通過API方法從CSM提取CSV格式的ACL

目錄

簡介

本檔案介紹如何透過CSM API方法提取由思科安全管理器(CSM)管理的裝置的存取控制清單(ACL)(以逗號分隔值(CSV)格式)。

必要條件

需求

思科建議您瞭解以下主題：

- 思科安全管理員(CSM)
- CSM API
- API基礎知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- CSM伺服器
- CSM API許可證
  ```
  Product Name: L-CSMPR-API
  Product Description: L-CSMPR-API : Cisco Security Manager Pro - License to enable API Access
  ```
- 由CSM管理的自適應安全裝置(ASA)
- API客戶端。您可以使用cURL、Python或Postman。本文展示了Postman的整個過程。 必須關閉CSM客戶端應用程式。如果CSM客戶端應用程式處於開啟狀態，則其使用者必須不同於使用API方法的使用者。否則，API將返回錯誤。有關使用API功能的其他必備條件，您可以使用下

一本指南。API前提條件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

思科安全管理器(CSM)具有一些需要通過API實施的受管裝置配置功能。

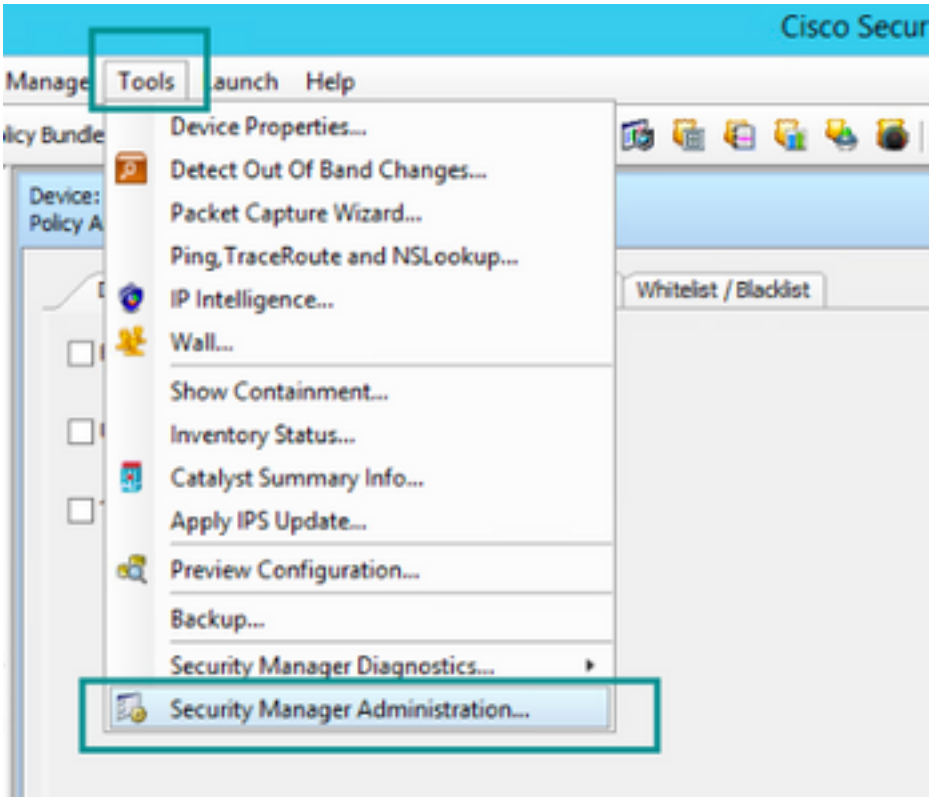
其中一個配置選項是提取由CSM管理的每台裝置中配置的訪問控制清單(ACL)清單的方法。使用CSM API是迄今為止實現此要求的唯一方法。

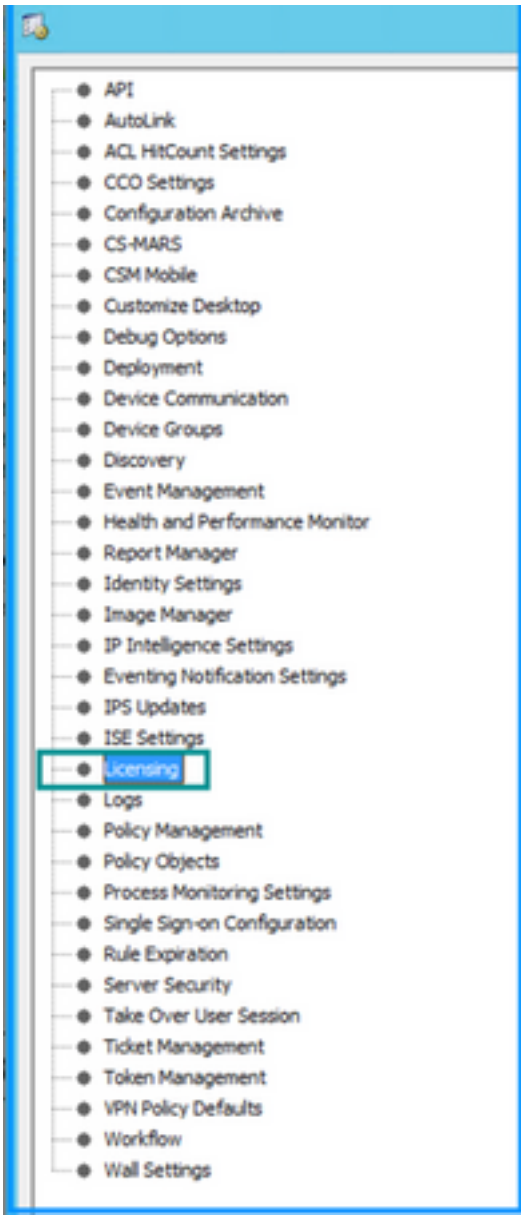
為此，Postman用作API客戶端和CSM版本4.19 SP1、ASA 5515版本9.8(4)。

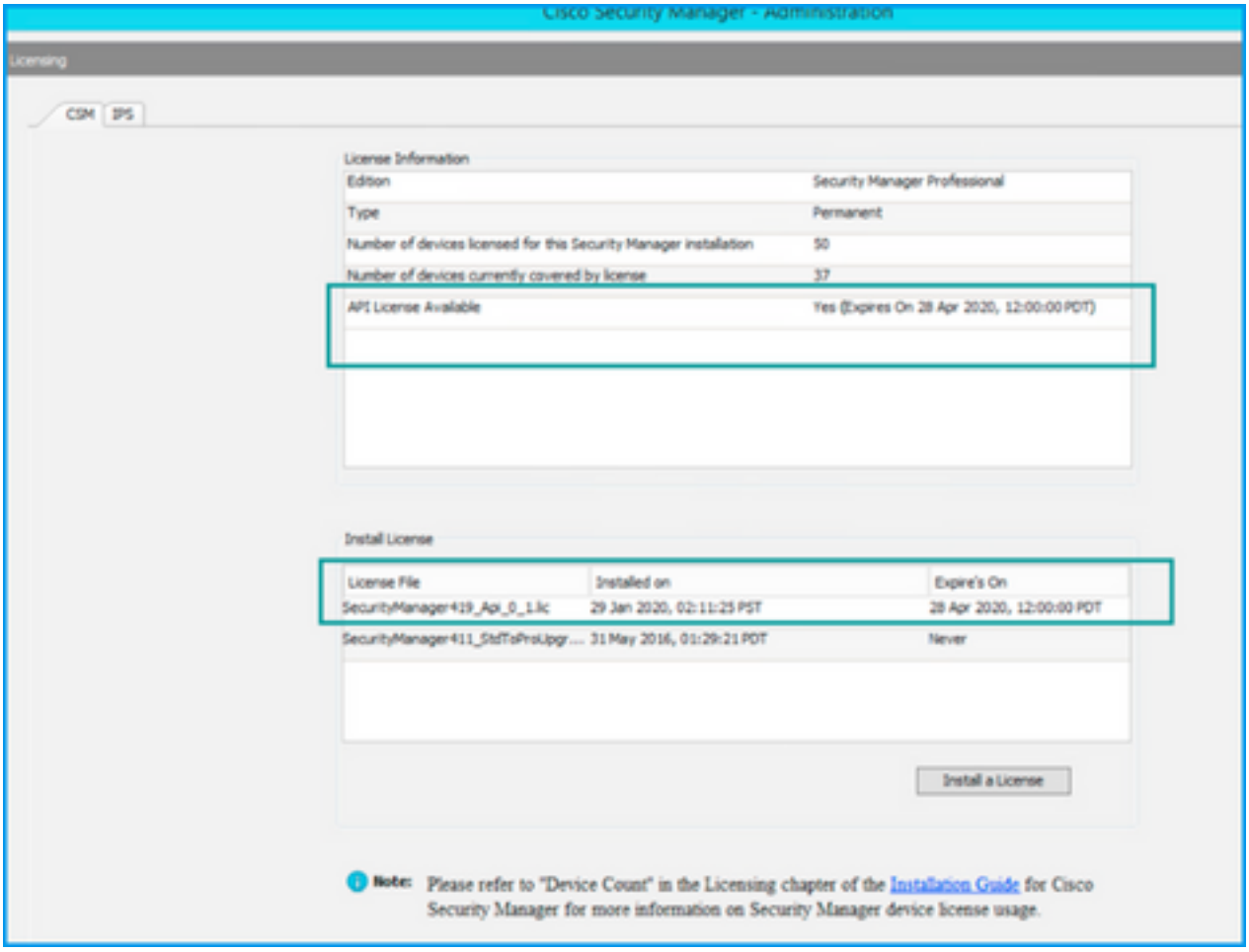
網路圖表

CSM API許可證安裝/驗證

CSM API是一種許可功能，您可以驗證CSM是否具有API許可證，在CSM客戶端中，導航到**Tools > Security Manager Administration > Licensing**頁面，確認您已安裝許可證。


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

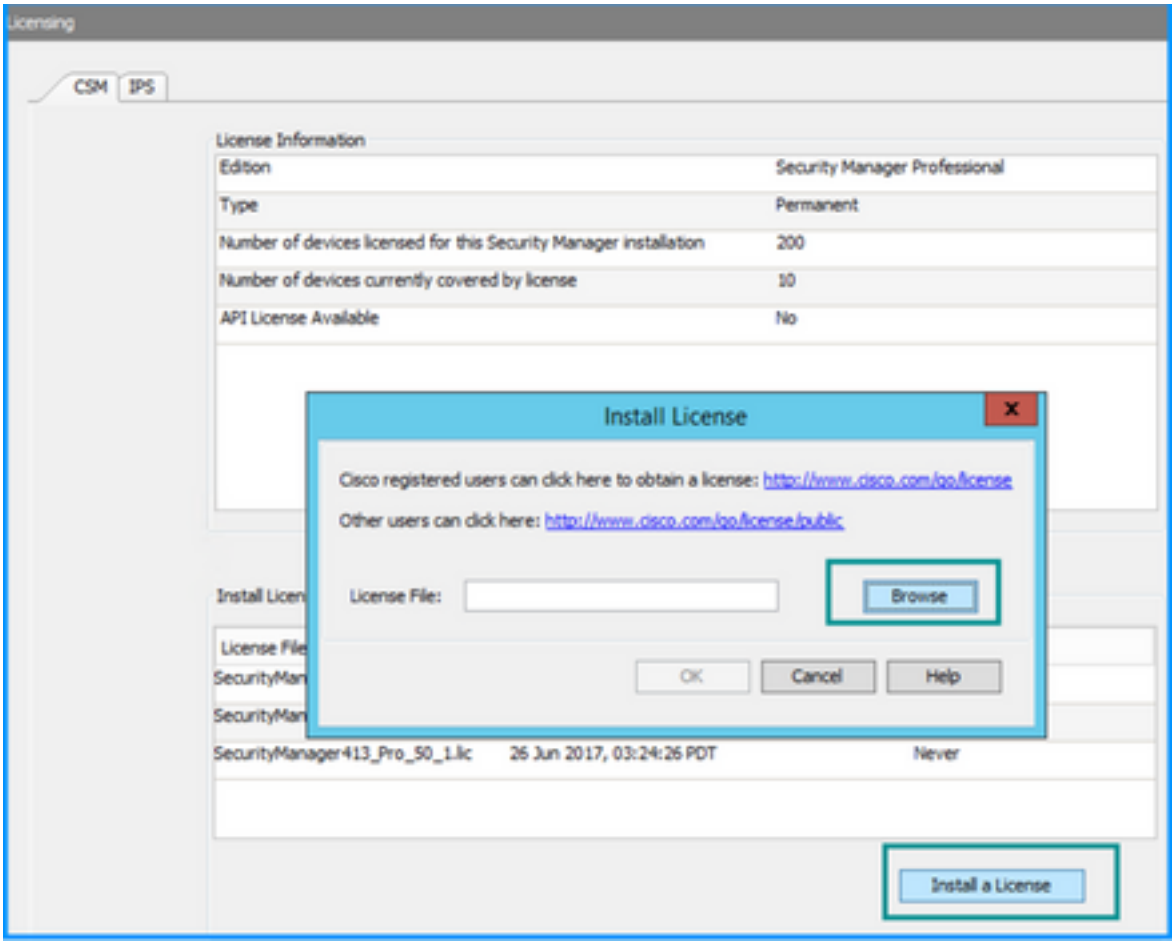

API
AutoLink
ACL HitCount Settings
CCO Settings
Configuration Archive
CS-MARS
CSM Mobile
Customize Desktop
Debug Options
Deployment
Device Communication
Device Groups
Discovery
Event Management
Health and Performance Monitor
Report Manager
Identity Settings
Image Manager
IP Intelligence Settings
Eventing 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

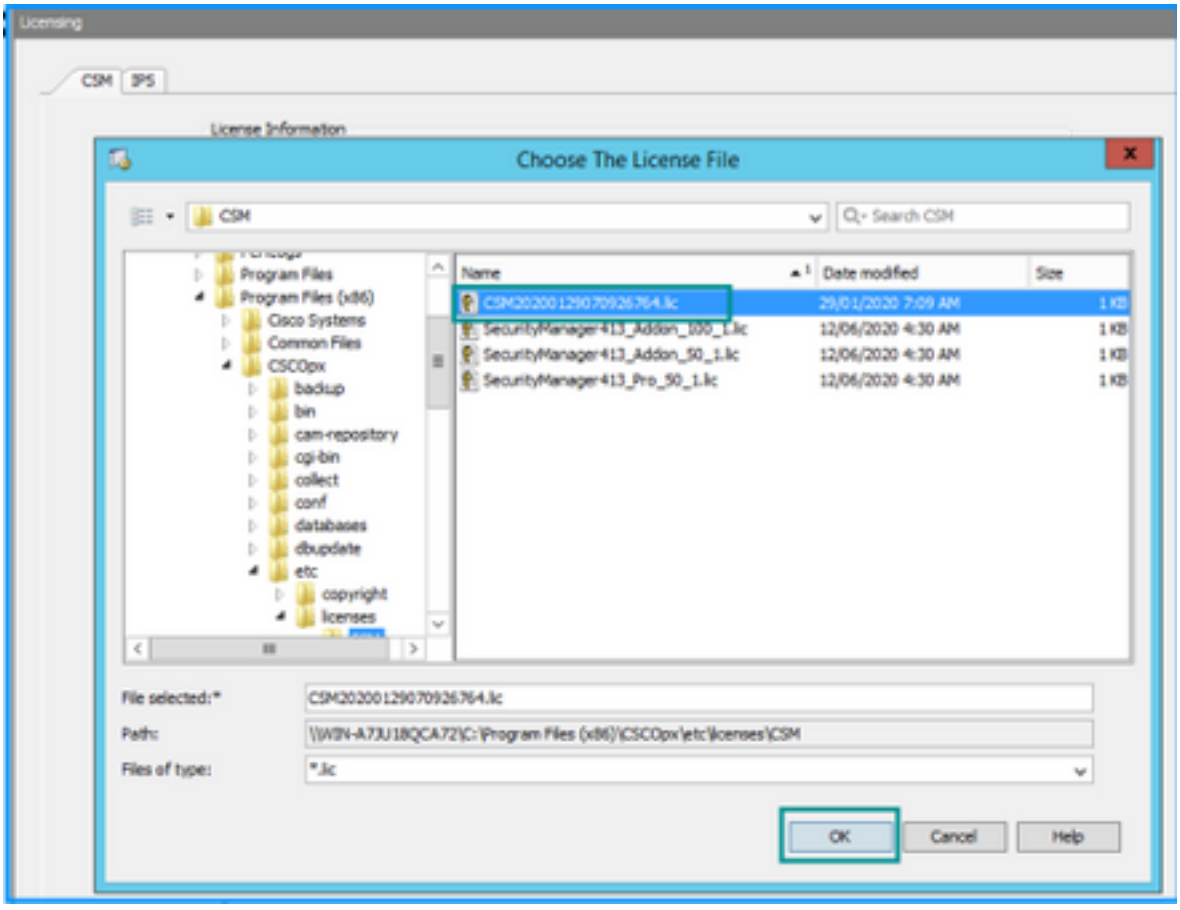


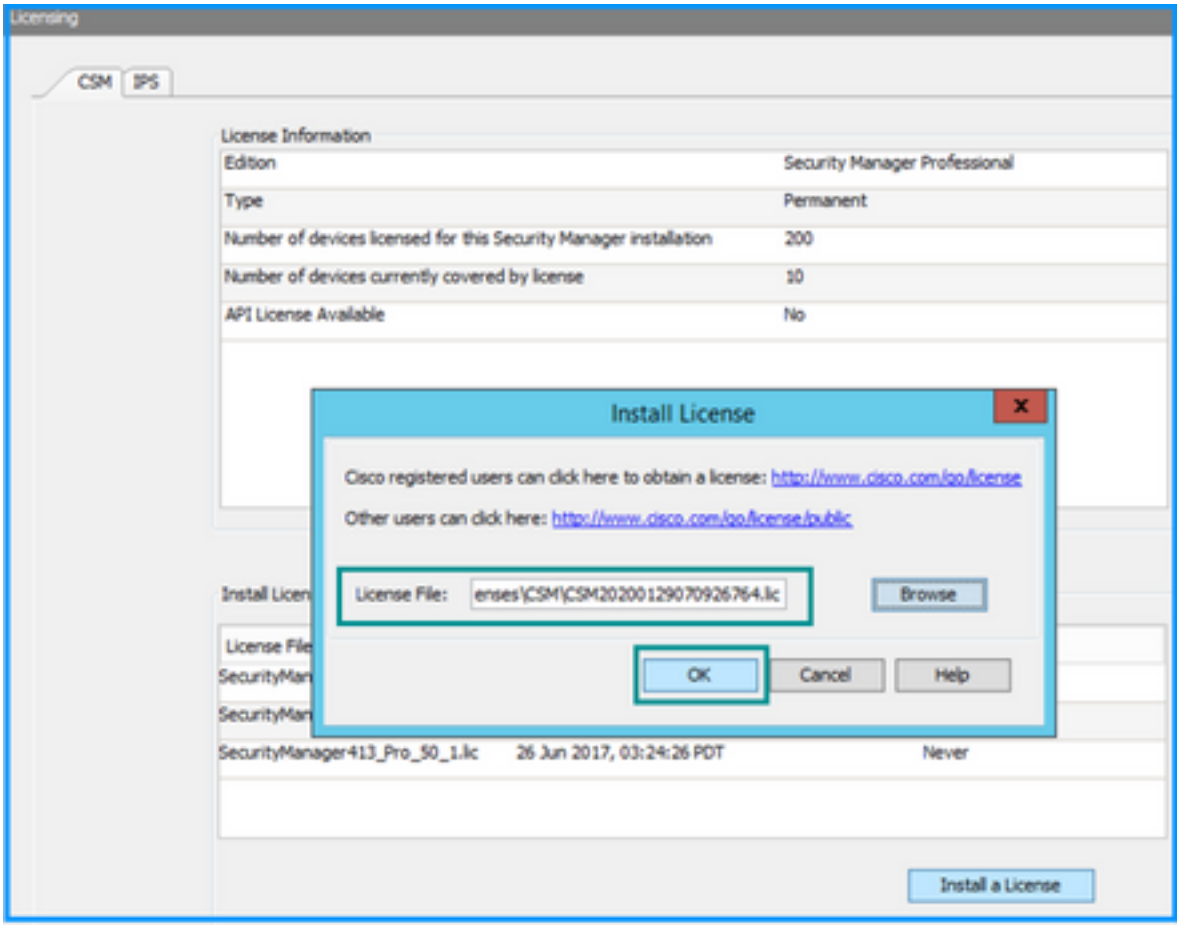
如果未應用API許可證，但您已有可以安裝許可證的.lic檔案，請按一下**Install a License**按鈕，必須將許可證檔案儲存在CSM伺服器所在的同一磁碟中。

要安裝較新的思科安全管理器許可證，請執行以下步驟：

步驟1.將隨附的許可證檔案(.lic)從您收到的電子郵件儲存到您的檔案系統。
步驟2.將儲存的許可證檔案複製到Cisco Security Manager伺服器檔案系統中的已知位置。
步驟3.啟動思科安全管理器客戶端。
步驟4.導覽至**工具 — >安全管理器管理……**
步驟5.在**Cisco Security Manager - Administration視窗中**，選擇**Licensing**
步驟6.按一下**Install a License按**鈕。
步驟7.從**Install License**對話方塊中，選擇**Browse**按鈕。
步驟8.導航至Cisco Security Manager伺服器檔案系統上儲存的許可證檔案，然後選擇**OK**按鈕。
步驟9.在**Install License**對話方塊中，按一下**OK**按鈕。
步驟10.確認顯示的許可證摘要資訊，然後按一下**Close**按鈕。


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許可證只能應用於授權使用CSM專業版的伺服器。許可證無法應用於運行許可證標準版的CSM。API許可證要求

配置步驟

API客戶端設定

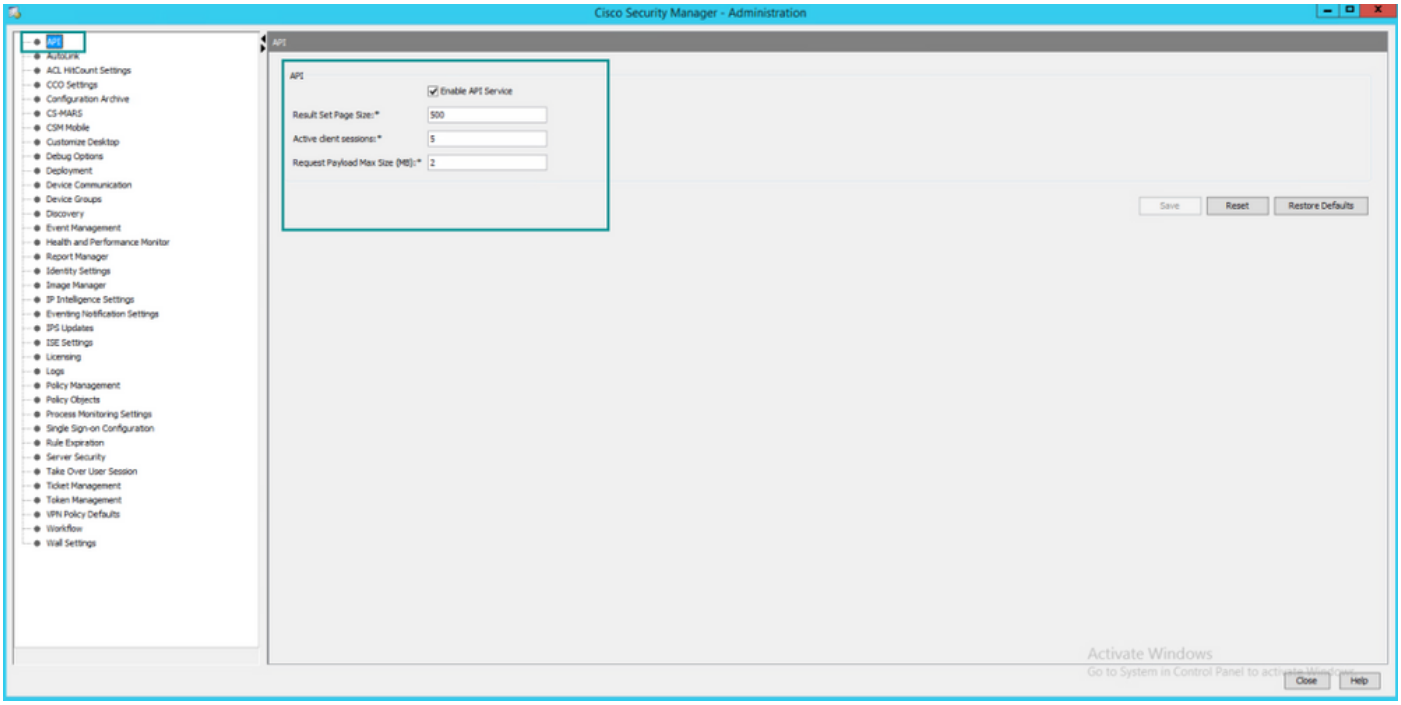
如果使用Postman，則需要配置某些設定，這取決於每個API客戶端，但必須相似。

- 代理已禁用
- SSL驗證 — 關閉

CSM設定

- 已啟用API。在**工具>安全管理器管理> API**下

API設定



使用CSM API

您需要在API客戶端中配置以下兩個呼叫：

1.登入方法

2.獲取ACL值

供整個流程參考：

本實驗中使用的CSM訪問詳細資訊：

CSM主機名（IP地址）：**192.168.66.116**。在API中，我們使用URL中的主機名。

使用者：**admin**

密碼：**Admin123**

登入方法

在其他服務上呼叫任何其他方法之前，必須呼叫此方法。

CSM API指南：方法登入

請求

1. HTTP方法：**POST**

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

3.本文：

其中：

使用者名稱:與會話關聯的CSM客戶端使用者名稱

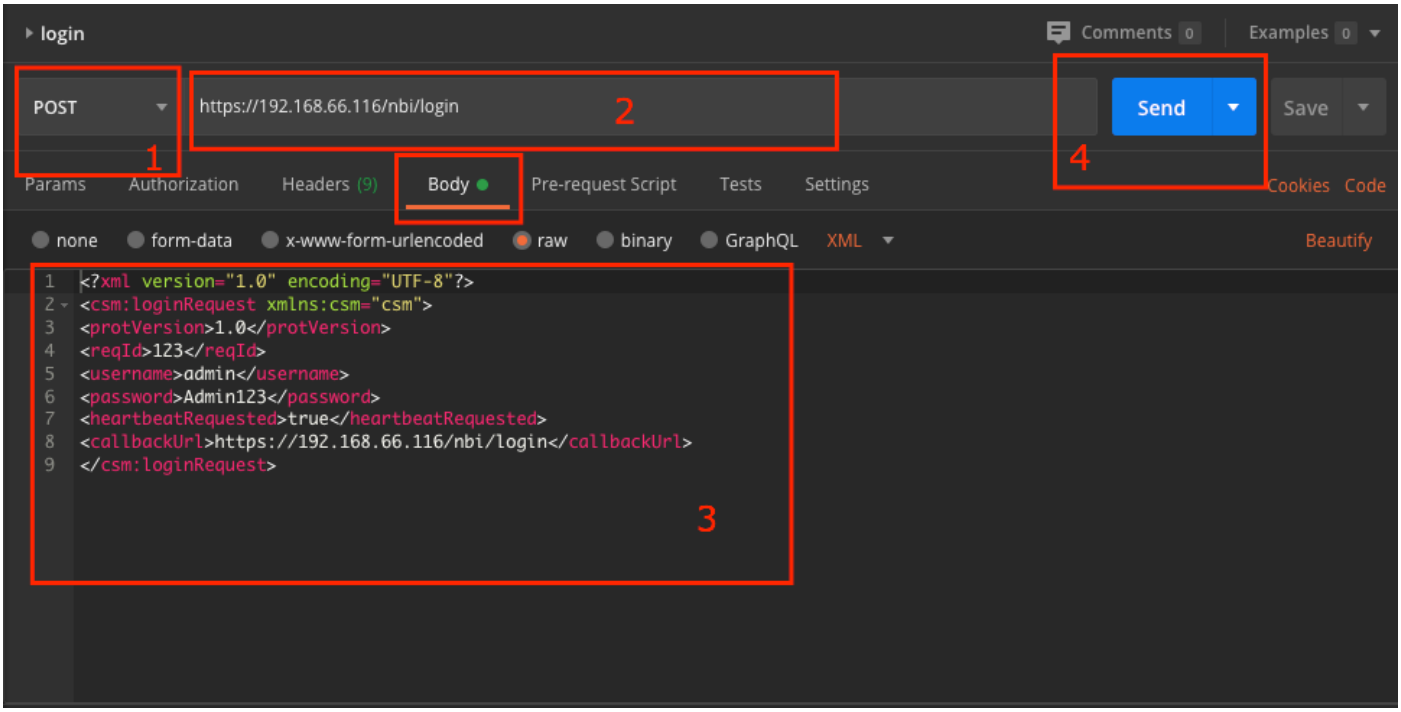
密碼:與會話關聯的CSM客戶端密碼。

reqId:此屬性唯一標識客戶端完成的請求，該值由CSM伺服器在相關響應中回顯。它可以設定為使用者希望用作識別符號的任何內容。

heartbeatRequested:此屬性可以可選地定義。如果屬性設定為true，則CSM客戶端從CSM伺服器接收心跳回撥。伺服器嘗試ping客戶端，其頻率接近（非活動超時）/2分鐘。如果客戶端不響應心跳，則API會在下一個間隔內重試心跳。如果心跳成功，會話不活動超時將被重置。

回撥Url:CSM伺服器進行回撥的URL。如果heartbeatRequested為true，則需要指定此項。僅允許基於HTTPS的回撥URL

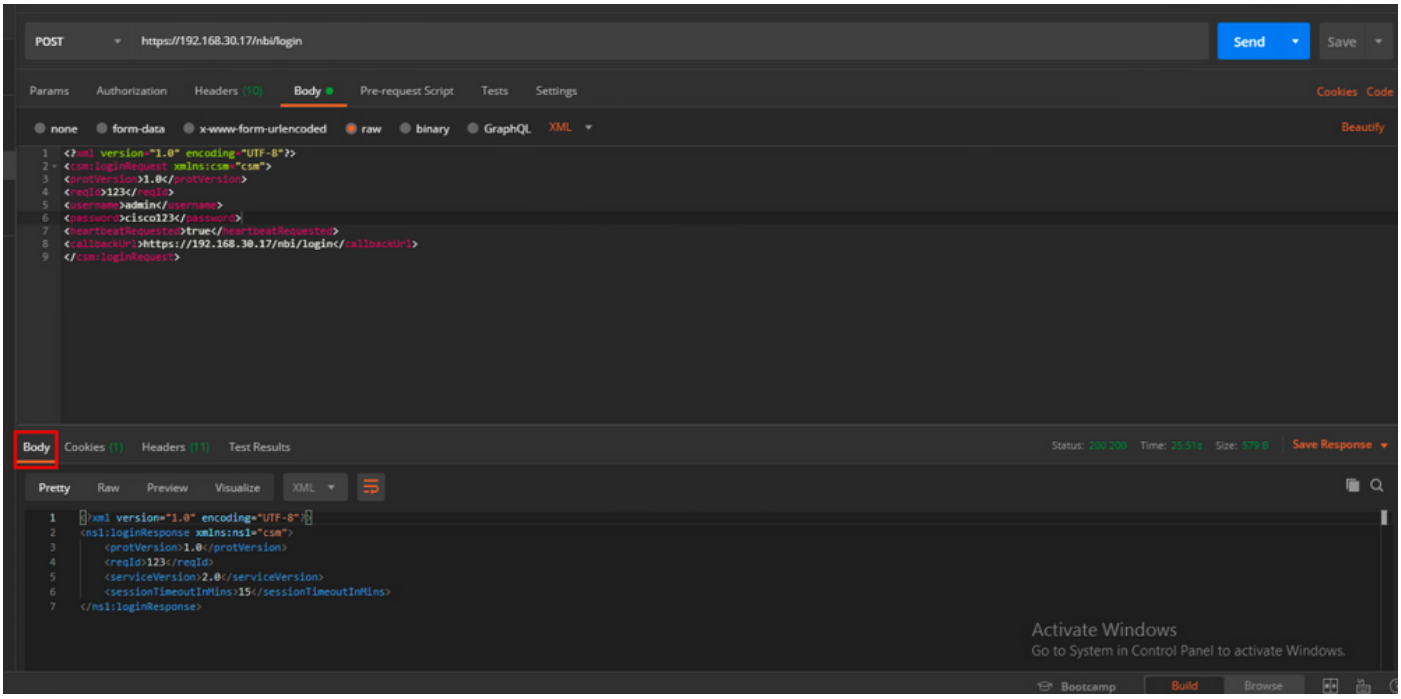
4.傳送



選擇原始選項，如本例所示。

響應

登入API驗證使用者憑證並將會話令牌作為安全cookie返回。會話值儲存在**asCookie**鍵下，您必須將此**值儲存**。



獲取ACL規則

方法execDeviceReadOnlyCLICmds。可通過此方法執行的命令集是只讀命令，如統計資訊、可提供有關特定裝置操作的附加資訊的監控命令。

CSM API使用手冊中的方法詳細資訊

請求

1. HTTP方法：**POST**

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

3. HTTP報頭：標識身份驗證會話的登入方法返回的cookie。

輸入**asCookie**值（先前從方法登入獲得）。

主要:輸入「asCookie」

值：已獲取輸入值。

按一下覈取方塊以啟用它。

4.本文：

附註：上述XML正文可用於執行任何「show」命令，例如：「show run all」、「show run object」、「show run nat」等。

XML「<deviceReadOnlyCLICmd>」元素表示「<cmd>」和「<argument>」中指定的命令必須為只讀。

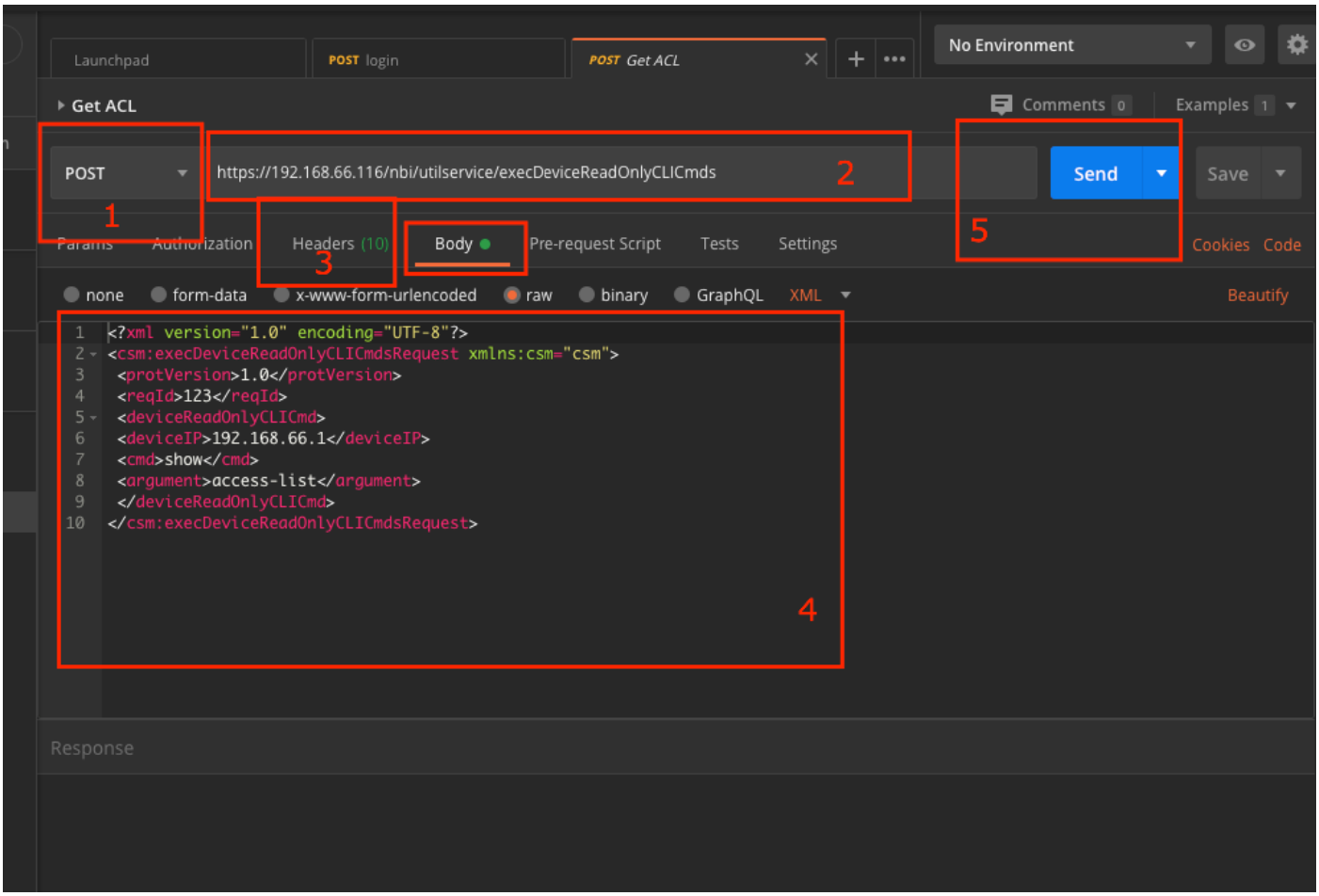
其中：

裝置IP:必須對其執行命令的裝置IP地址。

cmd:已修正**命令"show"。**Regex允許混合大小寫[sS][hH][oO][wW]

引數:show命令引數。如「run」顯示裝置的運行配置，或「**access-list」顯示訪問**清單詳細資訊。

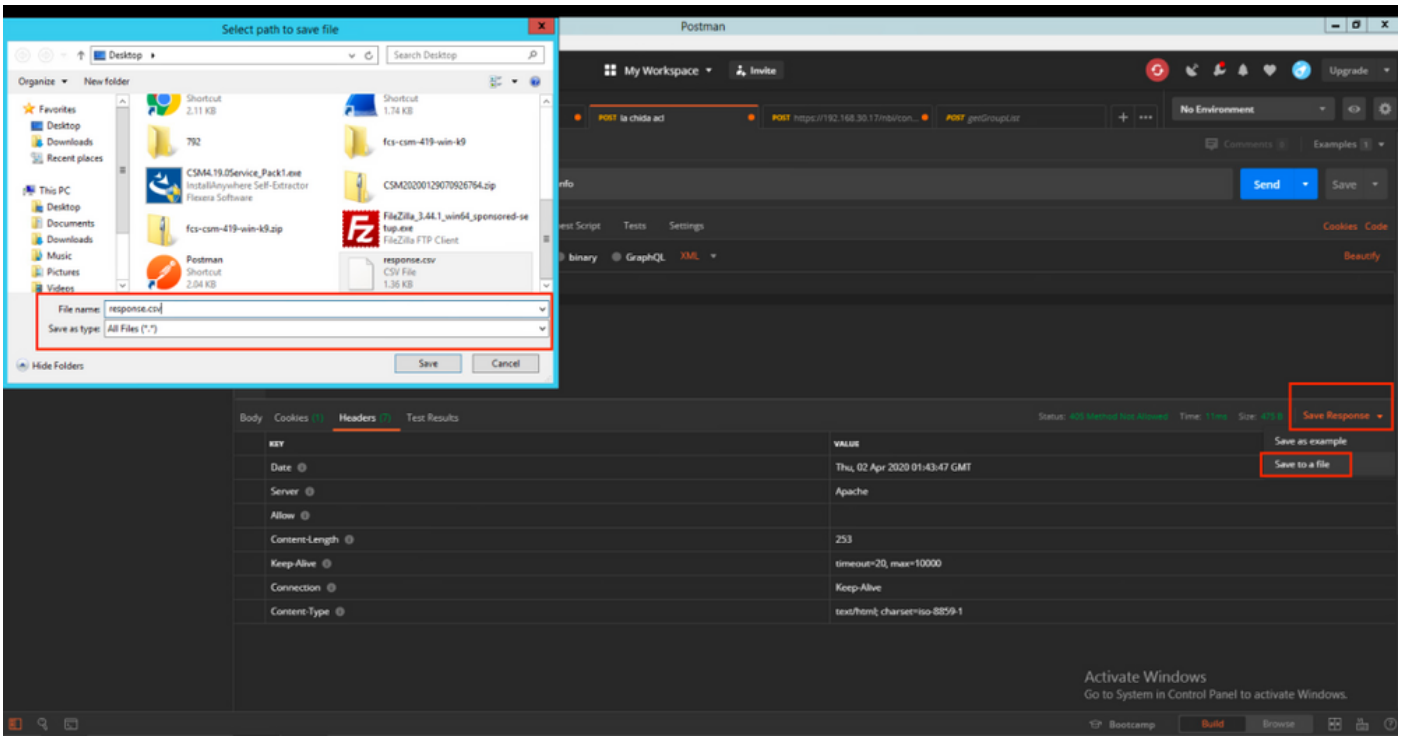
5.傳送



響應

驗證

您可以選擇將響應另存為檔案。導航到**Save Response > Save to a file**。然後選擇檔案位置並將其另存為.csv型別。



然後，您必須能夠使用Excel應用程式開啟此.csv檔案，例如。在.csv檔案型別中，可以將輸出儲存為其他檔案型別，例如PDF、TXT等。

疑難排解

使用API的可能故障響應。

1.未安裝API許可證。

原因：API許可證已過期、未安裝或未啟用。

可能的解決方案：在**Tools > Security Manager Administration > Licensing**頁面下驗證許可證的到期日期

驗證**工具>安全管理器管理> API**下是否啟用了API功能

確認本指南前面的**CSM API許可證安裝/驗證**部分的設定。

2.用於API登入的CSM IP地址錯誤。

原因：API呼叫的URL中CSM伺服器的IP地址錯誤。

可能的解決方案：在API客戶端的URL中驗證主機名是CSM伺服器的正確IP地址。

URL：https://**<hostname>**/nbi/login

3.錯誤的ASA IP地址。

原因：在<deviceIP></deviceIP>標籤之間的主體上定義的IP地址不能是正確的地址。

可能的解決方案：確認已在主體語法中定義了正確的裝置IP地址。

4.沒有與防火牆的連線。

原因：裝置與CSM沒有連線

可能的解決方案：從CSM伺服器運行測試連線，並對與裝置的進一步連線進行故障排除。

有關更多錯誤代碼和說明的資訊，請點選下一連結中的「思科安全管理器API規範指南」獲取更多詳情。