Uitvoeren ACL uit CSM in CSV-formaat via API-methode

Inhoud

Inleiding

Dit document beschrijft hoe u de toegangscontrolelijsten (ACL's), in een CSV-indeling (Comma-Separated Values) van een apparaat dat door Cisco Security Manager (CSM) wordt beheerd door de CSM API-methode.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- CSM-server
- CSM API-licentie
  ```
  Product Name: L-CSMPR-API
  Product Description: L-CSMPR-API : Cisco Security Manager Pro - License to enable API Access
  ```
- Adaptieve security applicatie (ASA), beheerd door CSM
- Een API-client. Je kunt cURL, Python of Postman gebruiken. Dit artikel laat het hele proces

met Postman zien. De CSM-clienttoepassing moet worden gesloten. Als een CSM client-toepassing geopend is, moet deze geopend zijn door een andere gebruiker dan de gebruiker die de API-methode gebruikt. Anders geeft API een fout terug. Voor extra vereisten om de API functie te gebruiken kunt u de volgende gids gebruiken. API-voorwaarden

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Cisco Security Manager (CSM) heeft bepaalde functies voor de configuratie van beheerde apparaten die via API moeten worden geïmplementeerd.

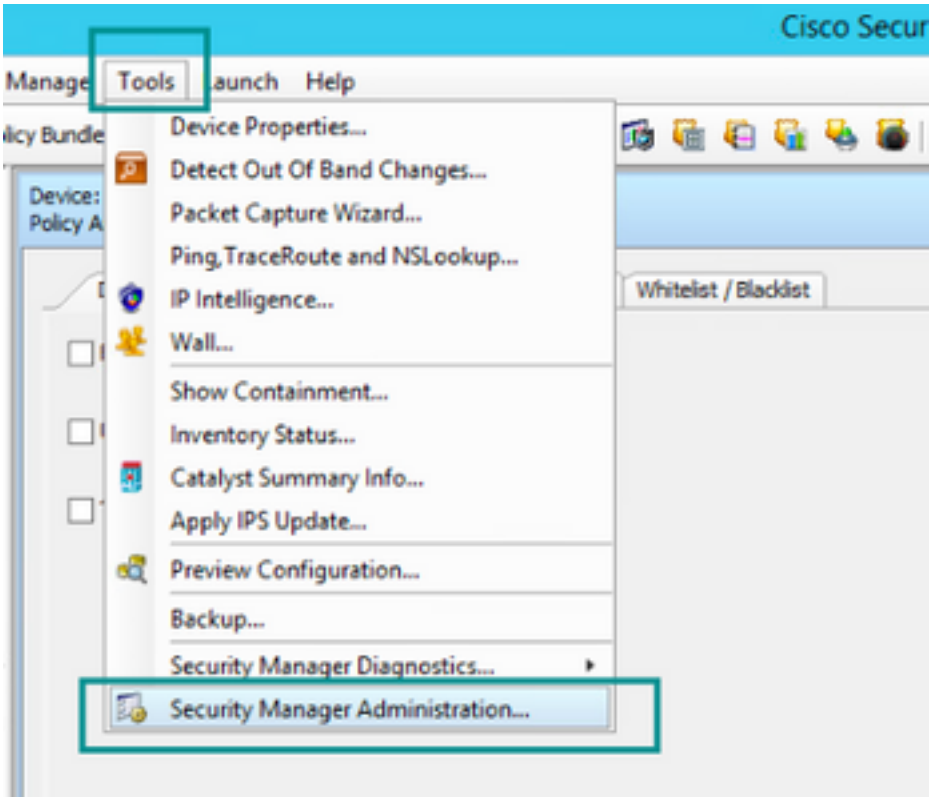
Een van deze configuratieopties is de methode om een lijst van de toegangscontrolelijst (ACL) te halen die in elk apparaat dat door CSM wordt beheerd. Het gebruik van CSM API is tot nu toe de enige manier om deze eis te verwezenlijken.

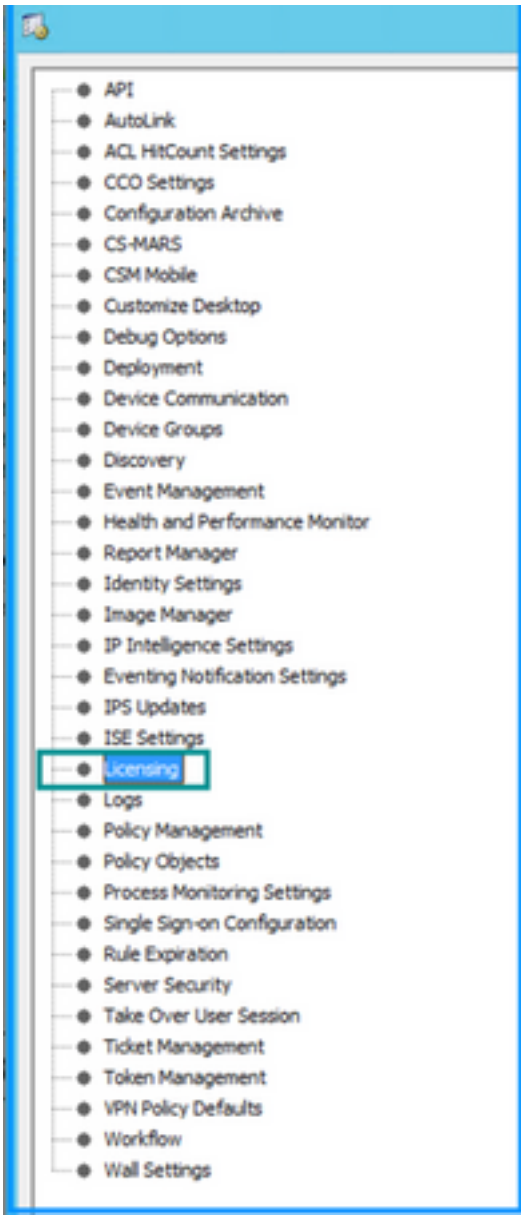
Voor deze doeleinden wordt Postman gebruikt als API-client en CSM versie 4.19 SP1, ASA 5515 versie 9.8(4).

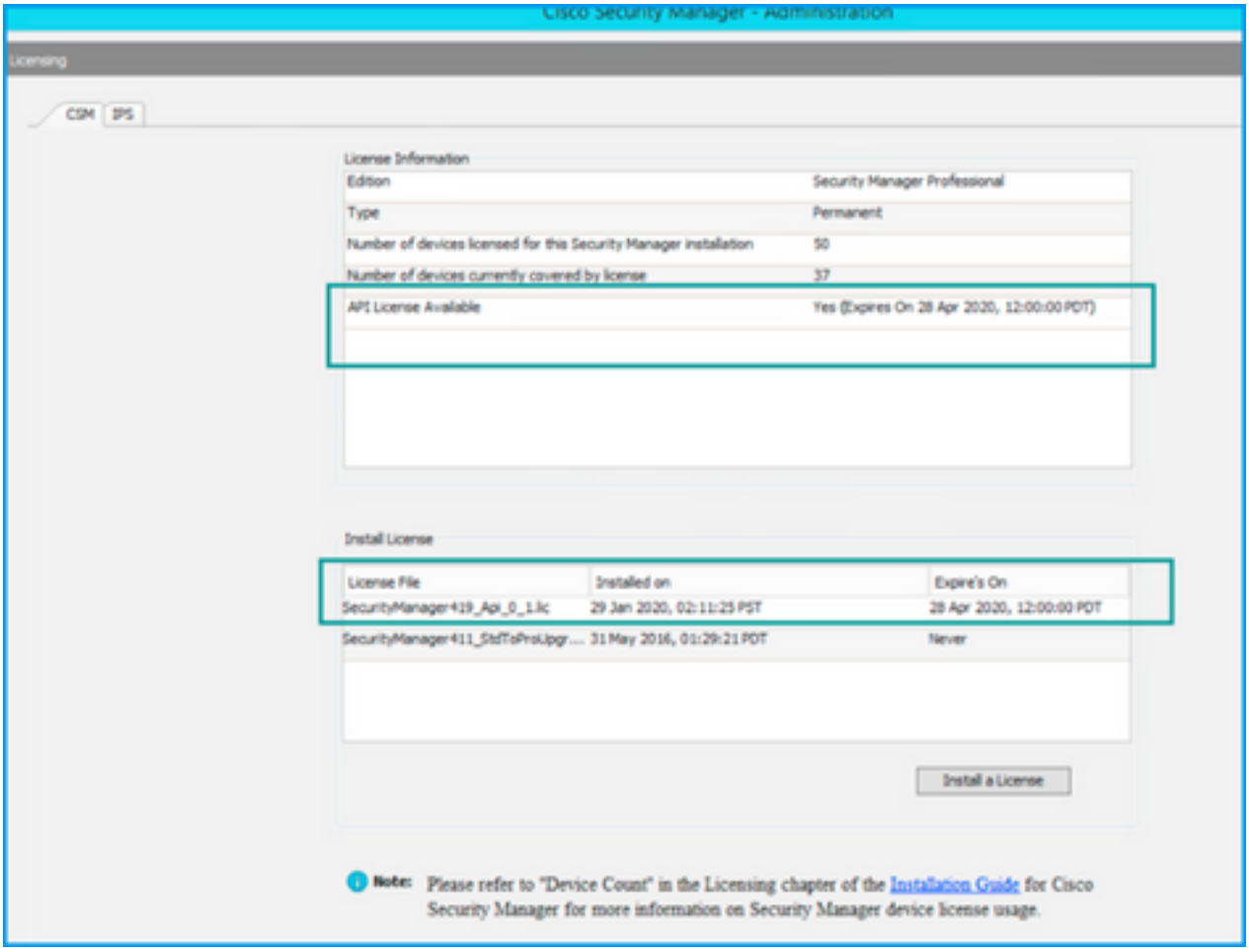
Netwerkdiagram

Installatie/verificatie van CSM API-licenties

CSM API is een gelicentieerde functie, u kunt controleren of CSM een API-licentie heeft, in de CSM-client navigeer naar **Gereedschappen > Beveiligingsbeheer > Licentiepagina** om te bevestigen dat u al een licentie hebt geïnstalleerd.


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

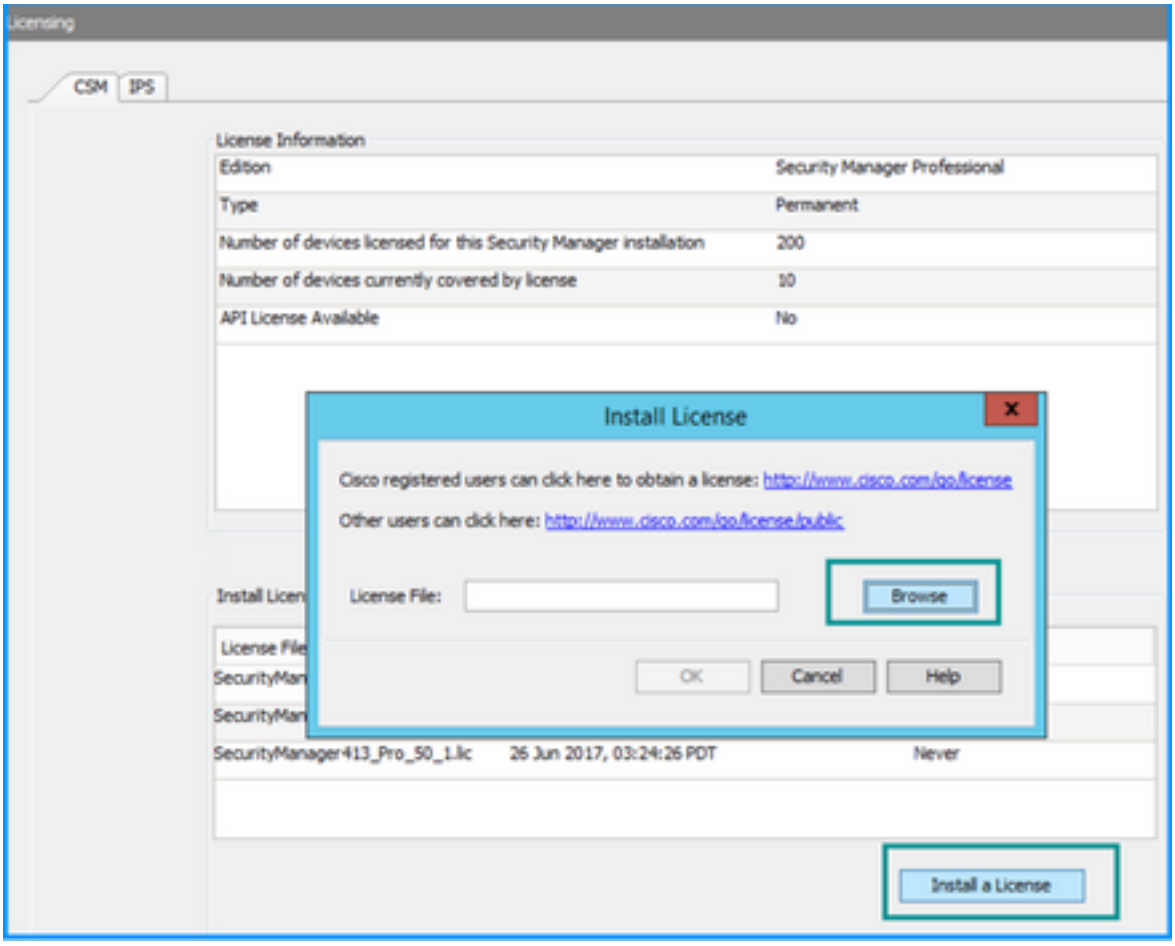

API
AutoLink
ACL HitCount Settings
CCO Settings
Configuration Archive
CS-MARS
CSM Mobile
Customize Desktop
Debug Options
Deployment
Device Communication
Device Groups
Discovery
Event Management
Health and Performance Monitor
Report Manager
Identity Settings
Image Manager
IP Intelligence Settings
Eventing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

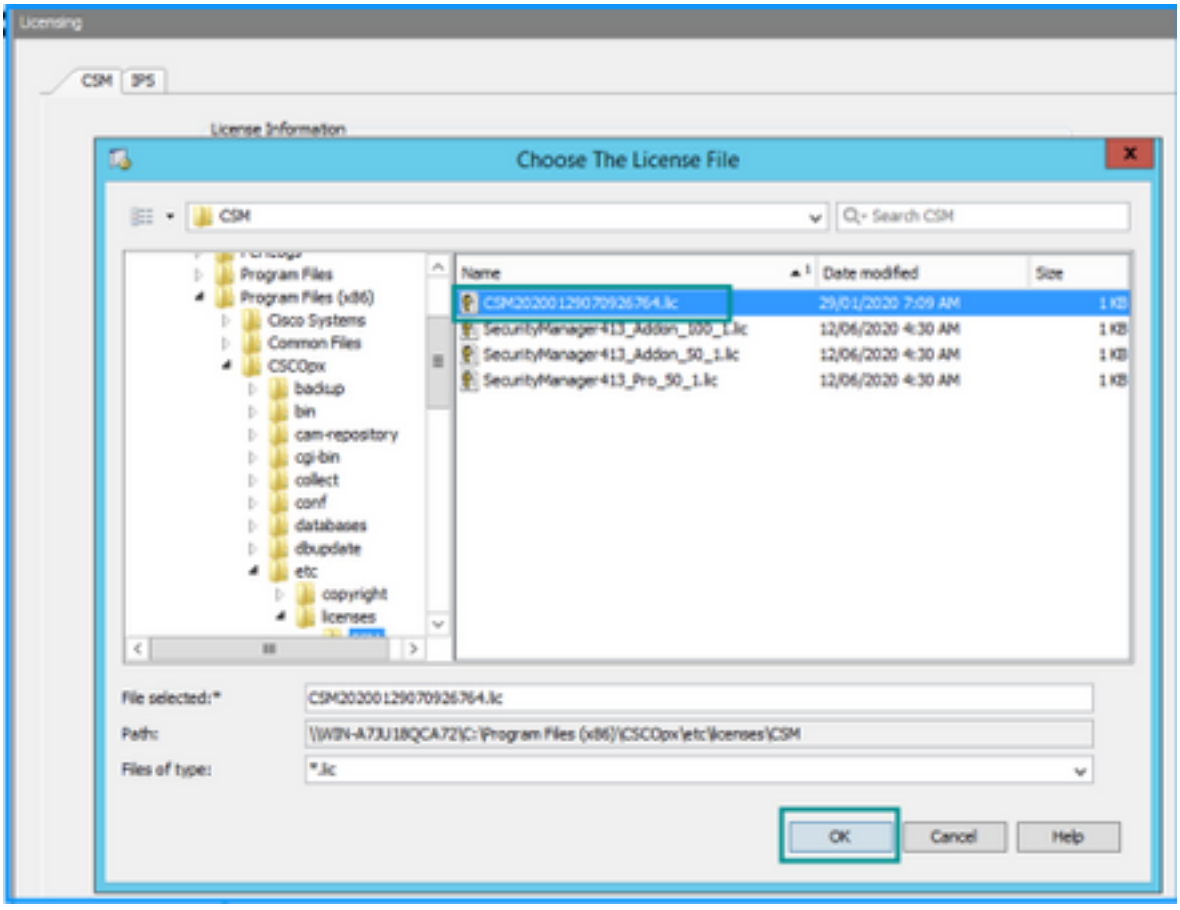


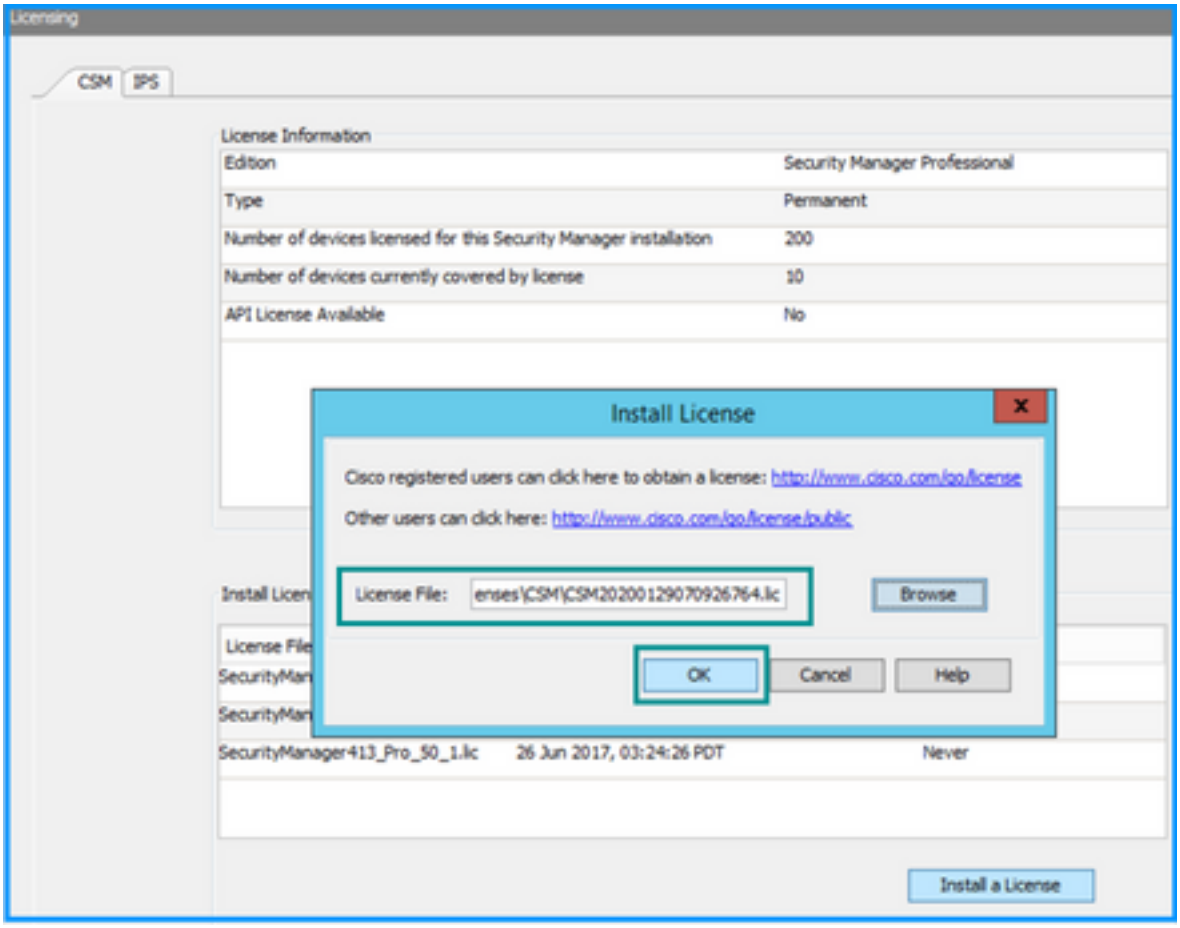
Als er geen API-licentie is toegepast maar u al het .lic-bestand hebt dat u uw licentie kunt installeren, klikt u op de knop **Installeer een licentie**. U moet het licentibestand dan opslaan op de dezelfde schijf waar de CSM-server zich bevindt.

U kunt een nieuwe Cisco Security Manager-licentie als volgt installeren:

Stap 1. Sla het aangehechte licentieserverbestand (.lic) op uit de e-mail die u naar uw bestandssysteem hebt ontvangen.
Stap 2. Kopieer het opgeslagen licentieserverbestand naar een bekende locatie in het Cisco Security Manager-serversysteem.
Stap 3. Start de Cisco Security Manager-client.
Stap 4. Navigeer naar **Gereedschappen ->Security Manager-beheer...**
Stap 5. **Selecteer Licentie** in het venster **Cisco Security Manager - Administration** in het venster
Stap 6. Klik op de knop **Installeer een** knop **Licentie**.
Stap 7. Selecteer in het dialoogvenster **Installeer** de knop **Bladeren**.
Stap 8. Navigeer naar het opgeslagen licentieserverbestand in Cisco Security Manager en selecteer de knop **OK**.
Stap 9. Klik in het dialoogvenster **Installeer Licentie** op de knop **OK**.
Stap 10. Bevestig de weergegeven informatie over de Licentie en klik op de knop **Sluiten**.


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



De API-licentie kan alleen worden toegepast op een server die onder licentie is geplaatst voor de CSM professionele editie. De licentie kan niet worden toegepast op CSM via een standaardeditie van de licentie. API-licentievereisten

Configuratiestappen

API-clientinstellingen

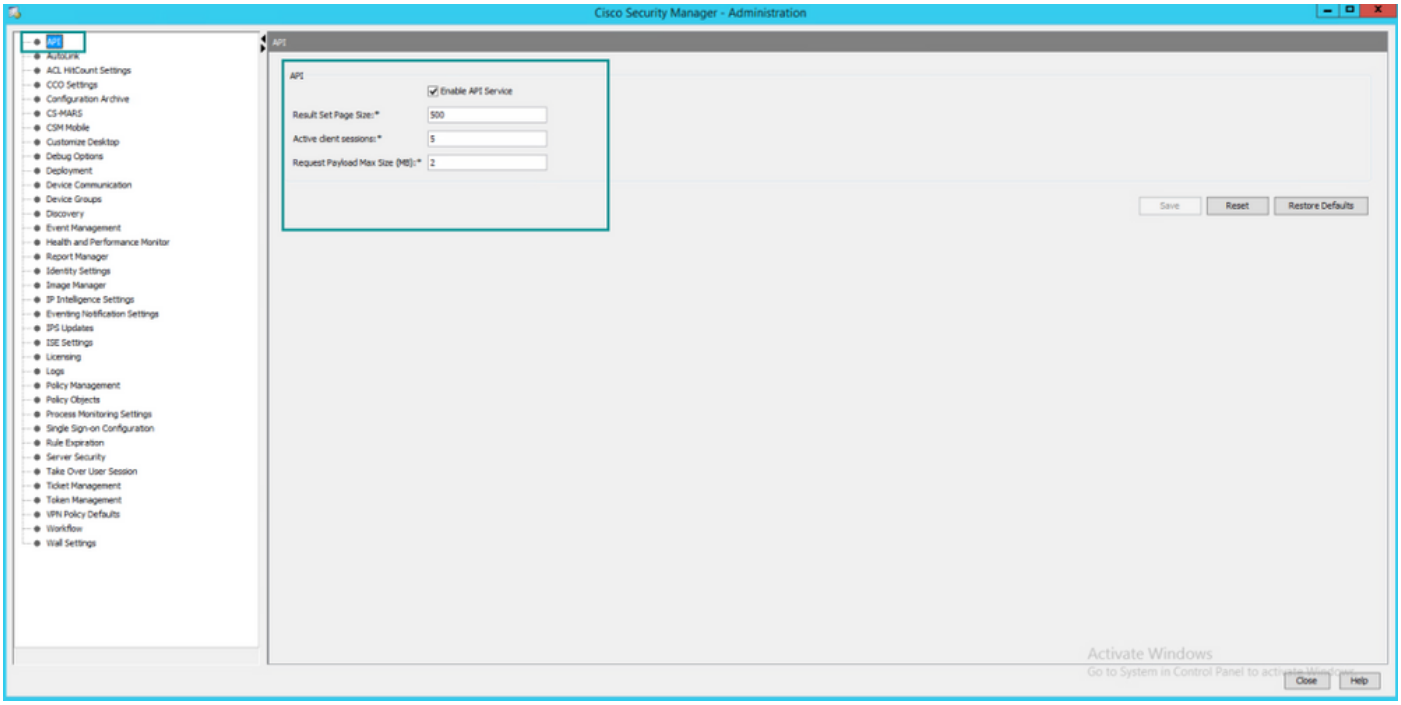
Als u Postman gebruikt zijn er een aantal instellingen die u moet configureren, hangt het af van elke API-client maar moet deze vergelijkbaar zijn.

- Proxy uitgeschakeld
- SSL-verificatie - OFF

CSM-instellingen

- Ingeschakeld API. Onder **Gereedschappen > Security Manager-beheer > API**

API-
instellingen



Werken met CSM API

U dient de volgende twee oproepen in de API-client te configureren:

1. Aanmelden

2. Verkrijg ACL-waarden

Voor referentie door middel van het proces:

CSM toegangsgegevens in dit laboratorium:

CSM Hostname (IP-adres): **192.168.66.116**. In de API gebruiken we de hostname in de URL.

Gebruiker: **besturen**

Wachtwoord: **Admin123**

Inlogmethode

Deze methode moet worden gebruikt vóór elke andere methode die op andere diensten wordt toegepast.

CSM API-gids: Methode om in te loggen

Aanvragen

1. HTTP-methode: **POST**

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

3. Tekst:

Wanneer:

Username: De gebruikersnaam van de CSM-client is gekoppeld aan de sessie

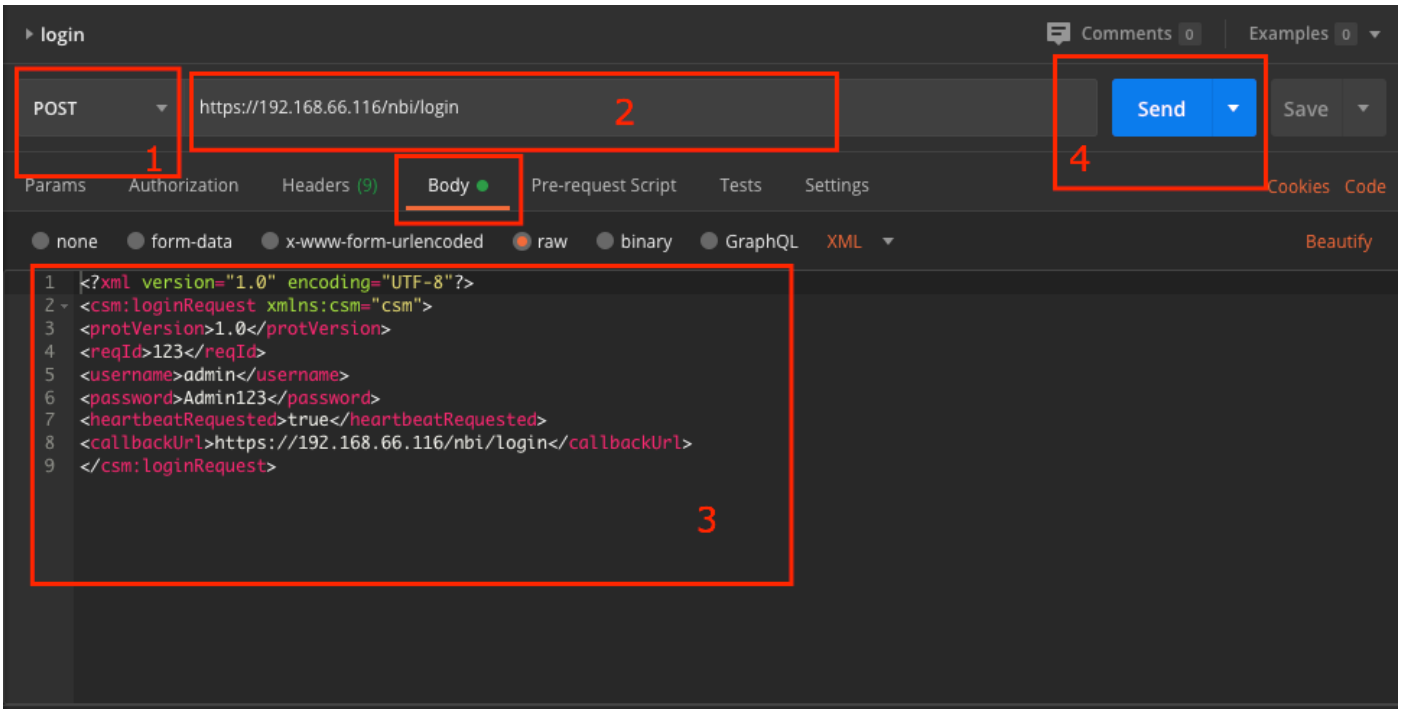
Wachtwoord: Het CSM client wachtwoord dat aan de sessie is gekoppeld.

reqID: Deze eigenschap identificeert een verzoek dat door de client wordt gedaan uniek, deze waarde echoën door de CSM Server in de geassocieerde reactie. Het kan worden ingesteld op alles wat de gebruiker als identificator wil gebruiken.

hartslagVereiste: Deze eigenschap kan naar keuze worden gedefinieerd. Als de eigenschap op waar wordt ingesteld, dan ontvangt de CSM client een hartslag callback van de CSM server. De server probeert de client te pingelen met een frequentie dichtbij (inactiviteit tijd uit) / 2 minuten. Als de client niet reageert op de hartslag, dan probeert API de hartslag tijdens het volgende interval opnieuw uit. Als de hartslag succesvol is, dan wordt de sessie-inactiviteit-tijd gereset.

callbackUrl: De URL waarmee de CSM server de callback maakt. Dit moet worden gespecificeerd indien het gevraagde hartslag juist is. Alleen HTTPS gebaseerde callback URL's zijn toegestaan

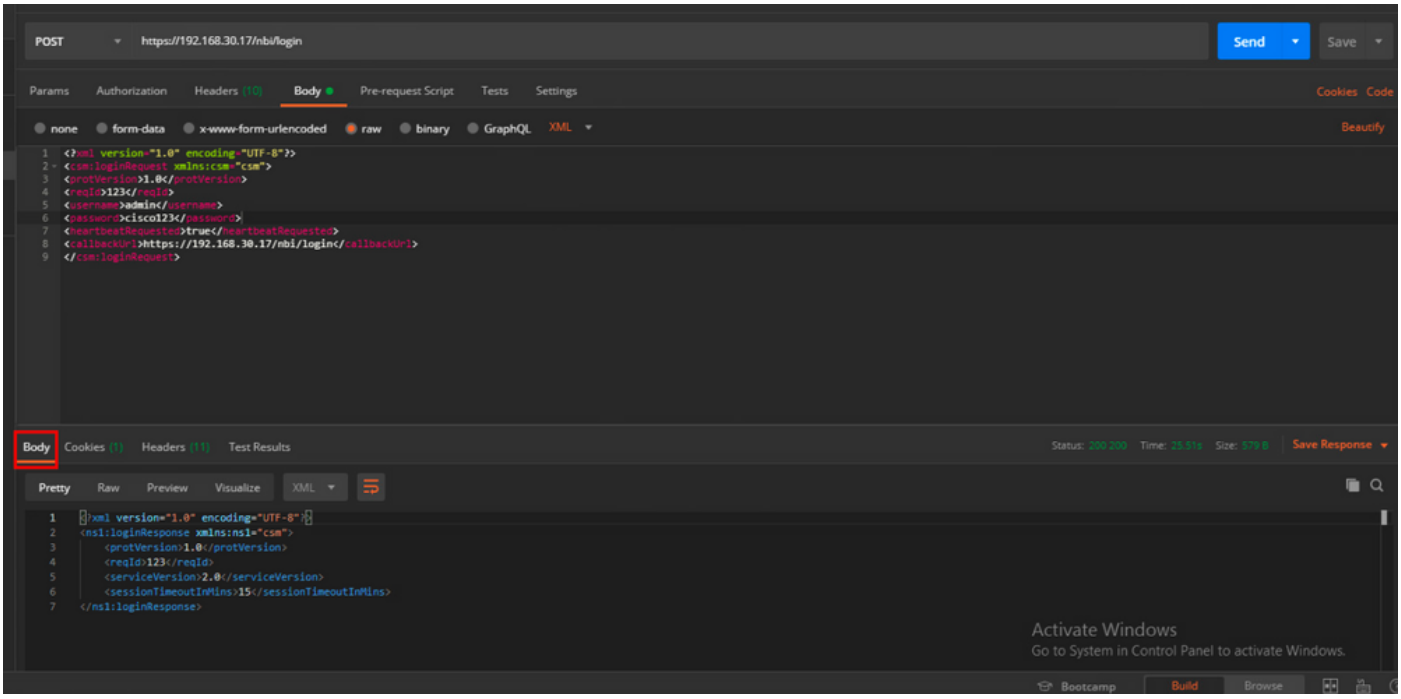
4. Verzend



Selecteer de ruwe optie om te zien zoals in dit voorbeeld.

respons

Login API bevestigt de gebruikersreferenties en geeft een sessiemenk terug als een veilig koekje. De waarde van de sessie wordt opgeslagen onder de **asCookie**-toets, u moet deze **als Cookie-waarde** opslaan.



ACL-regels verkrijgen

Methode execdeviceReadOnlyCLICmds. De reeks opdrachten die door deze methode kunnen worden uitgevoerd, is alleen-lezen opdrachten zoals statistieken, controleopdrachten die aanvullende informatie over de werking van het specifieke apparaat bieden.

Methode details van de CSM API-gebruikersgids

Aanvragen

1. HTTP-methode: **POST**

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

3. HTTP-header: Het cookie die wordt teruggestuurd door de inlogmethode die de authenticatiesessie identificeert.

Eerder verkregen waarde invoeren **als** Cookie-waarde bij methodevastlegging.

Sleutel: Voer "asCookie" in

Value: Invoerwaarde verkregen.

Klik op een selectieteken om het kinderslot in te schakelen.

4. Tekst:

Opmerking: Het XML lichaam hierboven kan gebruikt worden om elke "show" opdracht uit te voeren, bijvoorbeeld: "toon run all", "show run object", "show run nat" enz.
Het XML "<deviceReadOnlyCLICmd>"-element geeft aan dat de opdracht die gespecificeerd is in "<cmd>" en "<argument>" alleen gelezen MOET worden.

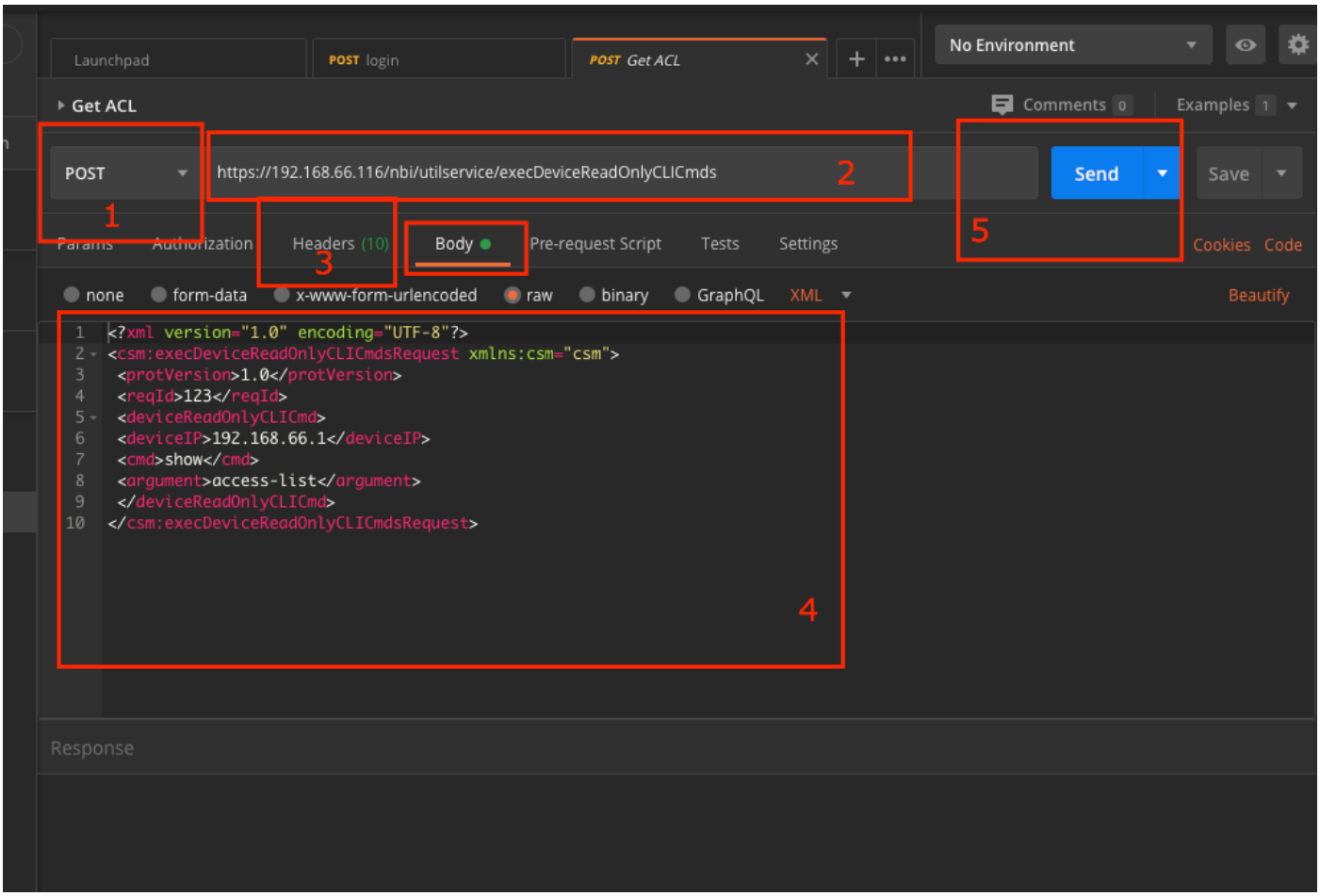
Wanneer:

apparaatIP: Het IP-adres van het apparaat waartegen de opdracht moet worden uitgevoerd.

cmd : Vaste opdracht **"show".** Met regex wordt gemengd geval [sS][hH][oO][wW] toegestaan

argument: De show commandoargumenten. Zoals "run" om de actieve configuratie van het apparaat te tonen of **"access-list"** om de details van de toegangslijst weer te geven.

5. Verzend

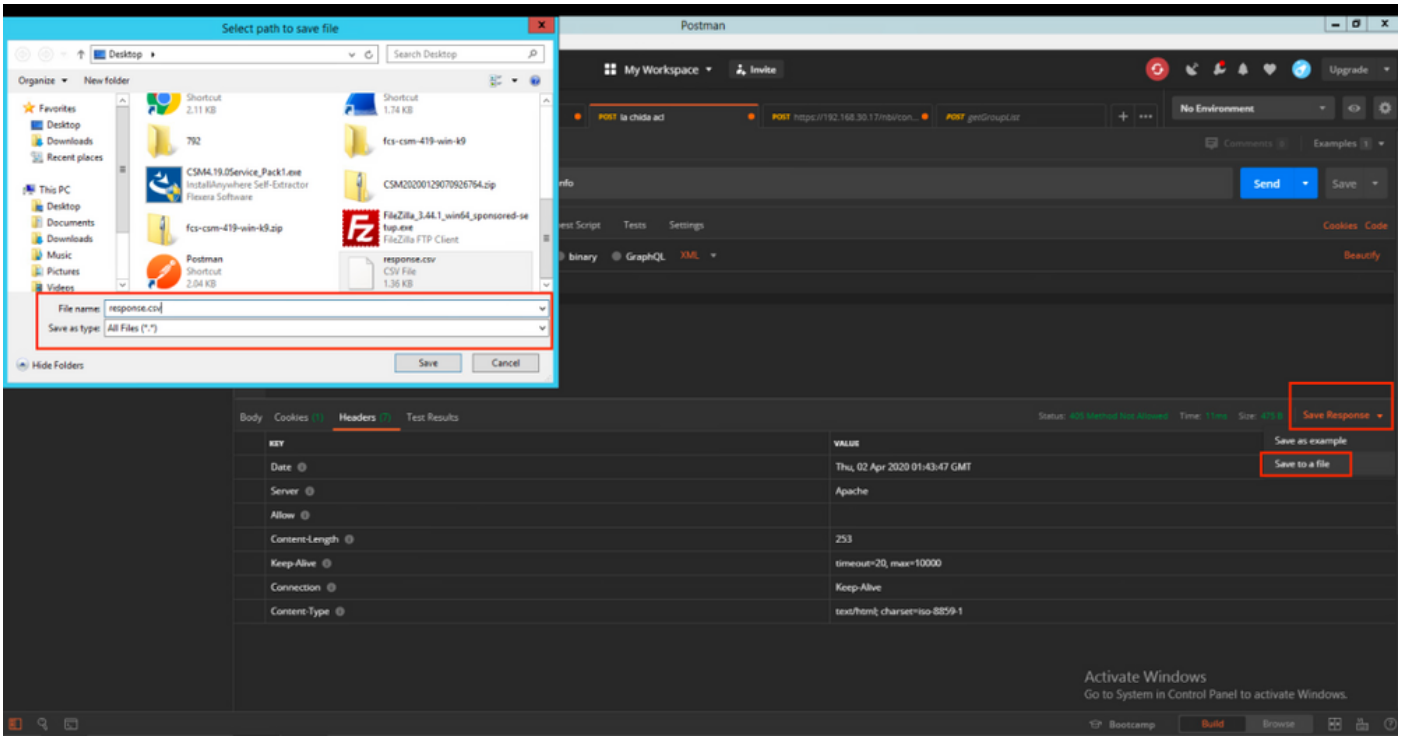


respons

```
<?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>
```


Verifiëren

U hebt de optie om respons als bestand op te slaan. Navigeren in om **respons op te slaan > Opslaan naar een bestand.** Selecteer vervolgens de bestandslocatie en bewaar het als een .csv-type.



U moet dit .csv-bestand bijvoorbeeld met Excel-toepassing kunnen openen. Van het type .csv-bestand kunt u de uitvoer opslaan als andere bestandstypen, zoals PDF, TXT, enzovoort.

Problemen oplossen

Mogelijke mislukkingsreacties met API.

1. Er is geen API-licentie geïnstalleerd.

Oorzaak: API-licentie verlopen, niet geïnstalleerd of niet ingeschakeld.

Mogelijke oplossing: Controleer de verloopdatum van de licentie, onder **Gereedschappen > Security Manager Administration > Licensing pagina**

Controleer of de API-functie is ingeschakeld onder **Gereedschappen > Security Manager Management > API**

Controleer de instellingen voor het gedeelte van de **installatie/verificatie** van de **CSM API-licentie** boven in deze handleiding.

2. Slecht CSM IP-adres voor de inlognaam van API.

Oorzaak: IP-adres van de CSM Server is fout in de URL van de API-oproep.

Mogelijke oplossing: Controleer in de URL van de API client dat de hostname het juiste IP-adres van de CSM server is.

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

3. Onjuist ASA IP-adres.

Oorzaak: Het IP-adres dat op het lichaam wordt gedefinieerd tussen de <deviceIP></deviceIP>-tags moet niet het juiste zijn.

Mogelijke oplossing: Bevestig dat het juiste IP-adres voor het apparaat is gedefinieerd door de Body Syntax.

4. Geen verbinding met de firewall.

Oorzaak: Het apparaat heeft geen verbinding met CSM

Mogelijke oplossing: Start een Test Connectivity van de CSM server en ontwikkel verdere connectiviteit op het apparaat.

Voor verdere foutcodes en beschrijving vind u meer details in de Cisco Security Manager API Specification Guide in de volgende link.