Extraktion der ACL aus CSM im CSV-Format mithilfe einer API-Methode

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Zugriffskontrolllisten (ACLs) im CSV-Format (Comma-Separated Values) eines Geräts extrahiert werden, das vom Cisco Security Manager (CSM) über die CSM-API-Methode verwaltet wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Security Manager (CSM)
- CSM-API
- API-Basiswissen

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- CSM-Server
- CSM-API-Lizenz
  ```
  Product Name: L-CSMPR-API
  Product Description: L-CSMPR-API : Cisco Security Manager Pro - License to enable API Access
  ```
- Adaptative Security Appliance (ASA), verwaltet durch CSM

- Ein API-Client. Sie können cURL, Python oder Postman verwenden. Dieser Artikel zeigt den gesamten Prozess mit Postman. Die CSM-Client-Anwendung muss geschlossen werden. Wenn eine CSM-Clientanwendung geöffnet ist, muss sie von einem anderen Benutzer sein als dem, der die API-Methode verwendet. Andernfalls gibt API einen Fehler zurück. Weitere Voraussetzungen für die Verwendung der API-Funktion finden Sie im nächsten Handbuch. API-Voraussetzungen

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Cisco Security Manager (CSM) verfügt über einige Funktionen für die Konfiguration verwalteter Geräte, die über API implementiert werden müssen.

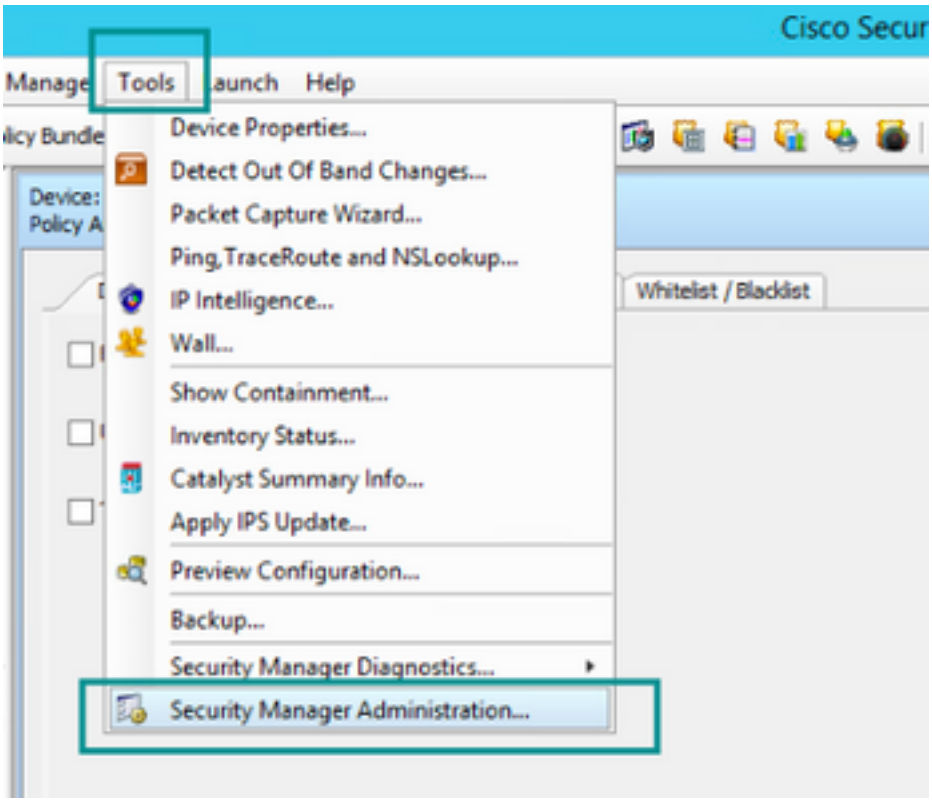
Eine dieser Konfigurationsoptionen ist die Methode zum Extrahieren einer Liste der Zugriffskontrolllisten (ACLs), die auf jedem vom CSM verwalteten Gerät konfiguriert sind. Die Verwendung der CSM-API ist die einzige Möglichkeit, diese Anforderung bisher zu erfüllen.

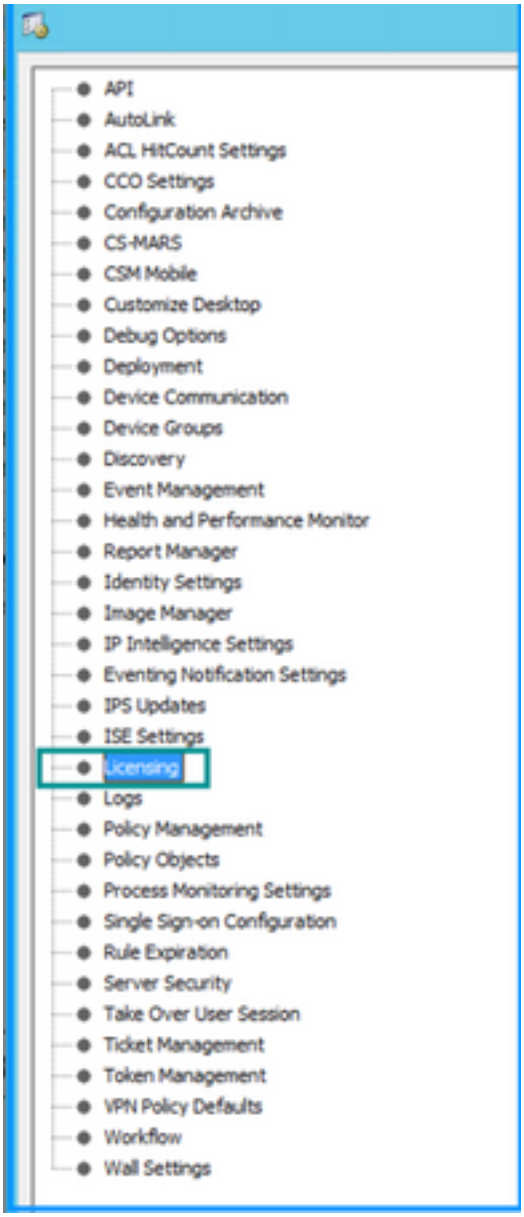
Zu diesem Zweck wurde Postman als API-Client und CSM Version 4.19 SP1, ASA 5515 Version 9.8(4) verwendet.

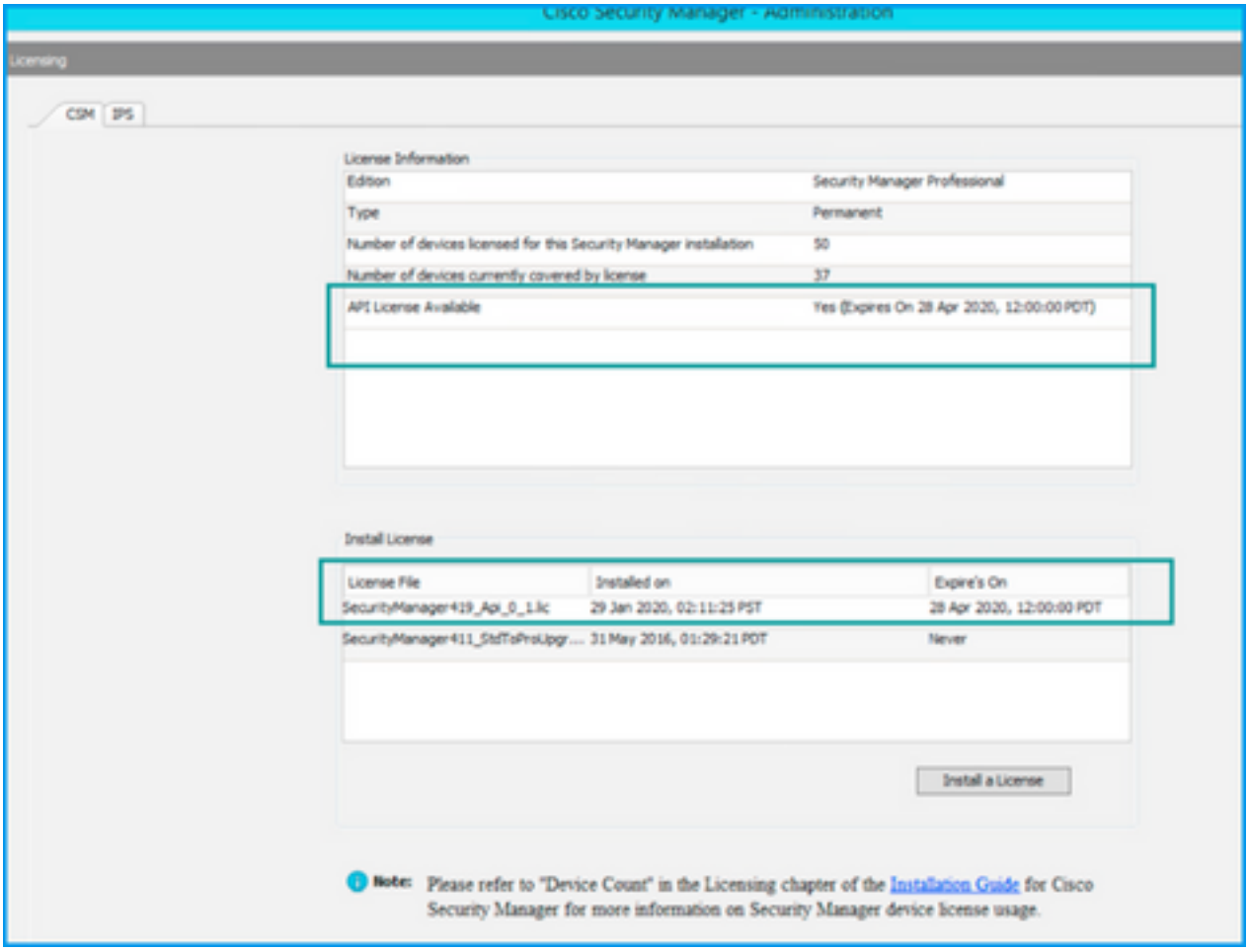
Netzwerkdiagramm

Installation/Verifizierung der CSM API-Lizenz

CSM API ist eine lizenzierte Funktion. Sie können überprüfen, ob das CSM über eine API-Lizenz verfügt. Navigieren Sie im CSM-Client zur **Seite Extras > Security Manager Administration > Licensing (Extras > Sicherheitsmanager-Verwaltung > Lizenzierung)**, um zu bestätigen, dass Sie bereits eine Lizenz installiert haben.


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

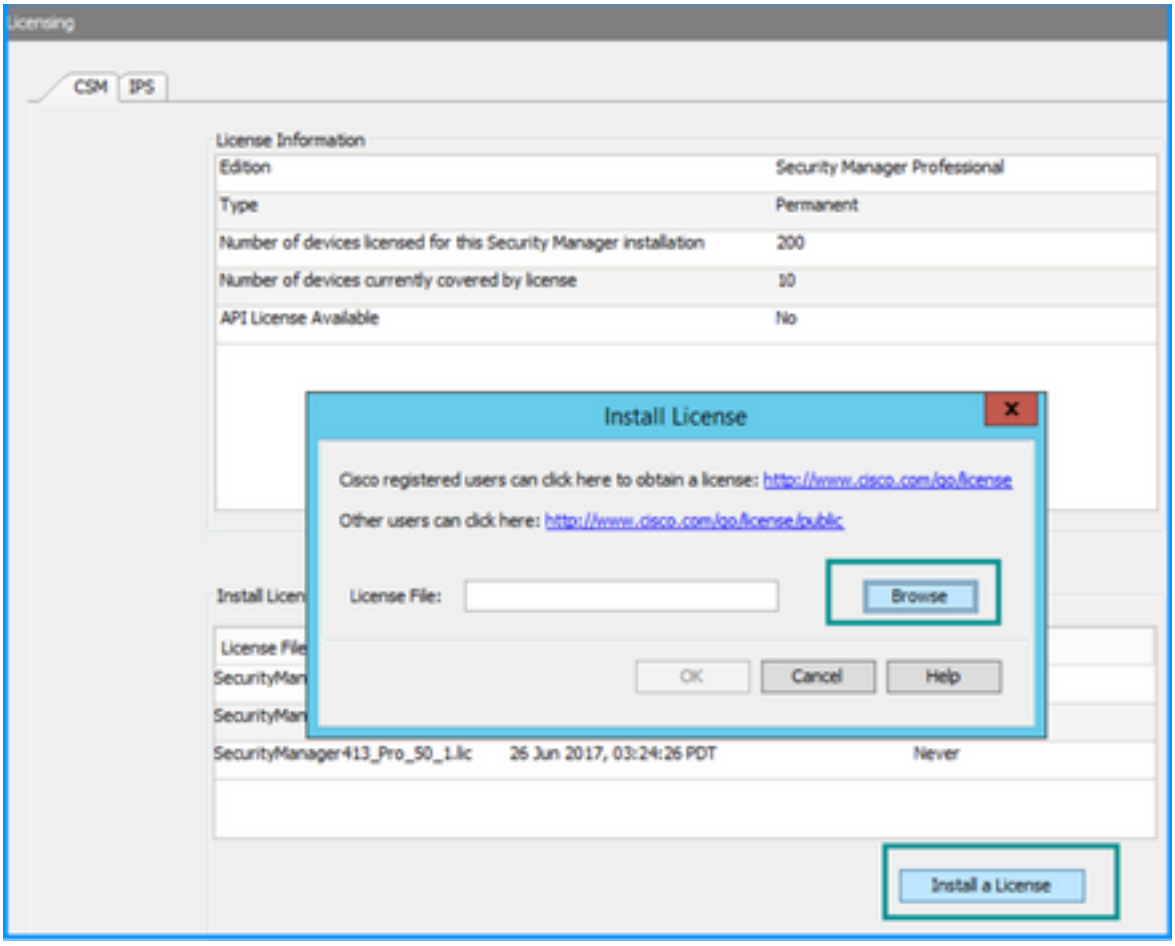

API
AutoLink
ACL HitCount Settings
CCO Settings
Configuration Archive
CS-MARS
CSM Mobile
Customize Desktop
Debug Options
Deployment
Device Communication
Device Groups
Discovery
Event Management
Health and Performance Monitor
Report Manager
Identity Settings
Image Manager
IP Intelligence Settings
Eventing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

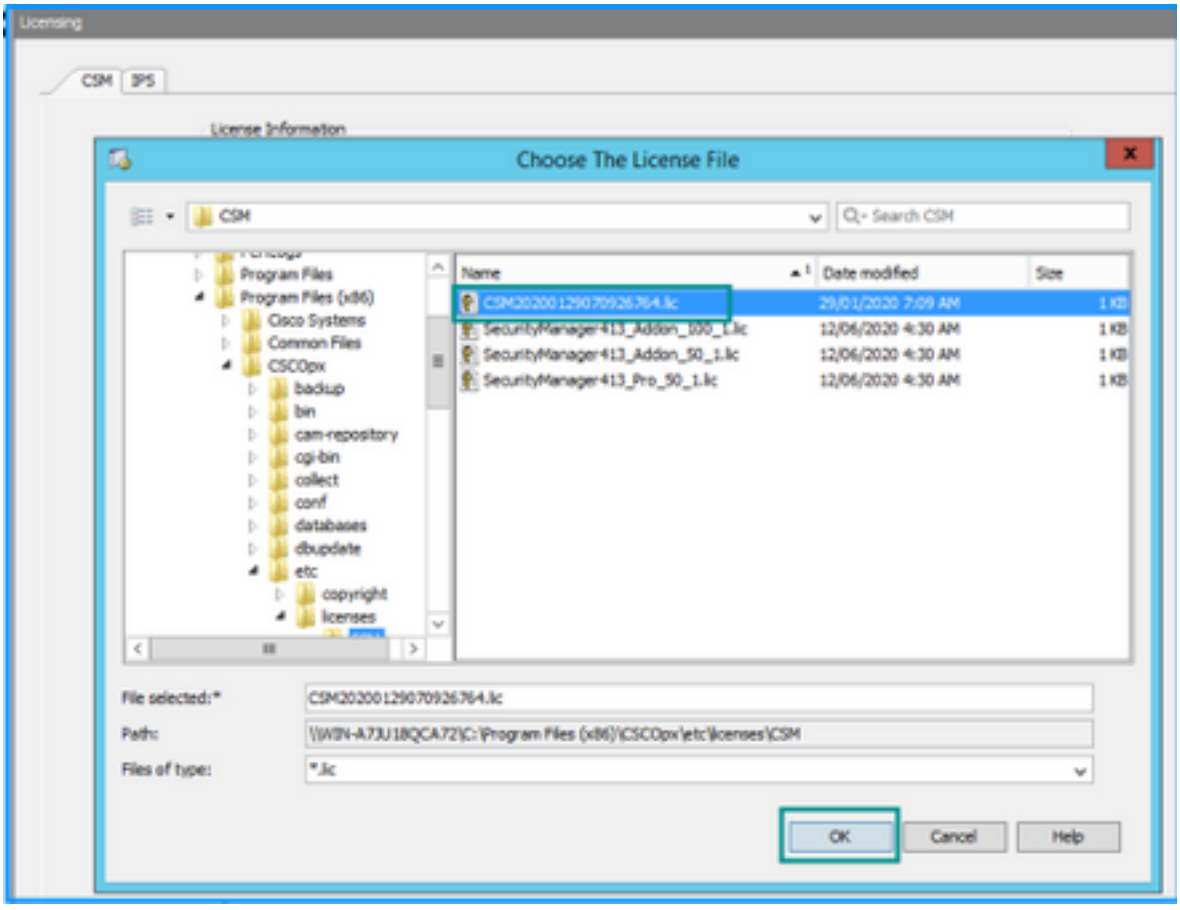


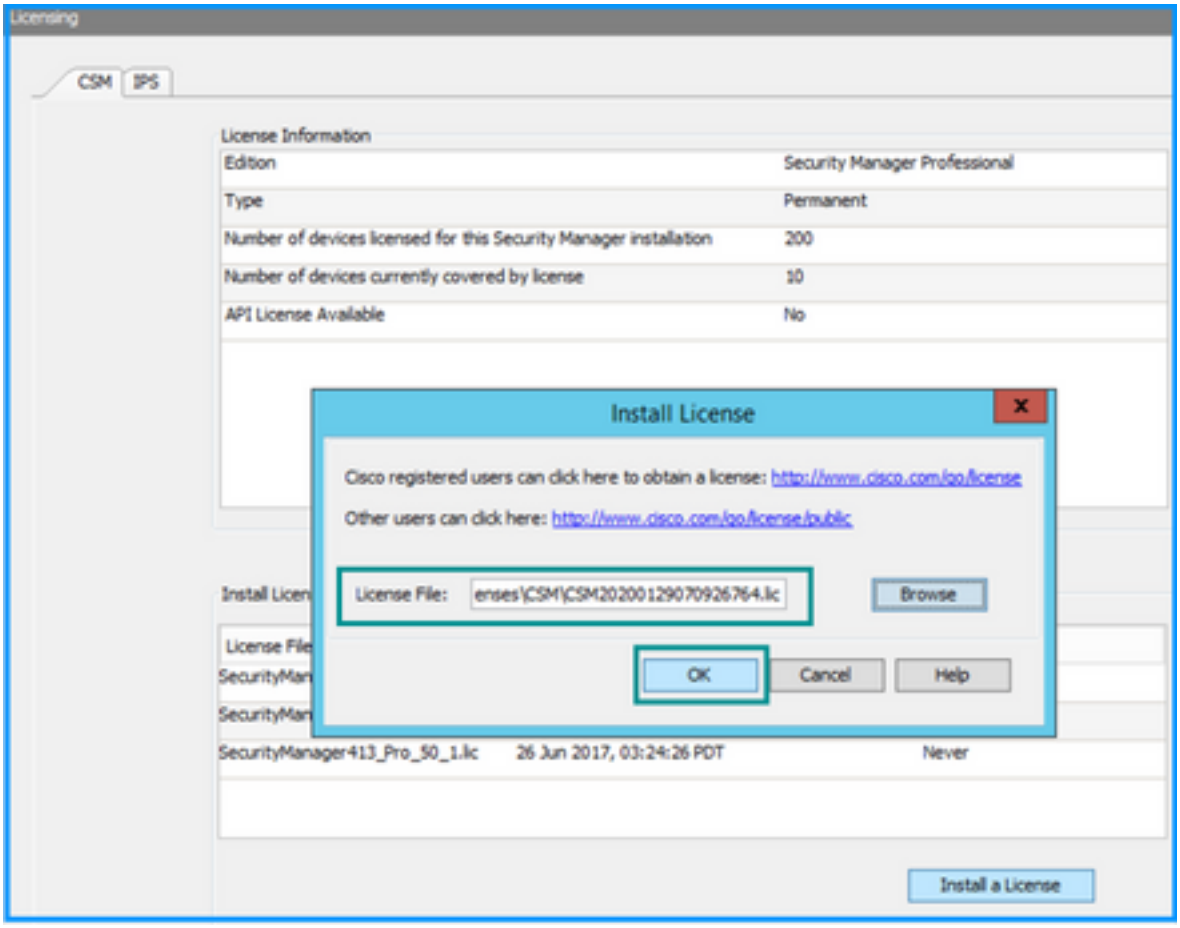
Wenn keine API-Lizenz angewendet wurde, Sie aber bereits über die .lic-Datei verfügen, die Sie zur Installation Ihrer Lizenz verwenden können, klicken Sie auf die Schaltfläche **Lizenz installieren**, müssen Sie die Lizenzdatei auf dem Datenträger speichern, auf dem sich der CSM-Server befindet.

So installieren Sie eine neuere Cisco Security Manager-Lizenz:

Schritt 1: Speichern Sie die angehängte Lizenzdatei (.lic) aus der erhaltenen E-Mail in Ihrem Dateisystem.
Schritt 2: Kopieren Sie die gespeicherte Lizenzdatei an einen bekannten Speicherort im Cisco Security Manager-Serverdateisystem.
Schritt 3: Starten Sie den Cisco Security Manager-Client.
Schritt 4: Navigieren Sie zu **Extras > Security Manager Administration..**
Schritt 5: Wählen Sie im Fenster **Cisco Security Manager - Administration** die Option **Licensing (Lizenzierung) aus.**
Schritt 6: Klicken Sie auf die Schaltfläche **Lizenz installieren**.
Schritt 7: Wählen Sie im Dialogfeld **Install License (Lizenz installieren)** die Schaltfläche **Browse (Durchsuchen**) aus.
Schritt 8: Navigieren Sie zum Dateisystem des Cisco Security Manager-Servers, und wählen Sie die gespeicherte Lizenzdatei aus, und wählen Sie die Schaltfläche **OK aus**.
Schritt 9: Klicken Sie im Dialogfeld **Install License (Lizenz installieren**) auf die **Schaltfläche OK**.
Schritt 10: Bestätigen Sie die angezeigten Informationen zur Lizenzübersicht, und klicken Sie auf die Schaltfläche **Schließen**.


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



Die API-Lizenz kann nur auf einem für die CSM Professional Edition lizenzierten Server angewendet werden. Die Lizenz kann nicht auf CSM angewendet werden, auf dem eine Standard Edition der Lizenz ausgeführt wird. API-Lizenzanforderungen

Konfigurationsschritte

API-Client-Einstellungen

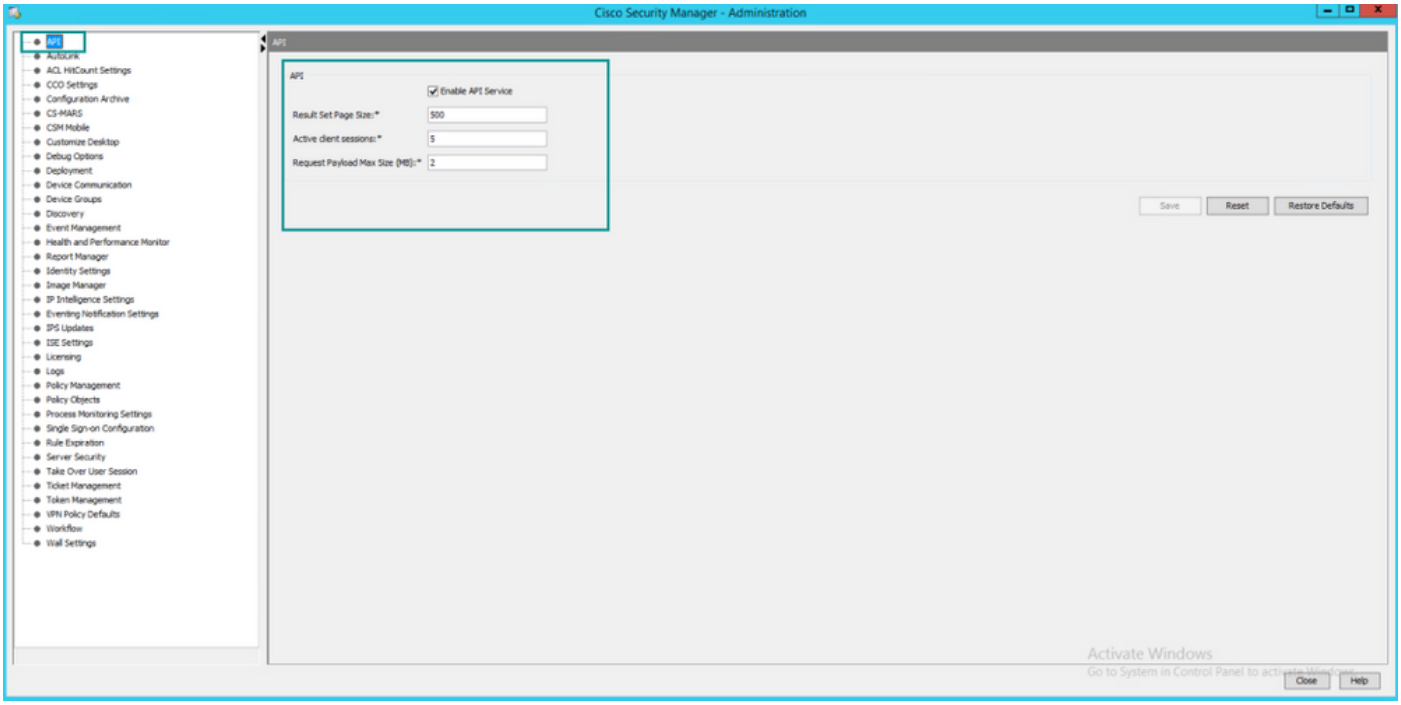
Wenn Sie Postman verwenden, gibt es einige Einstellungen, die Sie konfigurieren müssen, es hängt von jedem API-Client, sondern muss ähnlich sein.

- Proxy deaktiviert
- SSL-Verifizierung - OFF

CSM-Einstellungen

- Aktivierte API. Unter **Extras > Security Manager Administration > API**

API-
Einstellungen



Arbeiten mit CSM-API

Sie müssen im API-Client die folgenden beiden Anrufe konfigurieren:

1. Login-Methode

2. ACL-Werte abrufen

Zur Referenz während des Prozesses:

In dieser Übung verwendete CSM-Zugriffsdetails:

CSM-Hostname (IP-Adresse): **192.168.66.116.** In der API wird der Hostname in der URL verwendet.

Benutzer: **Administrator**

Kennwort: **Administrator123**

Anmeldungsmethode

Diese Methode muss vor jeder anderen Methode aufgerufen werden, die für andere Dienste aufgerufen wird.

Leitfaden zur CSM-API: Methodenanmeldung

Anfrage

1. HTTP-Methode: **POST**

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

3. Nachrichtentext:

Wo:

Benutzername: Der der Sitzung zugeordnete CSM-Client-Benutzername

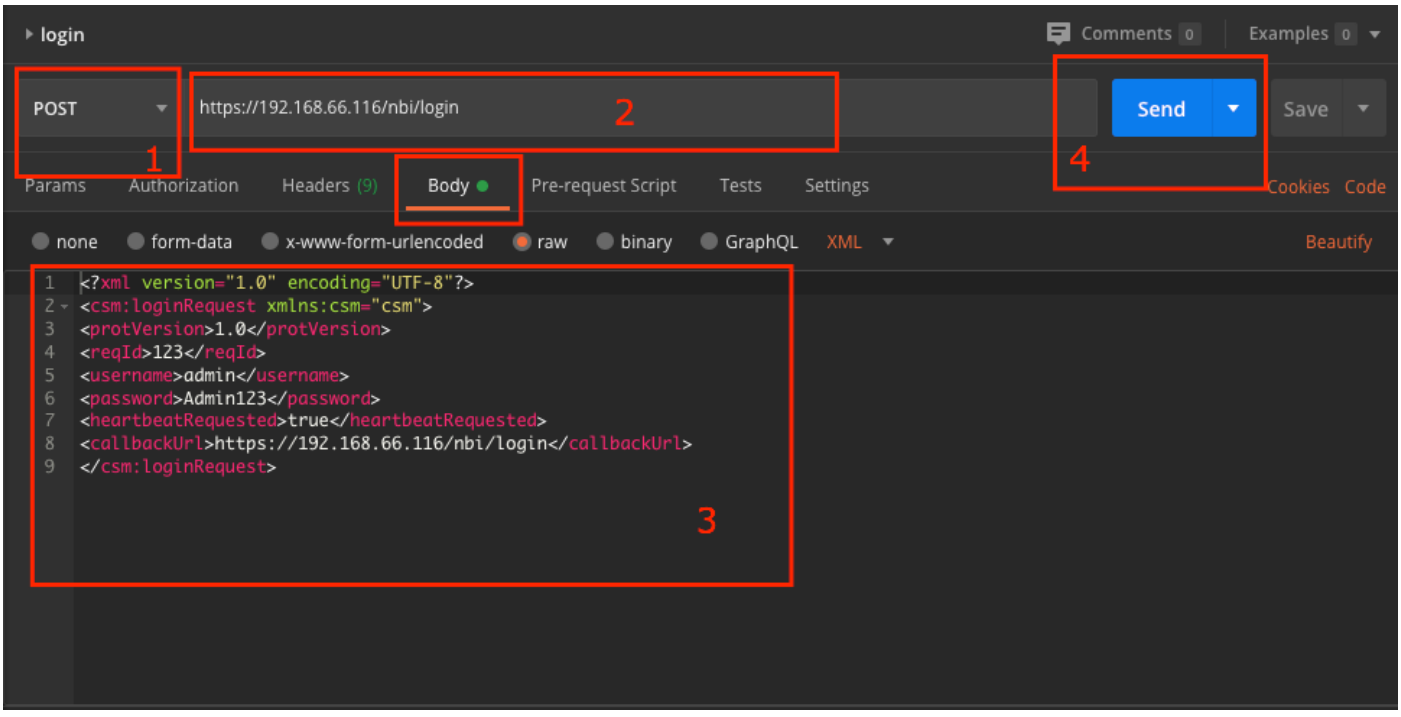
Kennwort: Das CSM-Client-Kennwort für die Sitzung.

reqId: Dieses Attribut identifiziert eindeutig eine vom Client ausgeführte Anforderung, die vom CSM-Server in der zugeordneten Antwort wiedergegeben wird. Sie kann auf alles festgelegt werden, was der Benutzer als Kennzeichnung verwenden möchte.

HeartbeatAngefordert: Dieses Attribut kann optional definiert werden. Wenn das Attribut auf true festgelegt ist, erhält der CSM-Client einen Heartbeat-Rückruf vom CSM-Server. Der Server versucht, einen Ping an den Client mit einer Frequenz nahe (Inaktivitäts-Timeout) / 2 Minuten. Wenn der Client nicht auf den Heartbeat reagiert, versucht die API den Heartbeat im nächsten Intervall erneut. Wenn der Heartbeat erfolgreich ist, wird das Timeout für die Sitzung bei Inaktivität zurückgesetzt.

CallbackUrl: Die URL, unter der der CSM-Server den Rückruf vornimmt. Dies muss angegeben werden, wenn heartbeatRequested true ist. Nur HTTPS-basierte Rückruf-URLs sind zulässig

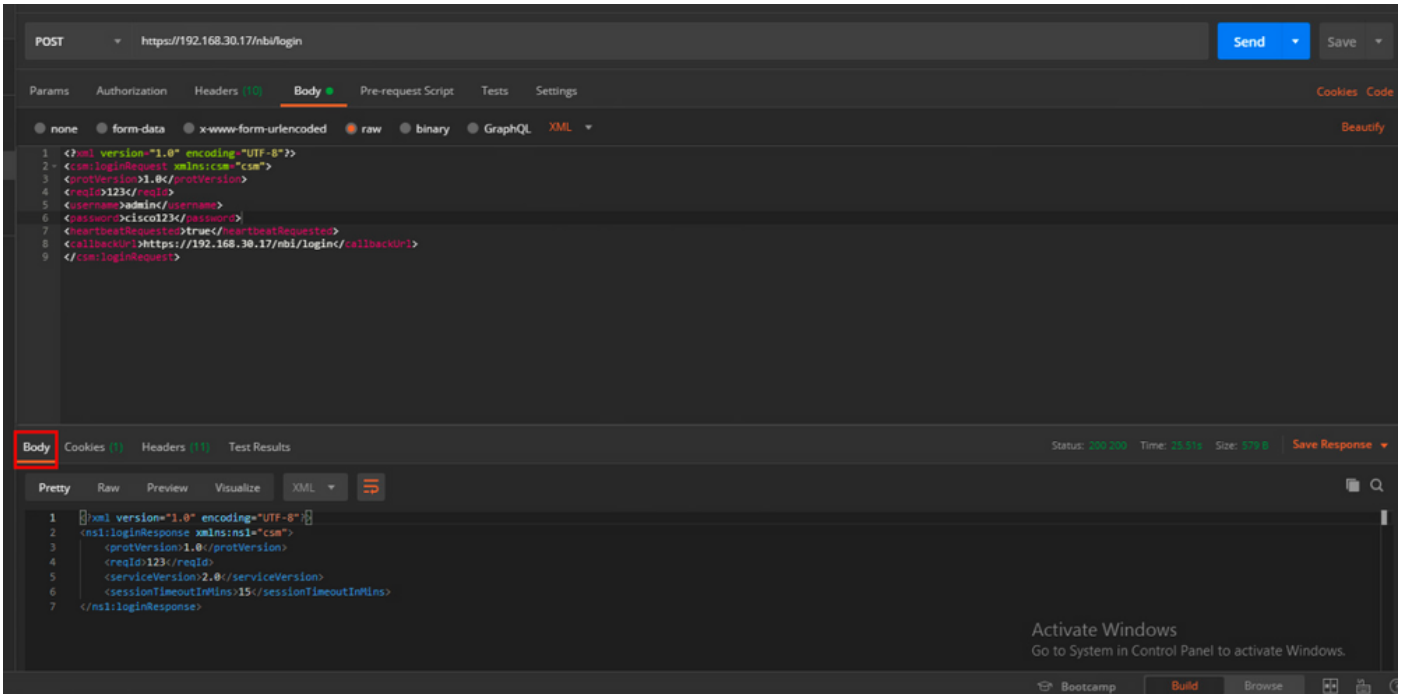
4. Senden



Wählen Sie die Rohoption aus, um wie in diesem Beispiel angezeigt zu werden.

Antwort

Die Anmelde-API validiert die Benutzeranmeldeinformationen und gibt ein Sitzungstoken als sicheres Cookie zurück. Der Sitzungswert wird unter dem Schlüssel **asCookie** gespeichert, Sie müssen diesen **als Cookie-Wert** speichern.



ACL-Regeln abrufen

Methode execDeviceReadOnlyCLICmds. Bei der Gruppe von Befehlen, die mit dieser Methode ausgeführt werden können, handelt es sich um schreibgeschützte Befehle wie Statistiken, Überwachungsbefehle, die zusätzliche Informationen über den Betrieb des jeweiligen Geräts bereitstellen.

Methodendetails finden Sie im CSM API-Benutzerhandbuch.

Anfrage

1. HTTP-Methode: **POST**

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

3. HTTP-Header: Das von der Anmeldemethode zurückgegebene Cookie, das die Authentifizierungssitzung identifiziert.

Geben Sie **alsCookie**-Wert ein, der zuvor von Method Login abgerufen wurde.

Wichtigste: Eingabe von "asCookie"

Wert: Erhaltener Eingabewert.

Aktivieren Sie das Kontrollkästchen.

4. Nachrichtentext:

Hinweis: Der obige XML-Text kann verwendet werden, um einen beliebigen Befehl "show" auszuführen, z. B.: "show run all", "show run object", "show run nat" usw.

Das XML-Element "<deviceReadOnlyCLICmd>" gibt an, dass der in "<cmd>" und "<argument>" angegebene Befehl nur gelesen werden MUSS.

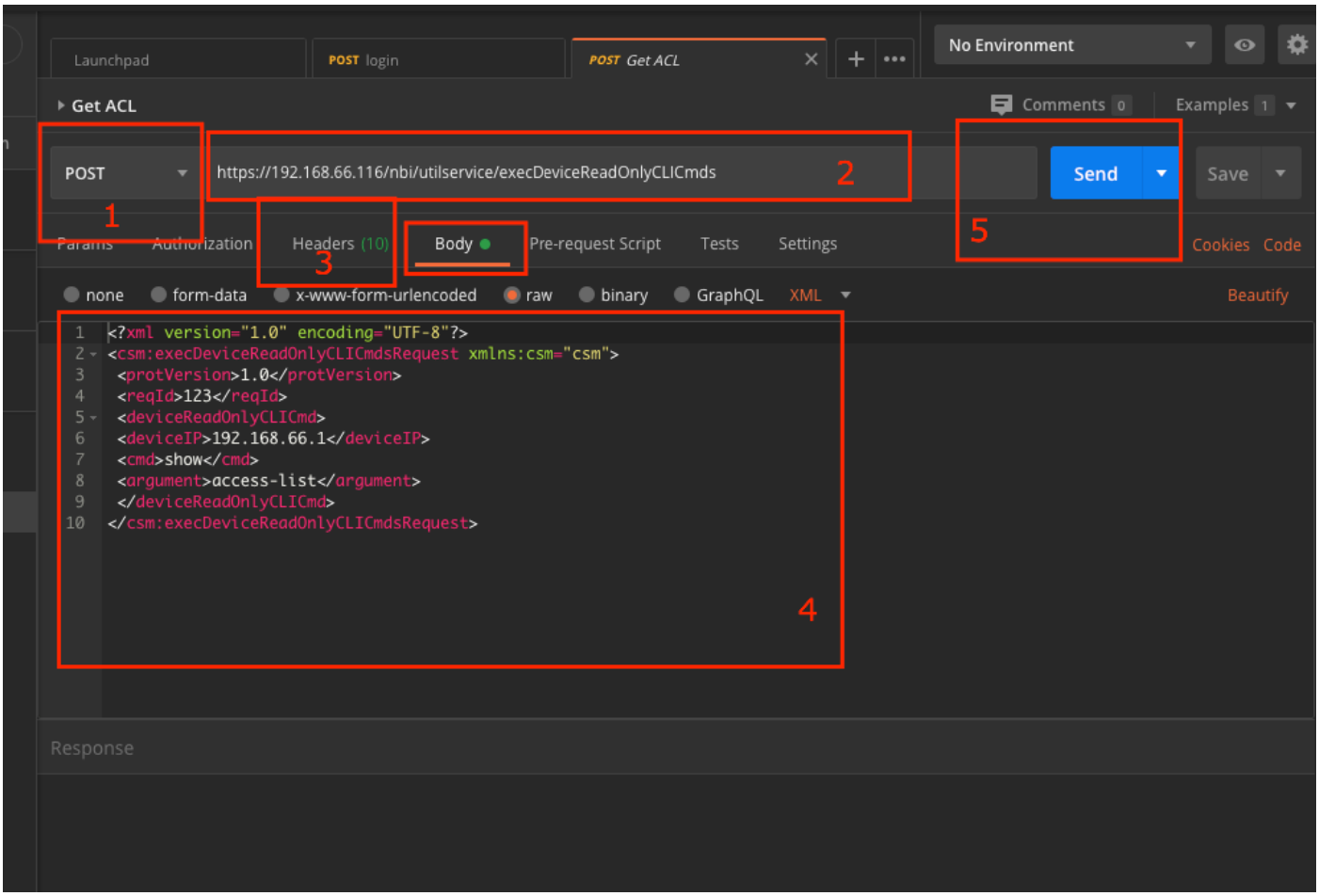
Wo:

GerätIP: Die Geräte-IP-Adresse, für die der Befehl ausgeführt werden muss.

cmd: Behoben-Befehl **"show".** Der reguläre Ausschnitt erlaubt gemischte Gehäuse [sS][hH][oO][wW]

Argument: Die Befehlsargumente show. Beispiel: "Ausführen" zum Anzeigen der aktuellen Konfiguration des Geräts oder **"Zugriffsliste"** zum Anzeigen der Zugriffslistendetails.

5. Senden

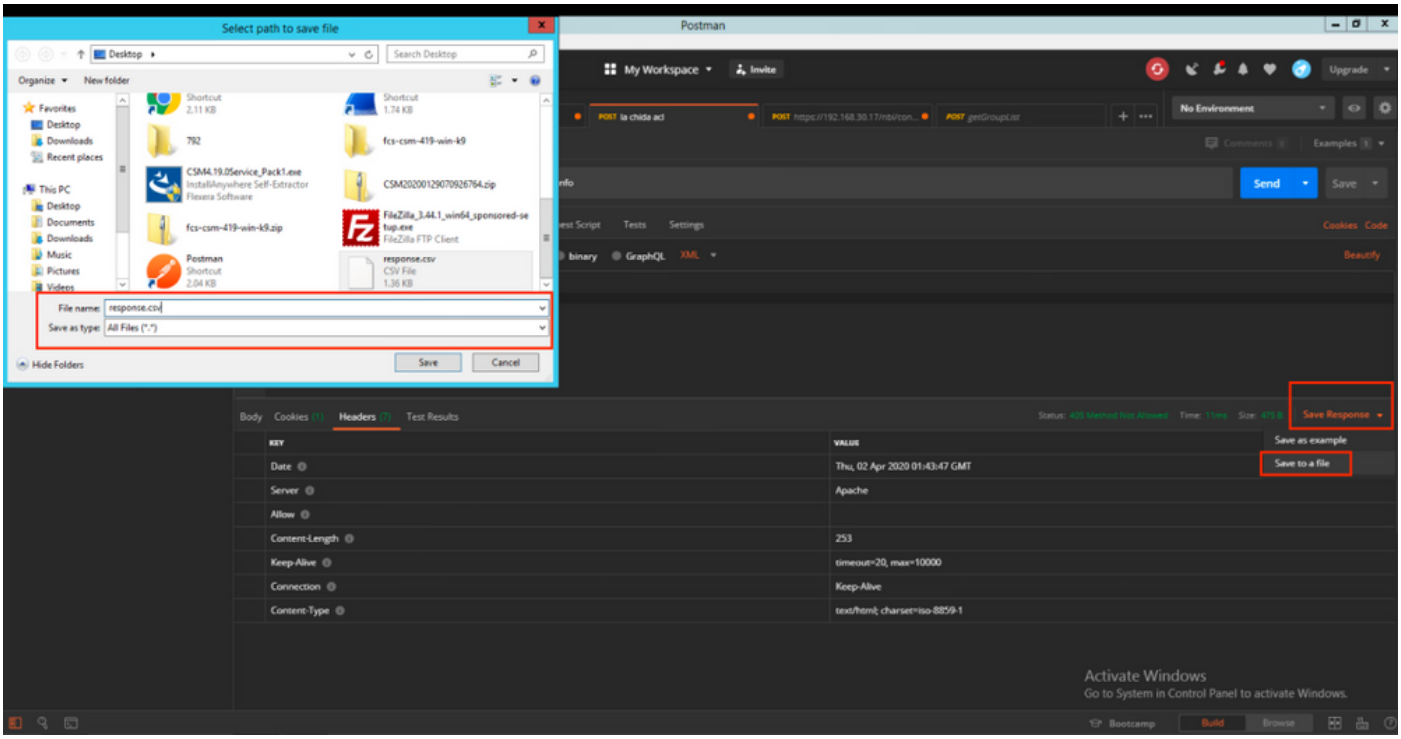


Antwort

```
<?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>
```

Überprüfung

Sie haben die Option Antwort als Datei speichern. Navigieren Sie zu **Antwort speichern > In Datei speichern.** Wählen Sie dann den Dateispeicherort aus, und speichern Sie ihn als CSV-Typ.



Dann müssen Sie diese CSV-Datei z.B. mit Excel-Anwendung öffnen können. Beim CSV-Dateityp können Sie die Ausgabe als andere Dateitypen wie PDF, TXT usw. speichern.

Fehlerbehebung

Mögliche Ausfallantworten über API.

1. Keine API-Lizenz installiert.

Ursache: API-Lizenz abgelaufen, nicht installiert oder nicht aktiviert.

Mögliche Lösung: Überprüfen Sie das Ablaufdatum der Lizenz unter **Extras > Security Manager Administration > Lizenzierungsseite.**

Überprüfen Sie, ob die API-Funktion unter **Extras > Security Manager Administration > API** aktiviert ist.

Bestätigen Sie die Einstellungen im Abschnitt **"Installation/Verifizierung** der **CSM API-Lizenz"**

weiter oben in diesem Leitfaden.

2. Falsche Verwendung der CSM-IP-Adresse für die API-Anmeldung.

Ursache: Die IP-Adresse des CSM-Servers ist in der URL des API-Aufrufs falsch.

Mögliche Lösung: Überprüfen Sie in der URL des API-Clients, ob der Hostname die richtige IP-Adresse des CSM-Servers ist.

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

3. Falsche ASA-IP-Adresse.

Ursache: Die im Body zwischen den **<**deviceIP**></**deviceIP**>**-Tags definierte IP-Adresse darf nicht die richtige sein.

Mögliche Lösung: Bestätigen Sie, dass die richtige Geräte-IP-Adresse in der Body Syntax definiert ist.

4. Keine Verbindung zur Firewall.

Ursache: Das Gerät hat keine Verbindung zum CSM.

Mögliche Lösung: Führen Sie eine Testverbindung vom CSM-Server aus, und beheben Sie weitere Verbindungsprobleme mit dem Gerät.

Weitere Informationen zu Fehlercodes und eine Beschreibung finden Sie im Cisco Security Manager API Specification Guide im nächsten Link.