
- 策略
- 版本

点击在本文的相关命令参见其使用方法示例。

API发出命令细分和示例

每个API命令包含相似的信息，并且根本划分到卷毛命令，并且可以看上去象这个：

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

当您以使用卷毛命令-o选项，允许您保存输出到文件。在这种情况下文件名是“yourfilename.json”。

提示：可以找到关于.json文件的更多信息[这里](#)。

在**卷毛**命令的下一步是设置与您的证件的地址在@符号前。当您generatie API证件，您认识clientID和APIKey，因此命令的此部分将类似于如下所示的链路。

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

添加版本号，并且什么您希望执行。对于此示例，请运行[GET /v1/computers](#)选项。完全命令如下所示：

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

在您运行命令后，您应该看到computers.json文件下载到您起动命令的目录。

```
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         0         0         0  --:--:--  0:00:02  --:--:--    0
```

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

Note:包括Windows的卷毛是[线上可以得到](#)和编译为大量平台(您通常将要使用Win32 –通用的版本)。

当您打开文件您将看到所有在单个线路的数据。 如果在其相应的格式希望发现此，您能安装插件的浏览器格式化它作为JSON和打开在浏览器的文件。 这显示您的计算机信息您能使用然而您将想要，例如：

connector_guid、主机名-，激活、链路、connector_version、operating_system、internal_ips、external_ip、group_guid、network_addresses、策略guid和策略名称。

```
{
  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"
}
```

即然您参见在动作的基本示例，您在您的环境里能使用各种命令选项拉和操作数据。

Related Information

- [终端API文档的Cisco AMP](#)

[Technical Support & Documentation - Cisco Systems](#)