通过API方法以CSV格式从CSM提取ACL

目录

简介

本文档介绍如何通过CSM API方法提取由思科安全管理器(CSM)管理的设备的以逗号分隔值(CSV)格式的访问控制列表(ACL)。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全管理器(CSM)
- CSM API
- API基础知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CSM服务器
- CSM API许可证
  ```
  Product Name: L-CSMPR-API
  Product Description: L-CSMPR-API : Cisco Security Manager Pro - License to enable API Access
  ```
- 由CSM管理的自适应安全设备(ASA)
- API客户端。您可以使用cURL、Python或Postman。本文演示了Postman的整个过程。 必须关闭CSM客户端应用。如果CSM客户端应用已打开，则必须由使用API方法的用户以外的用户使用。否则，API返回错误。有关使用API功能的其他必备条件，您可以使用下一个指南。[API必](#)

[备条件](#)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

思科安全管理器(CSM)具有一些用于受管设备配置的功能，需要通过API实施。

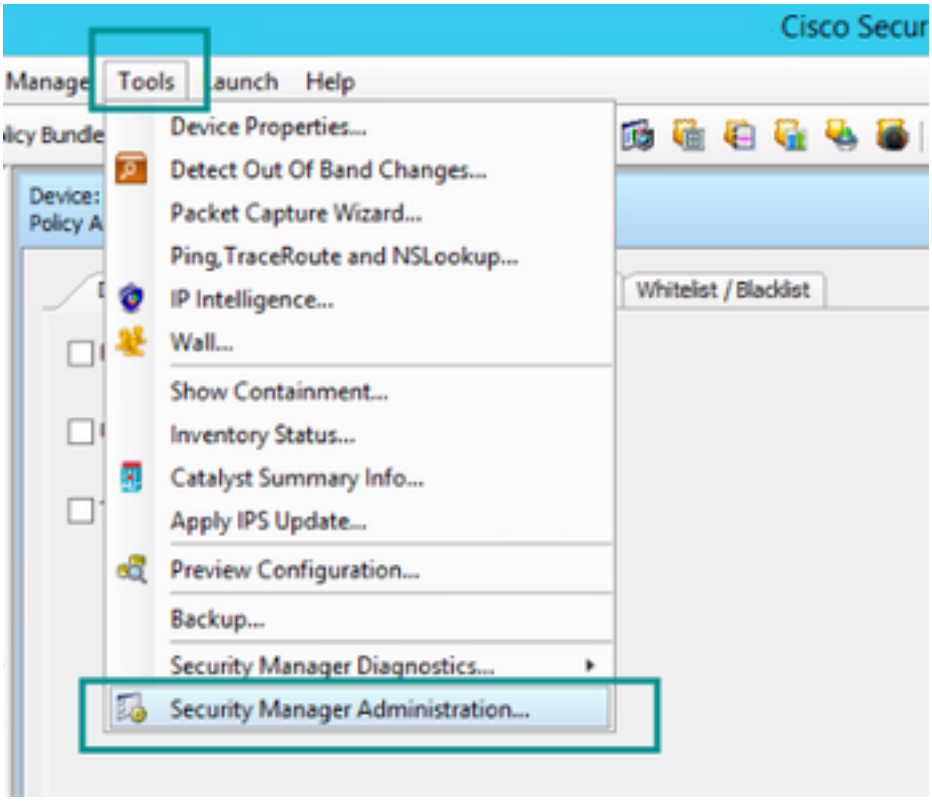
其中一个配置选项是提取在CSM管理的每台设备中配置的访问控制列表(ACL)列表的方法。到目前为止，使用CSM API是实现这一要求的唯一方法。

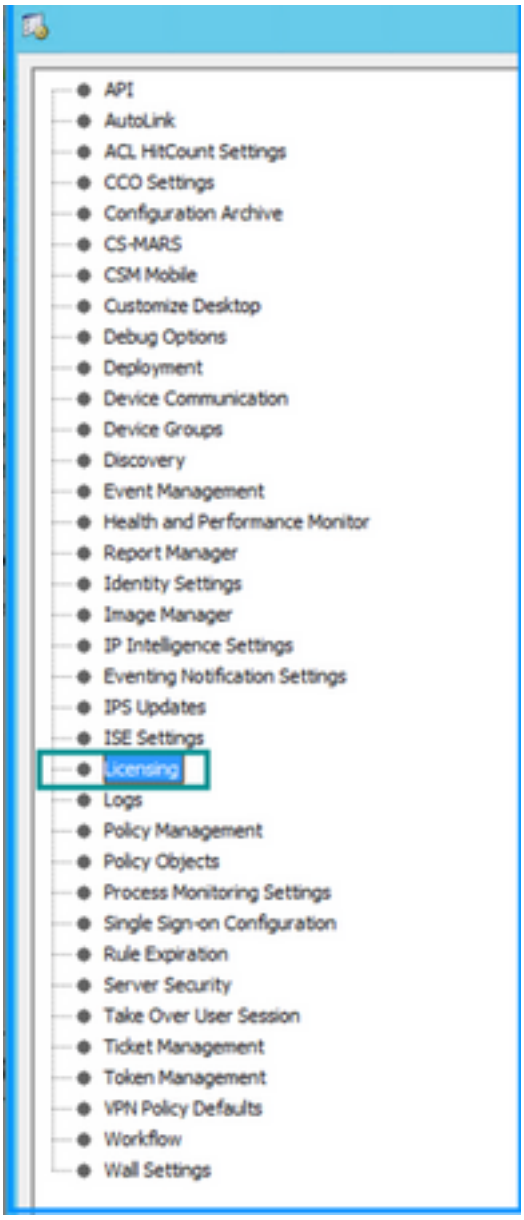
出于这些目的，Postman用作API客户端和CSM版本4.19 SP1、ASA 5515版本9.8(4)。

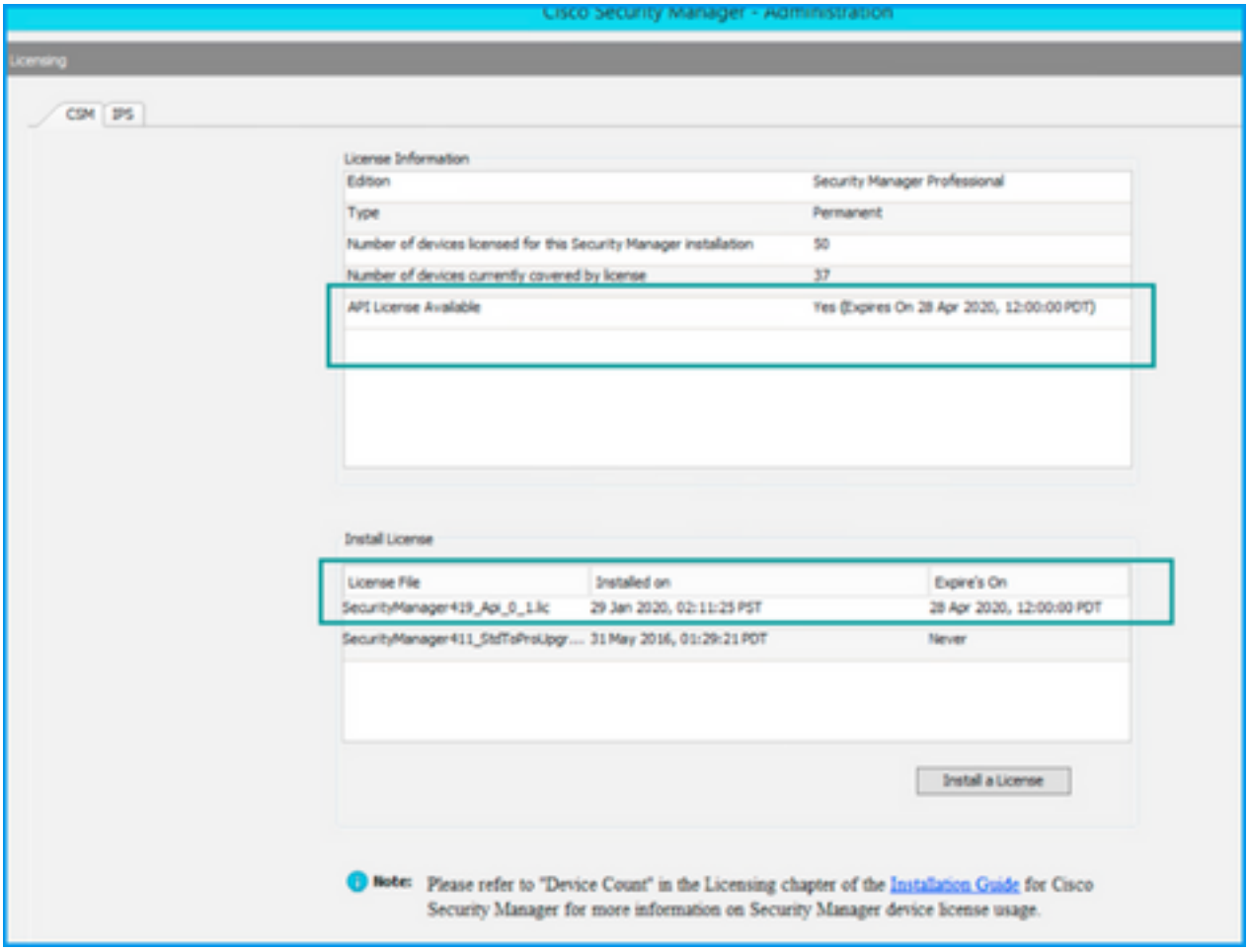
网络图

CSM API许可证安装/验证

CSM API是许可功能，您可以验证CSM是否具有API许可证，在CSM客户端中，导航至**Tools > Security Manager Administration > Licensing**页面以确认您已安装许可证。


Cisco Secur
Manage
Tools
Launch
Help
Device Properties...
Detect Out Of Band Changes...
Packet Capture Wizard...
Ping,TraceRoute and NSLookup...
IP Intelligence...
Wall...
Show Containment...
Inventory Status...
Catalyst Summary Info...
Apply IPS Update...
Preview Configuration...
Backup...
Security Manager Diagnostics...
Security Manager Administration...
Whitelist / Blacklist

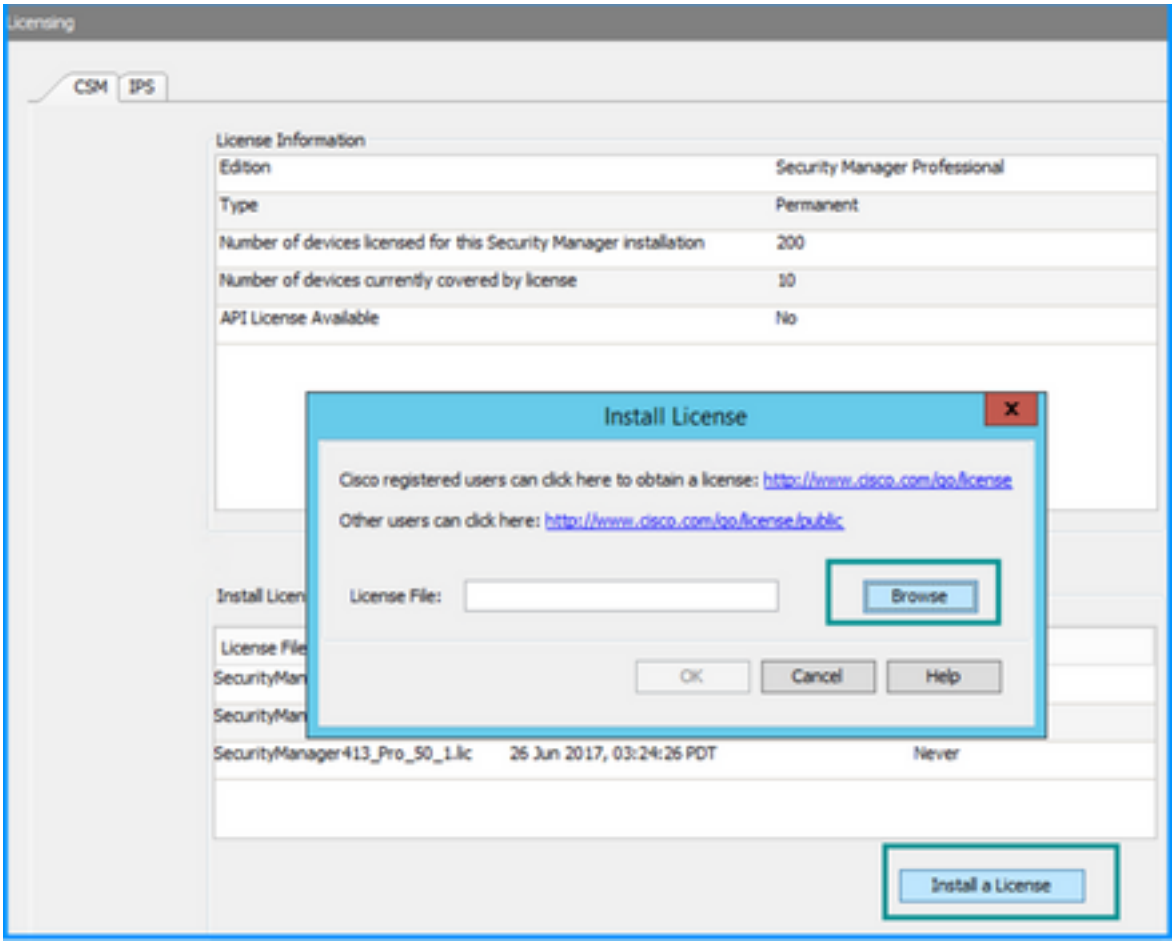

API
AutoLink
ACL HitCount Settings
CCO Settings
Configuration Archive
CS-MARS
CSM Mobile
Customize Desktop
Debug Options
Deployment
Device Communication
Device Groups
Discovery
Event Management
Health and Performance Monitor
Report Manager
Identity Settings
Image Manager
IP Intelligence Settings
Eventing Notification Settings
IPS Updates
ISE Settings
Licensing
Logs
Policy Management
Policy Objects
Process Monitoring Settings
Single Sign-on Configuration
Rule Expiration
Server Security
Take Over User Session
Ticket Management
Token Management
VPN Policy Defaults
Workflow
Wall Settings

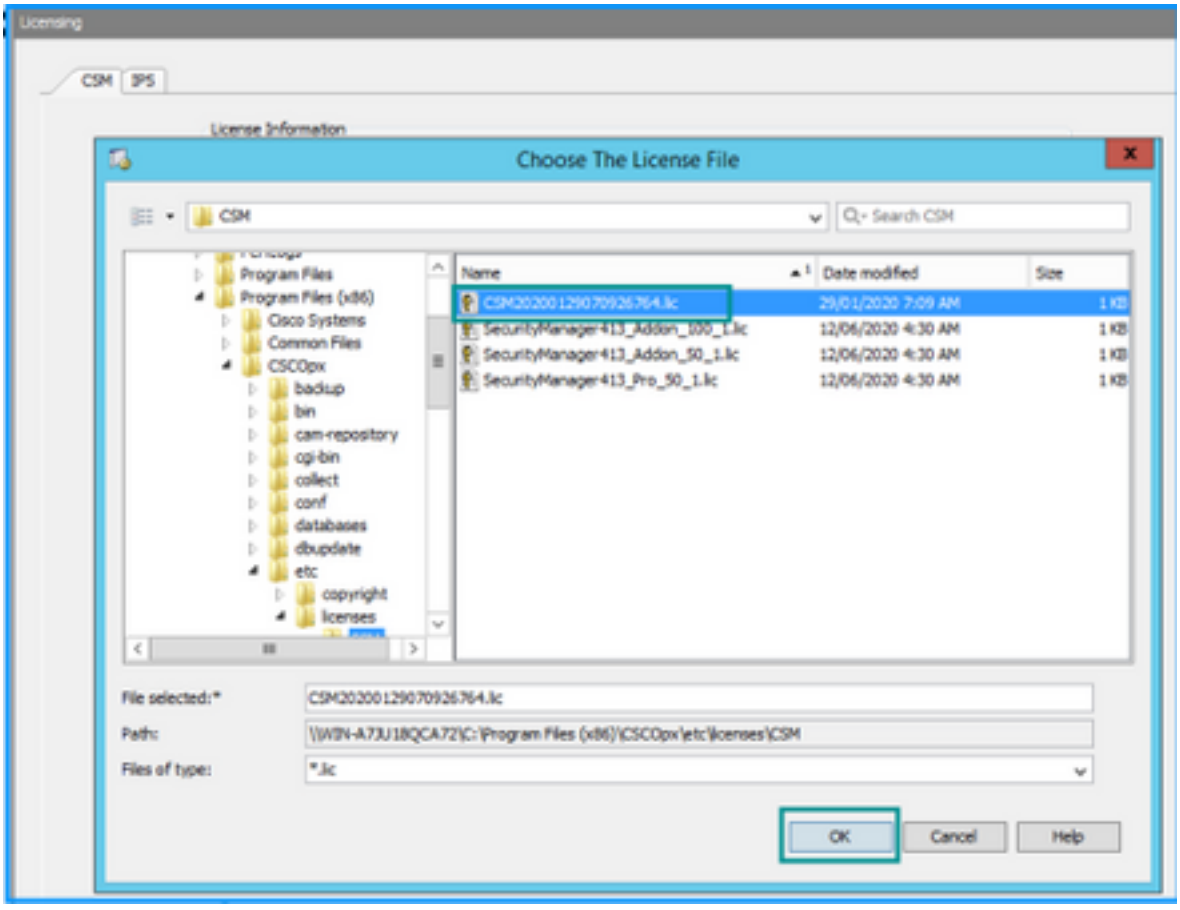


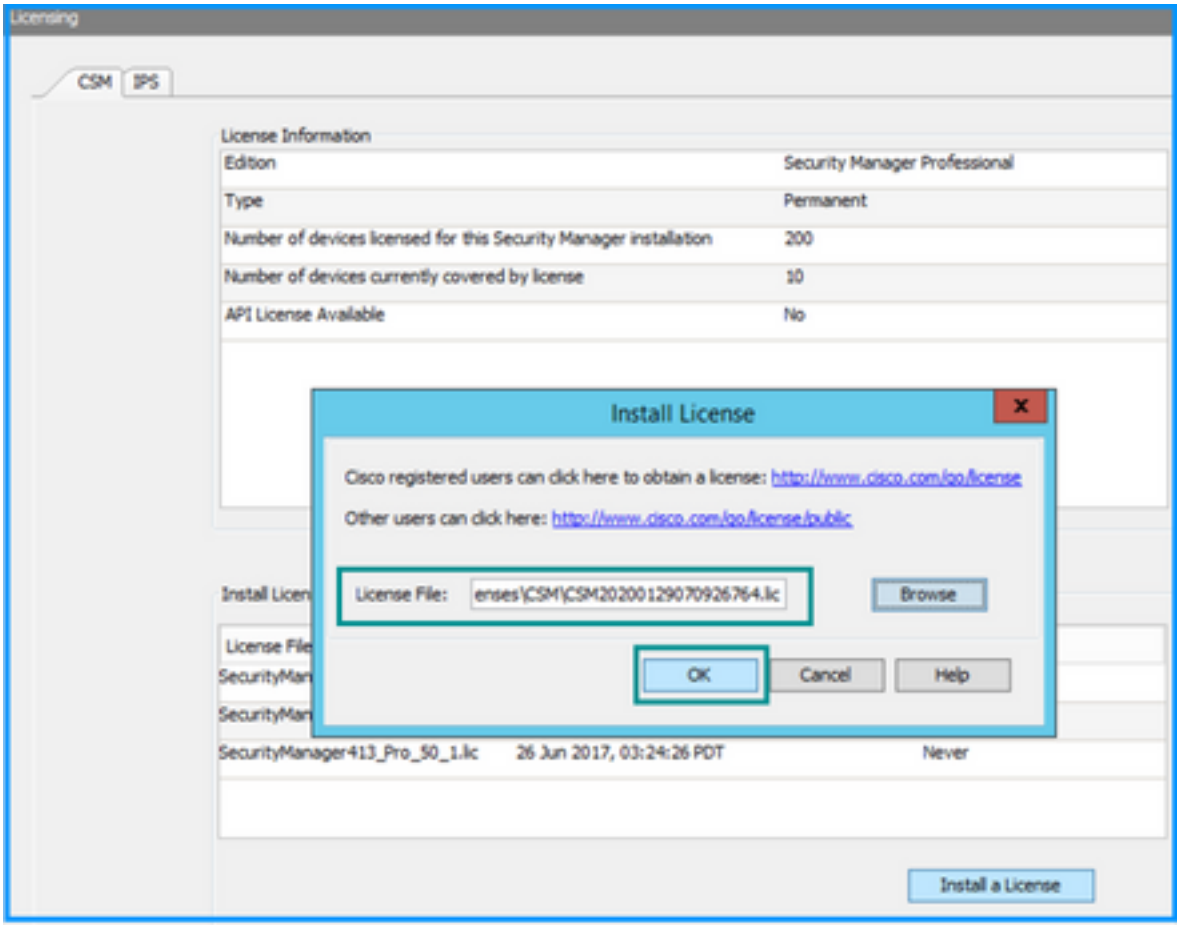
如果未应用API许可证，但您已拥有可安装许可证的.lic文件，请单击**Install a License**按钮，您必须将许可证文件存储在CSM服务器所在的同一磁盘下。

要安装更新的思科安全管理器许可证，请执行以下步骤：

步骤1.从您收到的邮件中保存随附的许可证文件(.lic)到文件系统。
步骤2.将保存的许可证文件复制到Cisco Security Manager服务器文件系统上的已知位置。
步骤3.启动Cisco Security Manager客户端。
步骤4.导航至**Tools->Security Manager Administration...**
步骤5.从“思科安全管**理器 — 管理”窗口**中，选择许**可**
步骤6.单击“安**装许可证”**按钮。
步骤7.从“安装许可**证”对**话框中，选择“浏**览”**按钮。
步骤8.导航到并选择Cisco Security Manager服务器文件系统上保存的许可证文件，然后选择“确定”**按**钮。
步骤9.在“安装许**可证”**对话框中，单击“**确定”**按钮。
步骤10.确认显示的“许可证摘要”信息，然后单击“关**闭”**按钮。


Licensing
CSM
IPS
License Information
Edition
Security Manager Professional
Type
Permanent
Number of devices licensed for this Security Manager installation
200
Number of devices currently covered by license
10
API License Available
No
Install License
Cisco registered users can click here to obtain a license: http://www.cisco.com/go/license
Other users can click here: http://www.cisco.com/go/license/public
License File:
Browse
OK
Cancel
Help
SecurityManager413_Pro_50_1.lic
26 Jun 2017, 03:24:26 PDT
Never
Install a License


Licensing
CSM
IPS
License Information
Choose The License File
CSM
Search CSM
Program Files
Program Files (x86)
Cisco Systems
Common Files
CSCOpx
backup
bin
cam-repository
cgi-bin
collect
conf
databases
dbupdate
etc
copyright
licenses
Name
Date modified
Size
CSM20200129070926764.lic
29/01/2020 7:09 AM
1 KB
SecurityManager413_Addon_100_1.lic
12/06/2020 4:30 AM
1 KB
SecurityManager413_Addon_50_1.lic
12/06/2020 4:30 AM
1 KB
SecurityManager413_Pro_50_1.lic
12/06/2020 4:30 AM
1 KB
File selected:*
CSM20200129070926764.lic
Path:
\\WIN-A73J18QCA72\C:\Program Files (x86)\CSCOpx\etc\licenses\CSM
Files of type:
*.lic
OK
Cancel
Help



API许可证只能应用于为CSM专业版许可的服务器。许可证无法应用到运行许可证标准版的CSM。
API许可证要求

配置步骤

API客户端设置

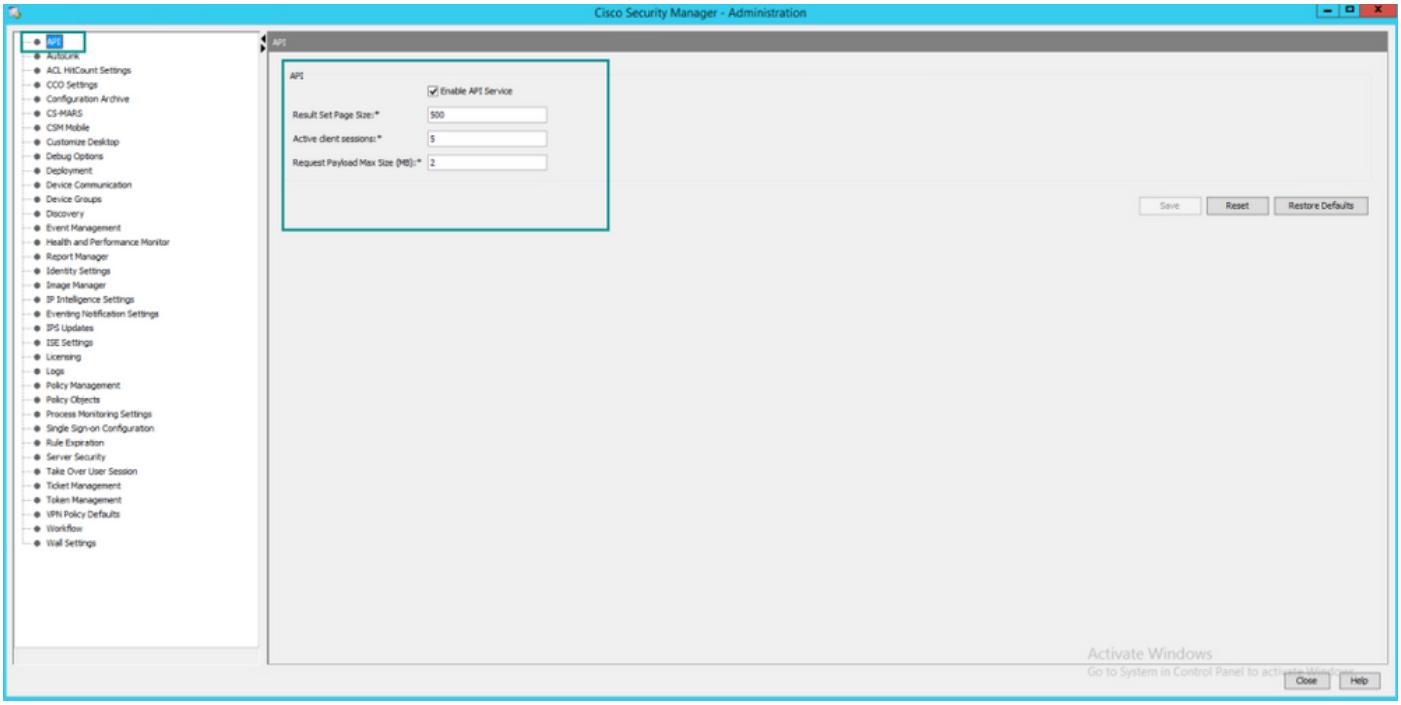
如果使用Postman，则需要配置一些设置，这取决于每个API客户端，但必须类似。

- 代理已禁用
- SSL验证 — 关闭

CSM设置

- 已启用API。在“工**具”>“安全管理器管理”>“API”**下

API设置



使用CSM API

您需要在API客户端中配置以下两个调用：

1.登录方法

2.获取ACL值

供整个流程参考：

本实验中使用的CSM访问详细信息：

CSM主机名（IP地址）：**192.168.66.116**。在API中，我们在URL中使用主机名。

用户名：**admin**

密码：**管理123**

登录方法

在对其他服务调用任何其他方法之前，必须先调用此方法。

CSM API指南：方法登录

请求

1. HTTP方法：**POST**

2.URL:https://<hostname>/nbi/**login**

3.正文：

其中：

username：与会话关联的CSM客户端用户名

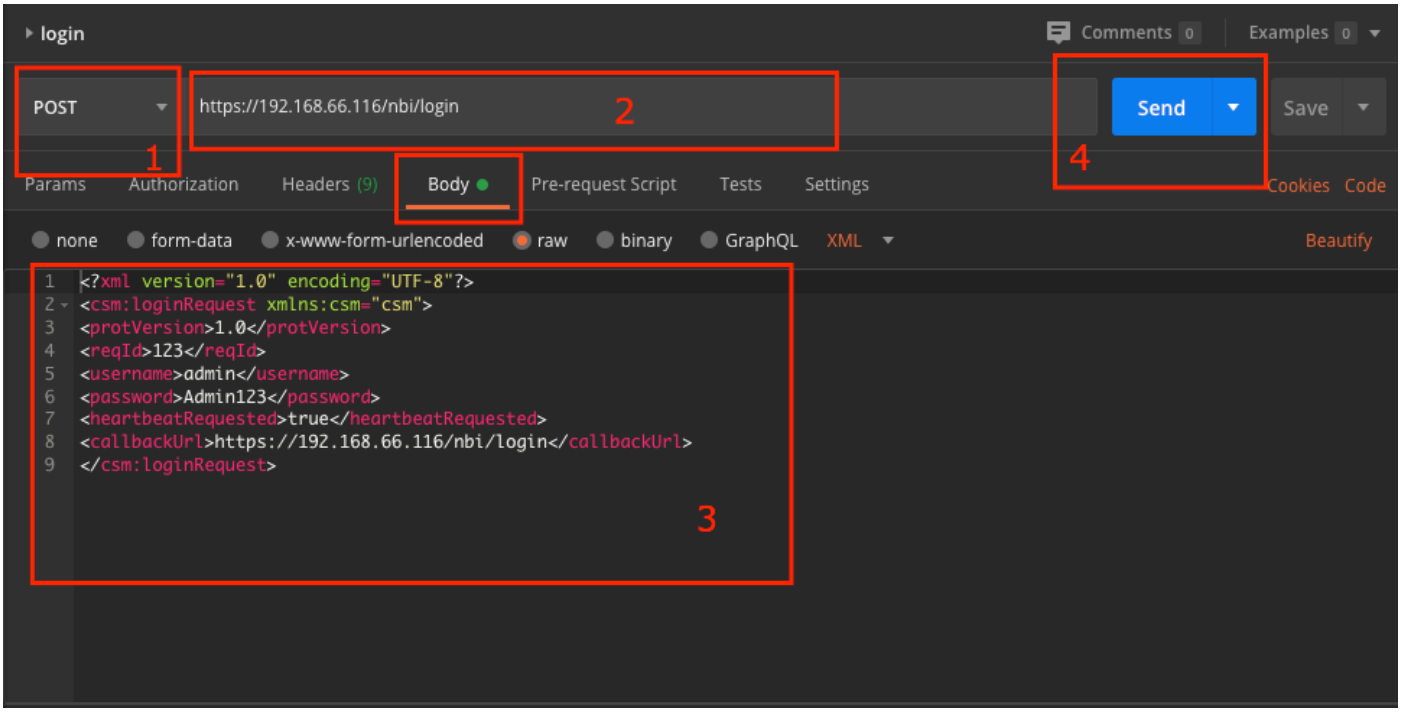
密码：与会话关联的CSM客户端密码。

reqId:此属性唯一标识客户端完成的请求，该值由CSM服务器在关联的响应中回显。它可设置为用户希望用作标识符的任何内容。

heartbeatRequested:此属性可以选择性地定义。如果属性设置为true，则CSM客户端从CSM服务器接收心跳回调。服务器尝试以接近（非活动超时）/ 2分钟的频率ping客户端。如果客户端不响应心跳，则API会在下一个间隔内重试心跳。如果心跳成功，则会重置会话非活动超时。

回叫URL:CSM服务器进行回调的URL。如果heartbeatRequested为true，则需要指定此值。仅允许基于HTTPS的回叫URL

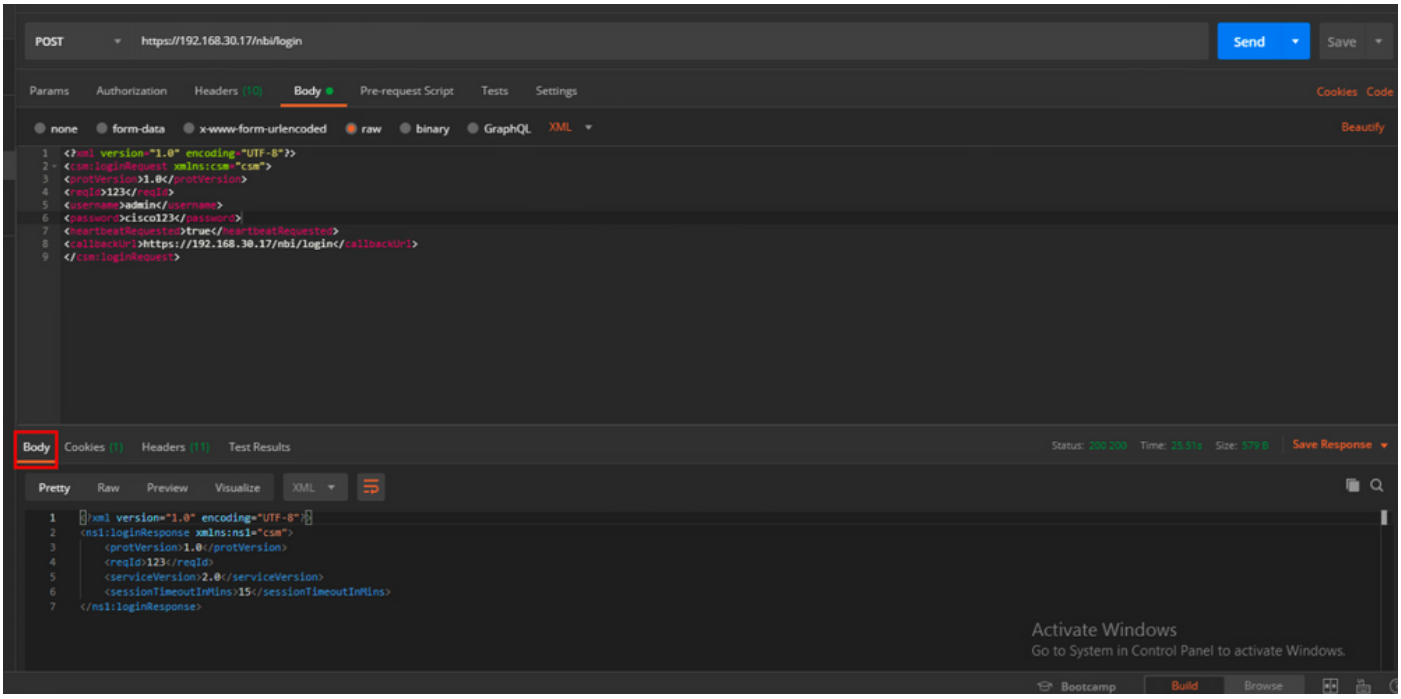
4.发送



选择要查看的原始选项，如本例所示。

回复

登录API验证用户凭证并返回会话令牌作为安全Cookie。会话值存储在asCookie**键下**，您必须将此值保存**为Cookie值**。



获取ACL规则

方法execDeviceReadOnlyCLICmds。通过此方法可以执行的一组命令是只读命令，例如提供关于特定设备操作的附加信息的统计信息、监控命令。

《CSM API用户指南》中的方法详细信息

请求

1. HTTP方法：**POST**

2.URL:https://hostname/nbi/utilservice/execDeviceReadOnlyCLICmds

3. HTTP报头：登录方法返回的用于标识身份验证会话的Cookie。

输入**asCookie**值，以前从“方法登录”中获取。

密钥:输入“asCookie”

值：获取的输入值。

单击复选框以启用它。

4.正文：

注意：以上XML正文可用于执行任何“show”命令，例如：“show run all”、“show run object”、“show run nat”等。

XML“<deviceReadOnlyCLICmd>”元素表示“<cmd>”和“<argument>”中指定的命令必须为只读。

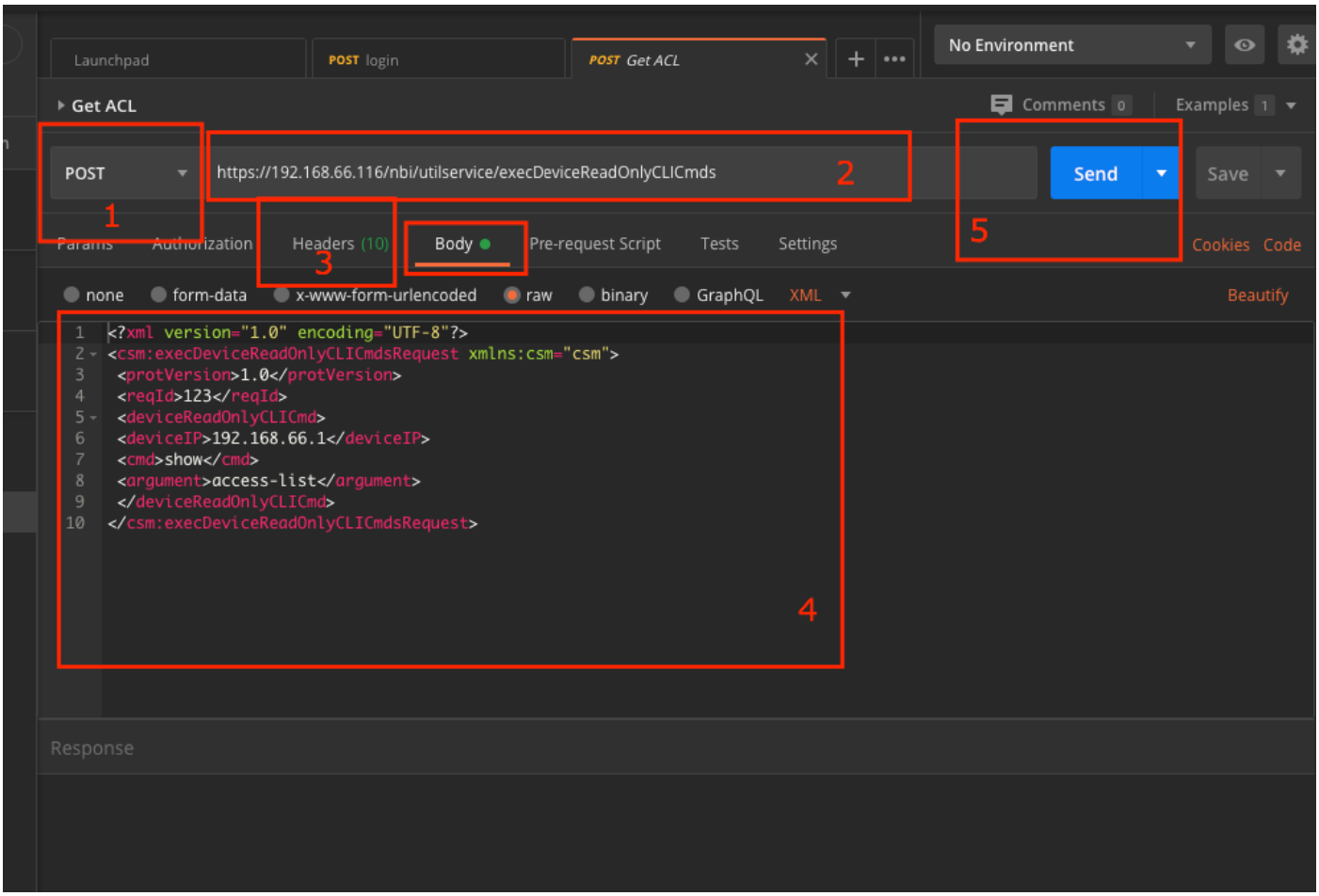
其中：

设备IP:必须对其执行命令的设备IP地址。

cmd:固定命**令“show”。**正则表达式允许混合大小写[sS][hH][oO][wW]

参数:show命令参数。例如“run”显示设备的运行配置或“access-list”**显示访问列**表详细信息。

5.发送

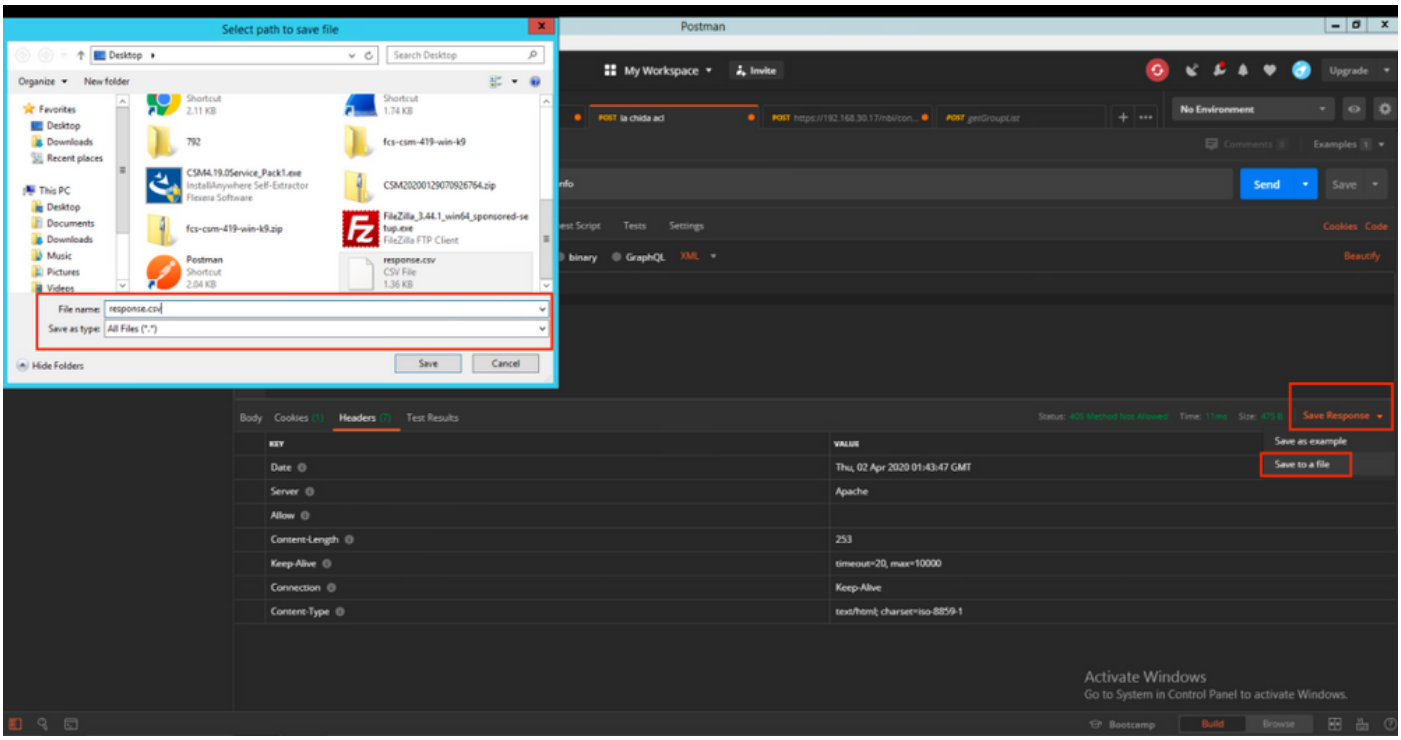


回复

```
<?xml version="1.0" encoding="UTF-8"?>
<ns1:execDeviceReadOnlyCLICmdsResponse xmlns:ns1="csm">
    <protVersion>1.0</protVersion>
    <reqId>123</reqId>
    <deviceCmdResult>
        <deviceIP>192.168.30.2</deviceIP>
        <deviceGID>00000000-0000-0000-0005-360119185746</deviceGID>
        <deviceName>asa.cisco.com</deviceName>
        <result>ok</result>
        <resultContent>access-list cached ACL log flows: total0, denied 0 (deny-flow-max 4096) alert-interval 300 access-list inside; 1 elements; name hash: 0x45467dcb access-list
            inside line 1 extended permit ip any any (hitcnt=8114506) 0x062c4905 access-list backbone; 1 elements;...</resultContent>
    </deviceCmdResult>
</ns1:execDeviceReadOnlyCLICmdsResponse>
```

验证

您可以选择将响应另存为文件。导航至**保存响应>保存到文件。**然后选择文件位置并将其另存为.csv类型。



然后，您必须能够打开此.csv文件，例如，使用Excel应用程序。从.csv文件类型中，可将输出另存为其他文件类型，如PDF、TXT等。

故障排除

使用API可能的故障响应。

1.未安装API许可证。

原因：API许可证已过期、未安装或未启用。

可能的解决方案:在“工具”>“安全管理器管理”>**“许可”页面下验证许可证的到期日期**

验证API功能是否在“工具”(Tools)**>“安全管理器管理”**(Security Manager Administration)**>“API”**(API)**下启用**

确认本指南上**面的“CSM API许可证安**装/验证”部分的设置。

2. API登录的CSM IP地址使用错误。

原因：CSM服务器的IP地址在API调用的URL中错误。

可能的解决方案:在API客户端的URL中验证主机名是CSM服务器的正确IP地址。

URL:https:// **<hostname>**/nbi/login

3.错误的ASA IP地址。

原因：<deviceIP></deviceIP>标签之间的正文上定义的IP地址不能正确。

可能的解决方案:确认正文语法中定义了正确的设备IP地址。

4.没有与防火墙的连接。

原因：设备与CSM无连接

可能的解决方案:从CSM服务器运行测试连接并排除与设备的进一步连接故障。

有关更多错误代码和说明，请在下一链接的《思科安全管理器API规范指南》中找到更多详细信息。