了解安全终端API概述

目录

[问题](#)
[分辨率](#)
[环境](#)
[API命令细分和示例](#)
[相关内容](#)

问题

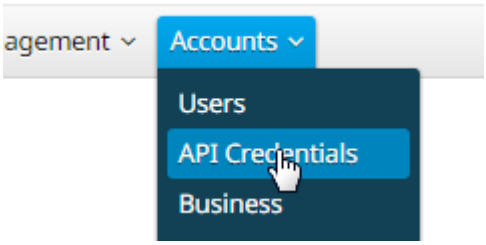
本文档介绍思科安全终端(SE)API使用情况。

分辨率

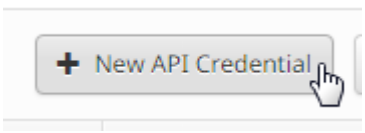
要使用SE API，请在SE控制台中创建API凭证。

本文中的示例使用Windows 7终端。

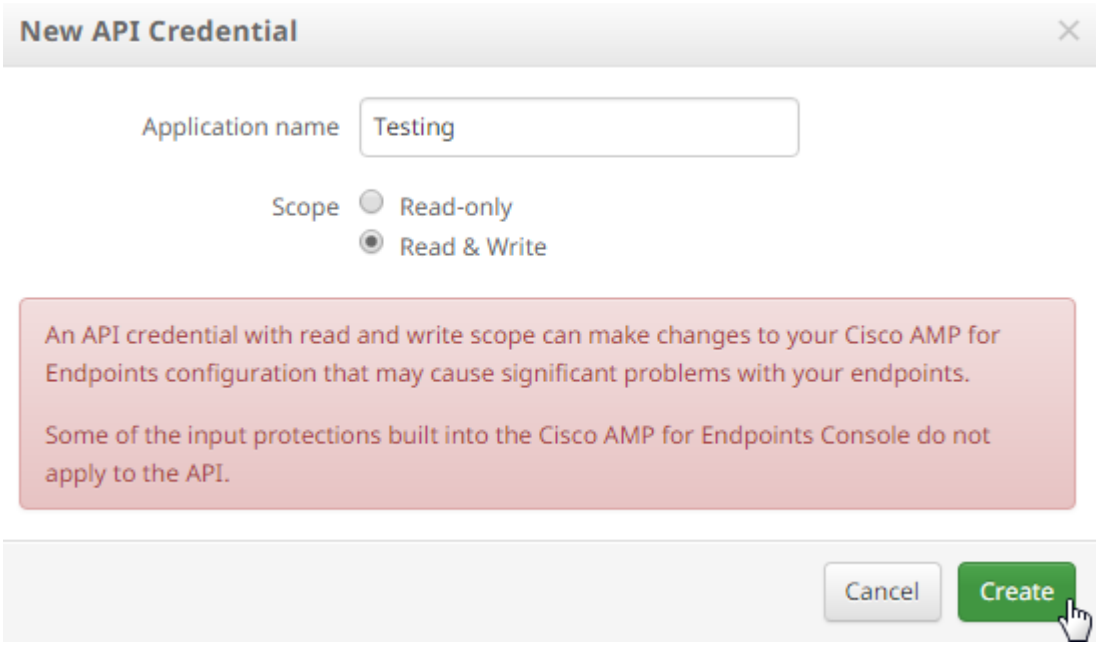
1.登录到控制台并导航到帐户> API凭证。



1.单击New API Credential以创建一组新的密钥。

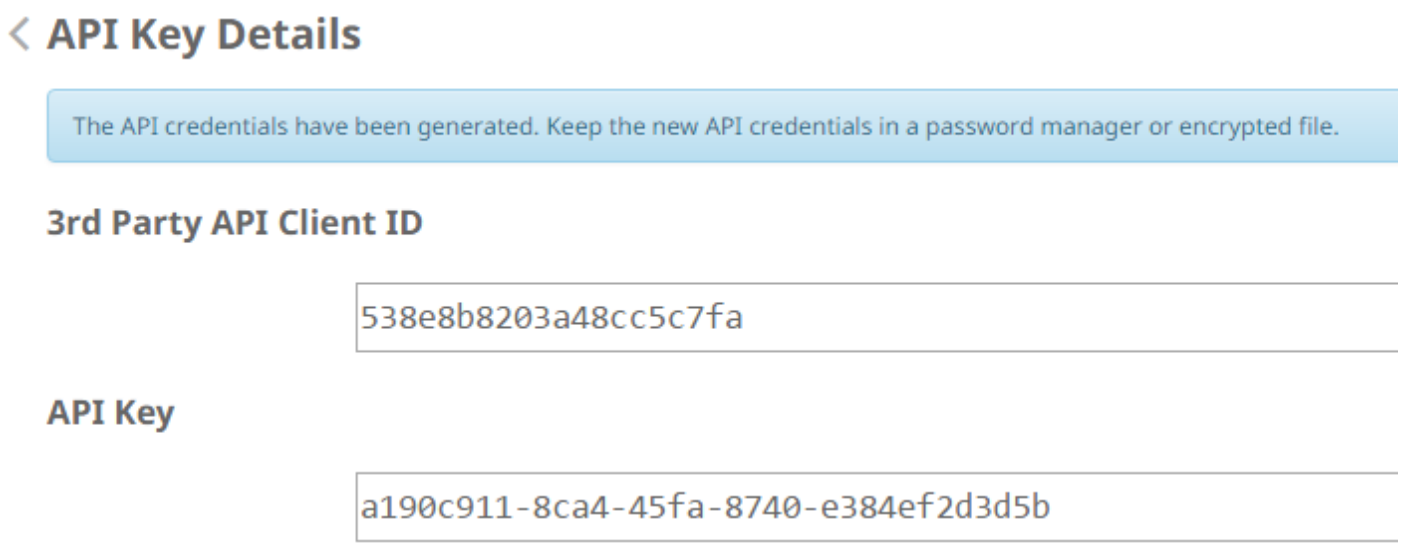


2.输入应用程序名称。选择Scope（只读范围）或Read & Write（读写）。



注意：具有读取和写入范围的API凭证可以更改您的Cisco SE配置，这可能导致终端出现严重问题。 Cisco SE控制台内置的一些输入保护不适用于API。

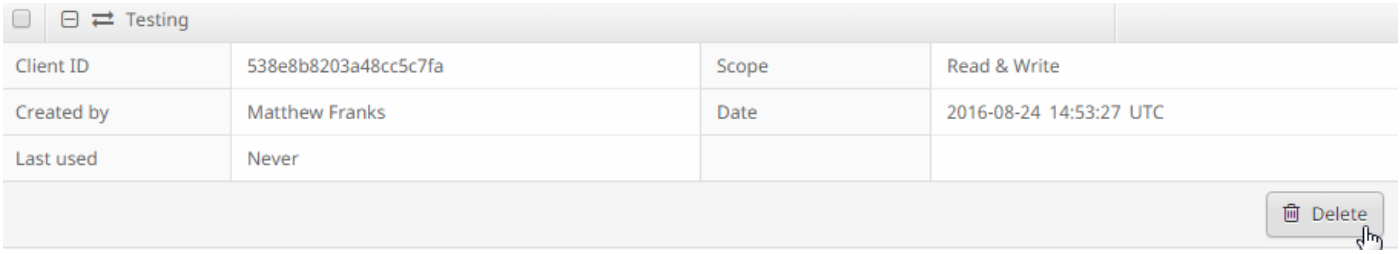
3.单击创建按钮。系统将显示API Key Details页面。保存此信息，因为某些信息在离开屏幕后不可用。



注意：API凭证（API客户端ID和API密钥）允许其他程序检索和修改您的思科SE数据。它在功能上等同于用户名和密码，必须按此方式处理。

警告：您的API凭证只显示一次。如果丢失凭证，您必须生成新凭证。

如果您怀疑某个应用的API凭证受到危害，请将其删除，并创建一个新凭证。 删除API凭证时，它会锁定使用旧凭证的客户端，因此使用新凭证更新它们。



环境

- 测试的终端：Windows 7终结点。
- 产品:思科SE
- 接入:具有创建和删除API凭证权限的控制台访问。
- API:SE API版本3、版本1和版本0（示例使用版本1）。
- 客户端工具:系统上安装的curl，用于运行API请求。

SE API目前有三个版本：版本3、版本1和版本0。与版本1和版本0相比，版本3提供其他功能。[版本3 API文档可通过此链接获](#)得。使用版本3可检索此信息：

- 审核日志
- 设备控制
- 设备
- 排除
- 主机防火墙
- IOC
- MSSP
- 组织
- 策略
- 计算机
- 漏洞

单击文档中的相关命令以查看其用法示例。

API命令细分和示例

每个API命令都包含类似信息，并分解为如下所示的curl命令：

```
curl -o yourfilename.json https://client_id:api_key@api.example.com/v1/whatyouwanttodo
```

当您使用带有 — o选项的curl命令时，它允许您将输出保存到文件。在本例中，文件名为“yourfilename.json”。

提示：有关.json文件的更多信息，请访问JSON网站。

curl命令的下一部分在@符号前指定凭证。生成API凭证后，在URL的此部分使用API客户端ID和API密钥。

```
https://client_id:api_key@
```

添加版本号和要执行的操作。在本例中，运行GET /v1/computers。完整命令如下所示：

```
curl -o computers.json https://client_id:api_key@api.example.com/v1/computers
```

运行该命令后，computers.json文件会出现在发出该命令的目录中。

```
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
```

注意：Curl可在线获得并编译用于许多平台，包括Windows（通常您想要使用Win32 — 通用版本）。

打开文件时，所有数据都显示在一行上。要在格式化布局中查看该文件，请安装一个格式为JSON的浏览器插件，然后在浏览器中打开该文件。此输出显示计算机的信息，例如：

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

<#root>

```
{
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

```
: "host.example.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

```
: "192.0.2.10",

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"
}
}
]
}
```


此示例显示一个基本API请求。现在，您可以使用其他命令选项来检索和修改环境中的数据。

相关内容

- 面向终端的思科AMP API文档
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。