Extraia a ACL do CSM no formato CSV através do método API

Contents

Introduction

Este documento descreve como extrair a ACL (Access Control Lists, listas de controle de acesso), no formato CSV (Comma-Separated Values, valores separados por vírgula), de um dispositivo gerenciado pelo Cisco Security Manager (CSM) através do método de API do CSM.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Security Manager (CSM)
- API CSM
- conhecimento básico de API

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Servidor CSM
- licença de API CSM
  ```
  Product Name: L-CSMPR-API
  Product Description: L-CSMPR-API : Cisco Security Manager Pro - License to enable API Access
  ```
- ASA (Adapative Security Appliance, dispositivo de segurança adaptável) gerenciado pelo CSM

- Um cliente de API. Você pode usar cURL, Python ou Postman. Este artigo demonstra todo o processo com o Postman. O aplicativo cliente CSM deve ser fechado. Se um aplicativo cliente CSM estiver aberto, deve ser feito por um usuário diferente daquele que usa o método API. Caso contrário, a API retorna um erro. Para pré-requisitos adicionais para usar o recurso API, você pode usar o próximo guia. Pré-requisitos de API

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O Cisco Security Manager (CSM) tem algumas funcionalidades para a configuração de dispositivos gerenciados que precisam ser implementadas através da API.

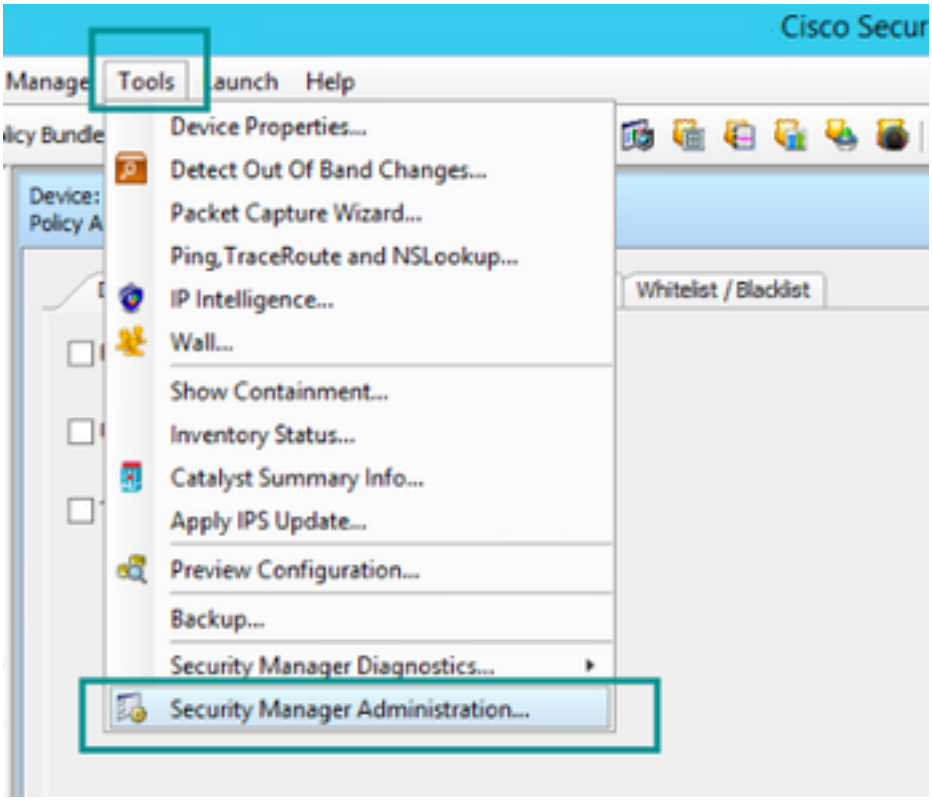
Uma dessas opções de configuração é o método para extrair uma lista da ACL (Access Control List, lista de controle de acesso) configurada em cada dispositivo gerenciado pelo CSM. O uso da API do CSM é a única forma de atingir esse requisito até agora.

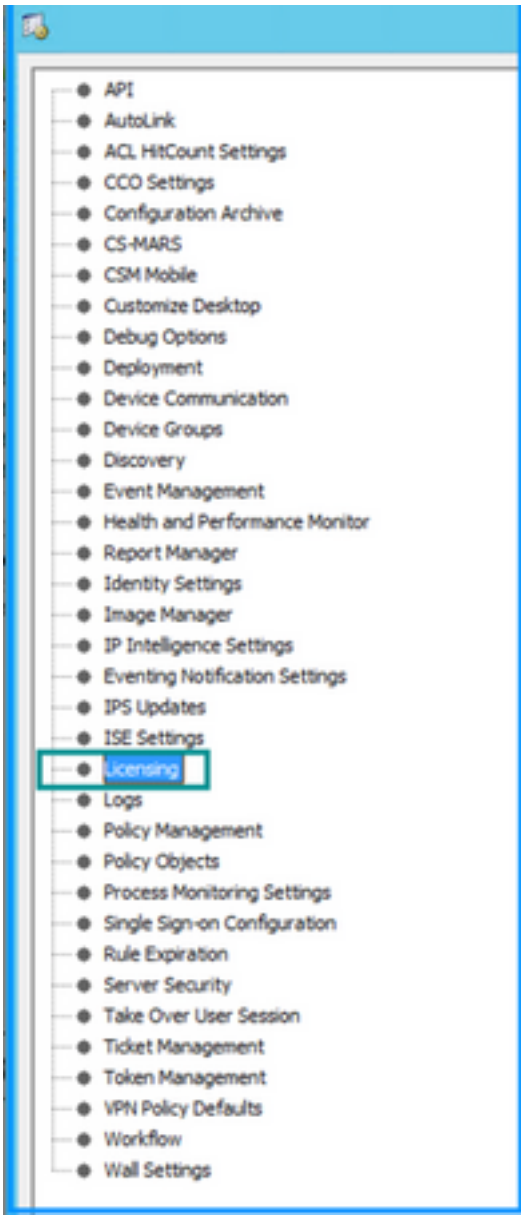
Para esses fins, o Postman usou como Cliente API e CSM versão 4.19 SP1, ASA 5515 versão 9.8(4).

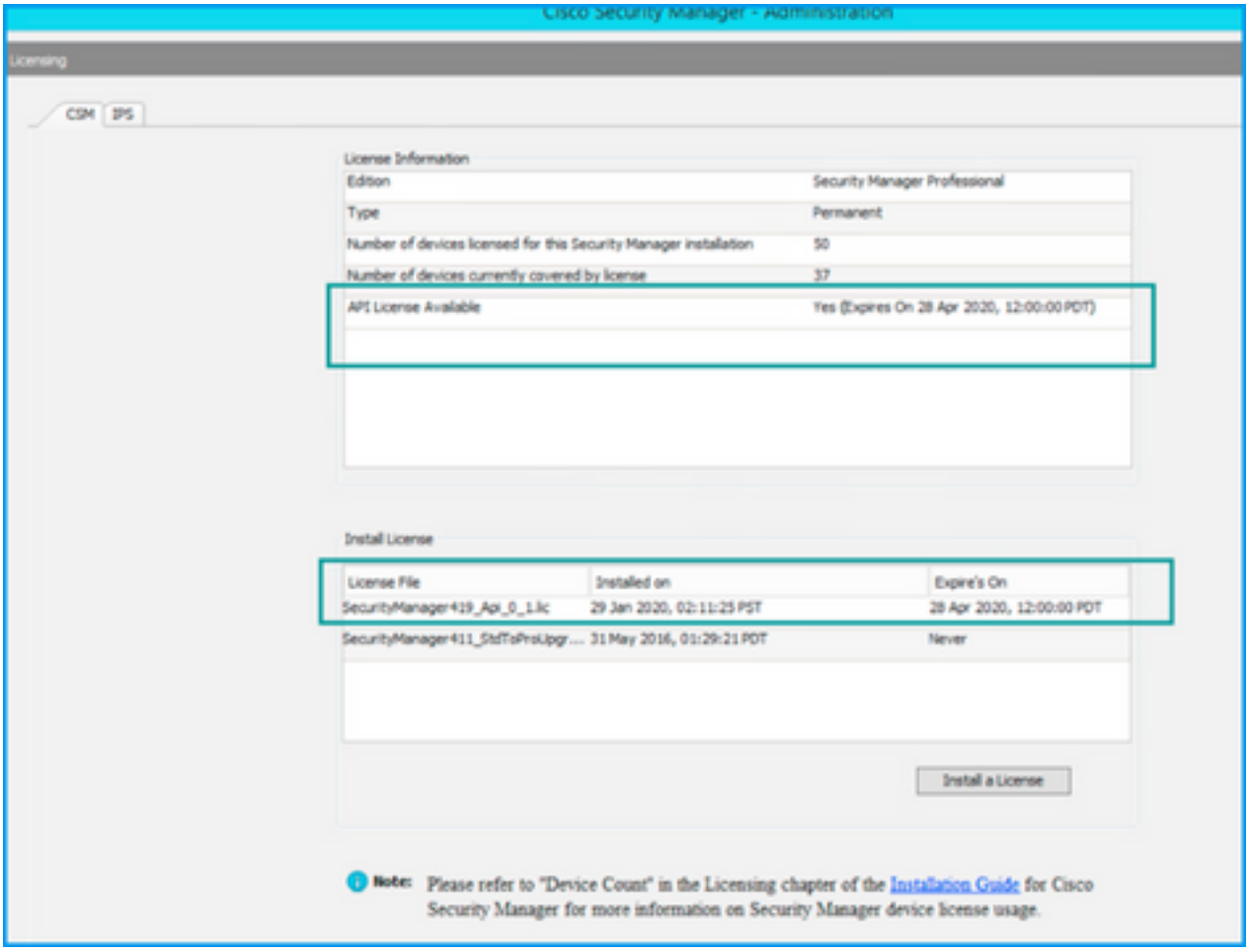
Diagrama de Rede

Instalação/verificação de licença de API CSM

A API do CSM é um recurso licenciado. Você pode verificar se o CSM tem uma licença de API, no cliente do CSM, navegue para **Ferramentas > Administração do Security Manager > Licenciamento** para confirmar se você já tem uma licença instalada.


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

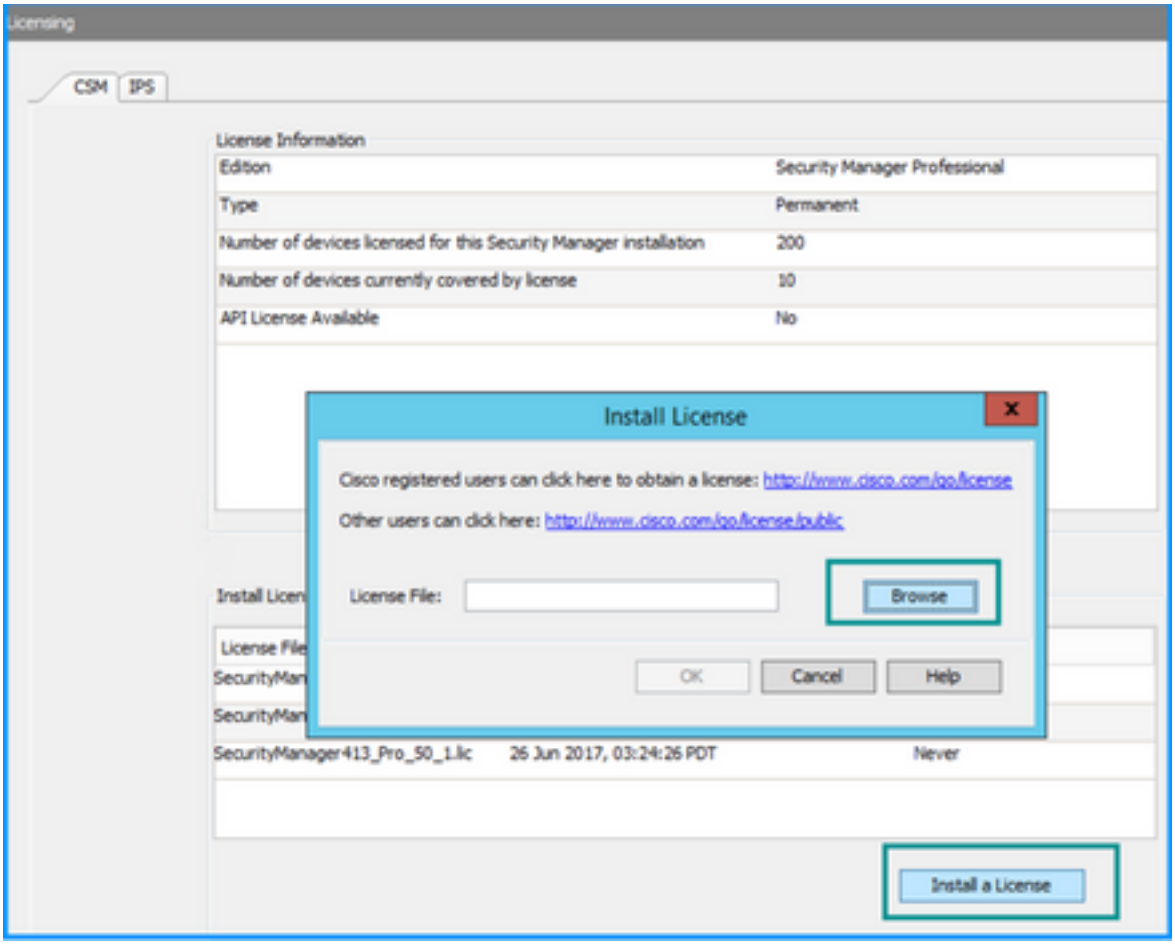

API
AutoLink
ACL HitCount Settings
CCO Settings
Configuration Archive
CS-MARS
CSM Mobile
Customize Desktop
Debug Options
Deployment
Device Communication
Device Groups
Discovery
Event Management
Health and Performance Monitor
Report Manager
Identity Settings
Image Manager
IP Intelligence Settings
Eventing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

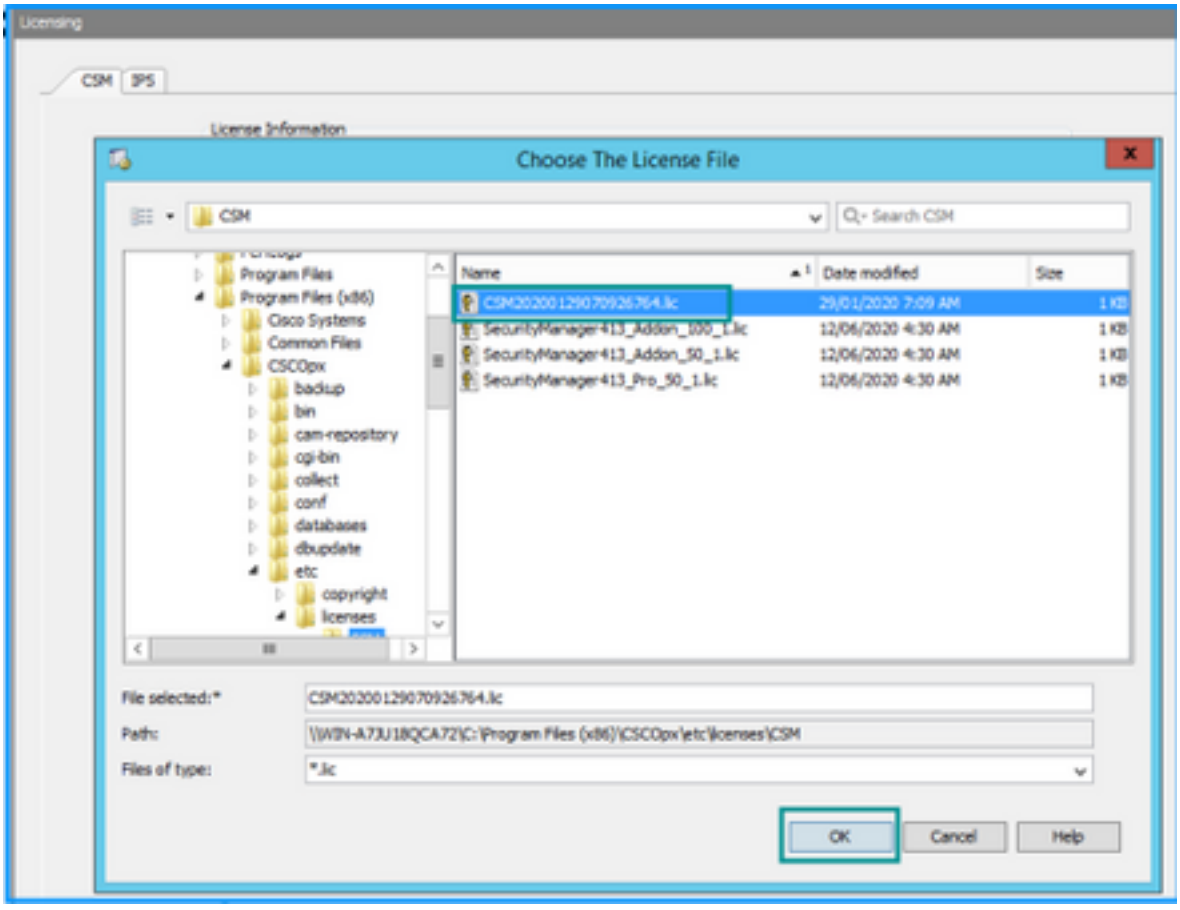


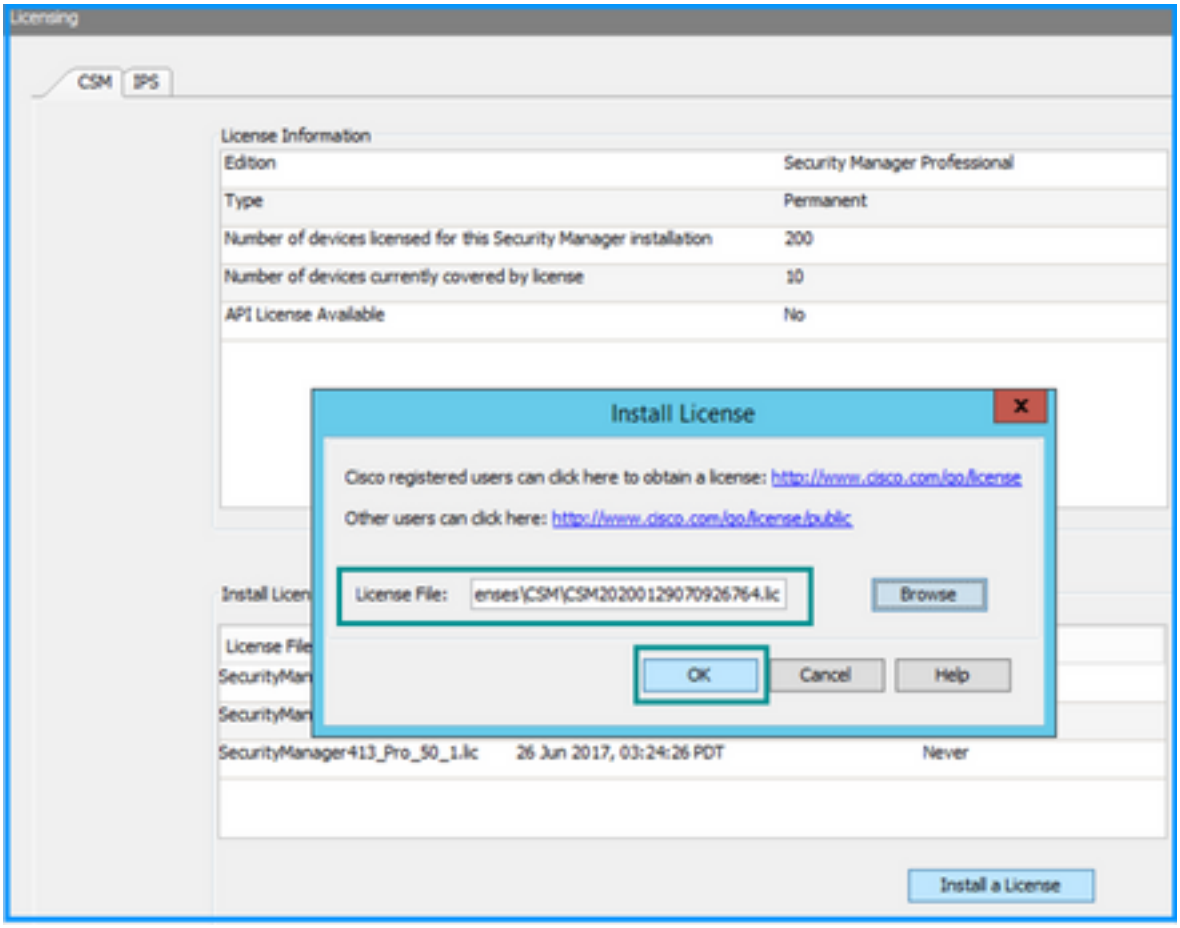
Se não houver licença de API aplicada, mas você já tiver o arquivo .lic que pode instalar sua licença, clique no botão **Instalar uma licença**, você deve armazenar o arquivo de licença no mesmo disco onde o servidor CSM está localizado.

Para instalar uma licença mais recente do Cisco Security Manager, siga estas etapas:

Etapa 1. Salve o arquivo de licença anexado (.lic) do e-mail que você recebeu no sistema de arquivos.
Etapa 2. Copie o arquivo de licença salvo para um local conhecido no sistema de arquivos do servidor do Cisco Security Manager.
Etapa 3. Inicie o Cisco Security Manager Client.
Etapa 4. Navegue até **Ferramentas->Administração do Gerenciador de Segurança...**
Etapa 5. Na janela **Cisco Security Manager - Administration**, selecione **Licensing**
Etapa 6. Clique no botão **Instalar uma licença**.
Passo 7. Na caixa de diálogo **Instalar licença**, selecione o botão **Procurar**.
Etapa 8. Navegue até o arquivo de licença salvo no sistema de arquivos do servidor do Cisco Security Manager e selecione o botão **OK**.
Etapa 9. Na caixa de diálogo **Instalar licença**, clique no botão **OK**.
Etapa 10. Confirme as informações de Resumo da licença exibidas e clique no botão **Fechar**.


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



A licença da API só pode ser aplicada em um servidor licenciado para a edição profissional do CSM. A licença não pode ser aplicada ao CSM que executa uma edição padrão da licença.
Requisitos de licença de API

Configuration Steps

Configurações do cliente API

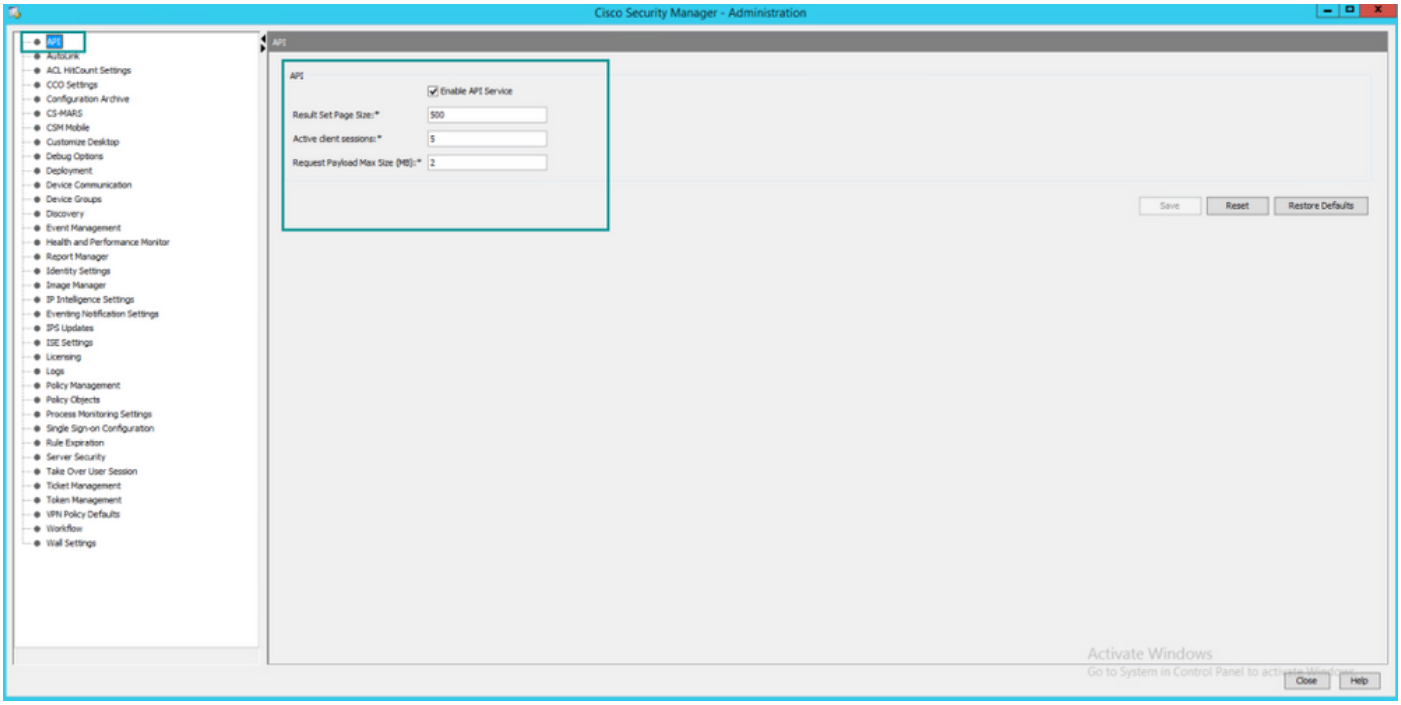
Se você usa o Postman, há algumas configurações que você precisa configurar, depende de cada cliente de API, mas deve ser semelhante.

- Proxy desabilitado
- Verificação SSL - DESLIGADO

Configurações do CSM

- API ativada. Em **Ferramentas > Administração do Security Manager > API**

Configurações de
API



Trabalhar com API CSM

Você precisa configurar no cliente API as duas chamadas abaixo:

1. Método de login

2. Obter valores de ACL

Para referência através do processo:

Detalhes de acesso CSM usados neste laboratório:

Nome de host CSM (endereço IP): **192.168.66.116.** Na API, usamos o nome de host na URL.

Usuário: **admin**

Senha: **Admin123**

Método de login

Esse método deve ser chamado antes de qualquer outro método chamado em outros serviços.

Guia de API do CSM: Login do método

Requisição

1. Método de HTTP: **POST**

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

3. Corpo:

Where:

Nome de usuário: O nome de usuário do cliente CSM associado à sessão

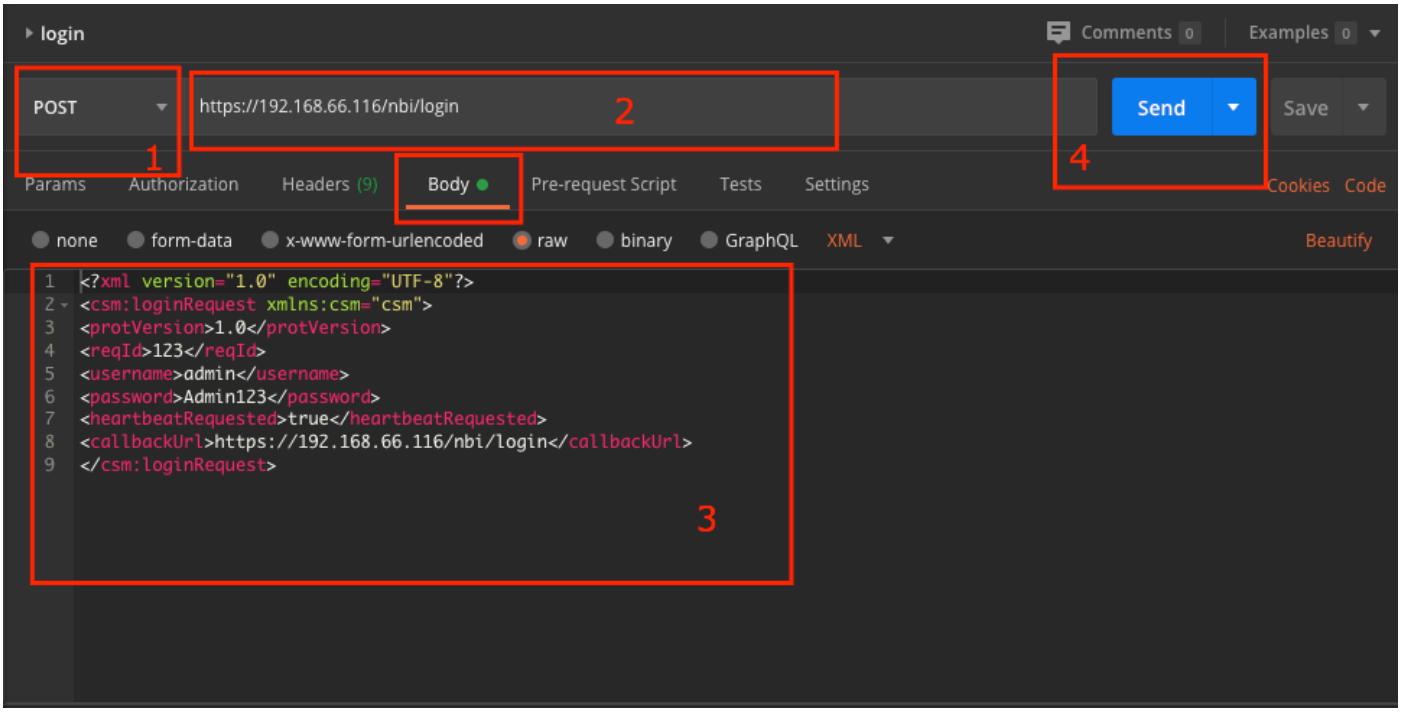
Senha: A senha do cliente CSM associada à sessão.

reqId: Este atributo identifica exclusivamente uma solicitação feita pelo cliente, esse valor ecoa pelo servidor CSM na resposta associada. Ele pode ser definido para qualquer coisa que o usuário queira usar como um identificador.

heartbeat solicitado: Esse atributo pode ser opcionalmente definido. Se o atributo estiver definido como verdadeiro, o cliente CSM receberá um retorno de chamada de pulsação do servidor CSM. O servidor tenta fazer ping no cliente com uma frequência próxima a (tempo limite de inatividade) / 2 minutos. Se o cliente não responder ao ritmo cardíaco, a API repetirá o ritmo cardíaco durante o próximo intervalo. Se o heartbeat for bem-sucedido, o tempo limite de inatividade da sessão será redefinido.

callbackUrl: O URL no qual o servidor CSM faz o retorno de chamada. Isso precisa ser especificado se o heartbeatRequested é verdadeiro. Somente URLs de retorno de chamada baseados em HTTPS são permitidos

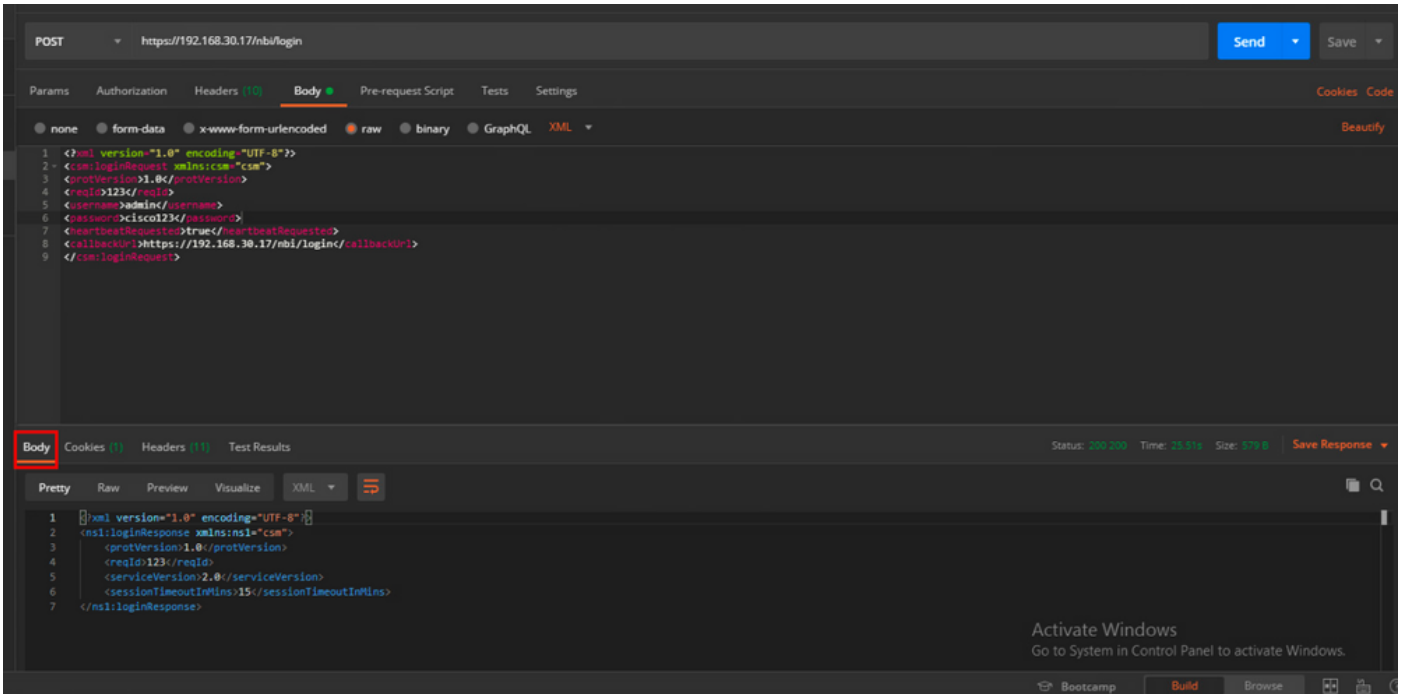
4. Enviar



Selecione a opção bruta para ver como neste exemplo.

Resposta

A API de Logon valida as credenciais do usuário e retorna um token de sessão como um cookie seguro. O valor da sessão é armazenado na chave **asCookie**, você deve salvá-lo **comoCookie**.



Obter regras de ACL

Método execDeviceReadOnlyCLICmds. O conjunto de comandos que podem ser executados por esse método são comandos somente leitura, como estatísticas, comandos de monitoramento que fornecem informações adicionais sobre a operação do dispositivo específico.

Detalhes do método no Guia do usuário da API do CSM

Requisição

1. Método de HTTP: **POST**

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

3. Cabeçalho HTTP: O cookie retornado pelo método de login que identifica a sessão de autenticação.

Valor de entrada **asCookie** obtido anteriormente do Login do método.

Chave: Digite "asCookie"

Valor: Valor de entrada obtido.

Clique na caixa de seleção para ativá-la.

4. Corpo:

Note: O corpo XML acima pode ser usado para executar qualquer comando "show", por exemplo: "show run all", "show run object", "show run nat" etc.

O elemento XML "<deviceReadOnlyCLICmd>" indica que o comando especificado em "<cmd>" e "<argumento>" DEVE ser somente leitura.

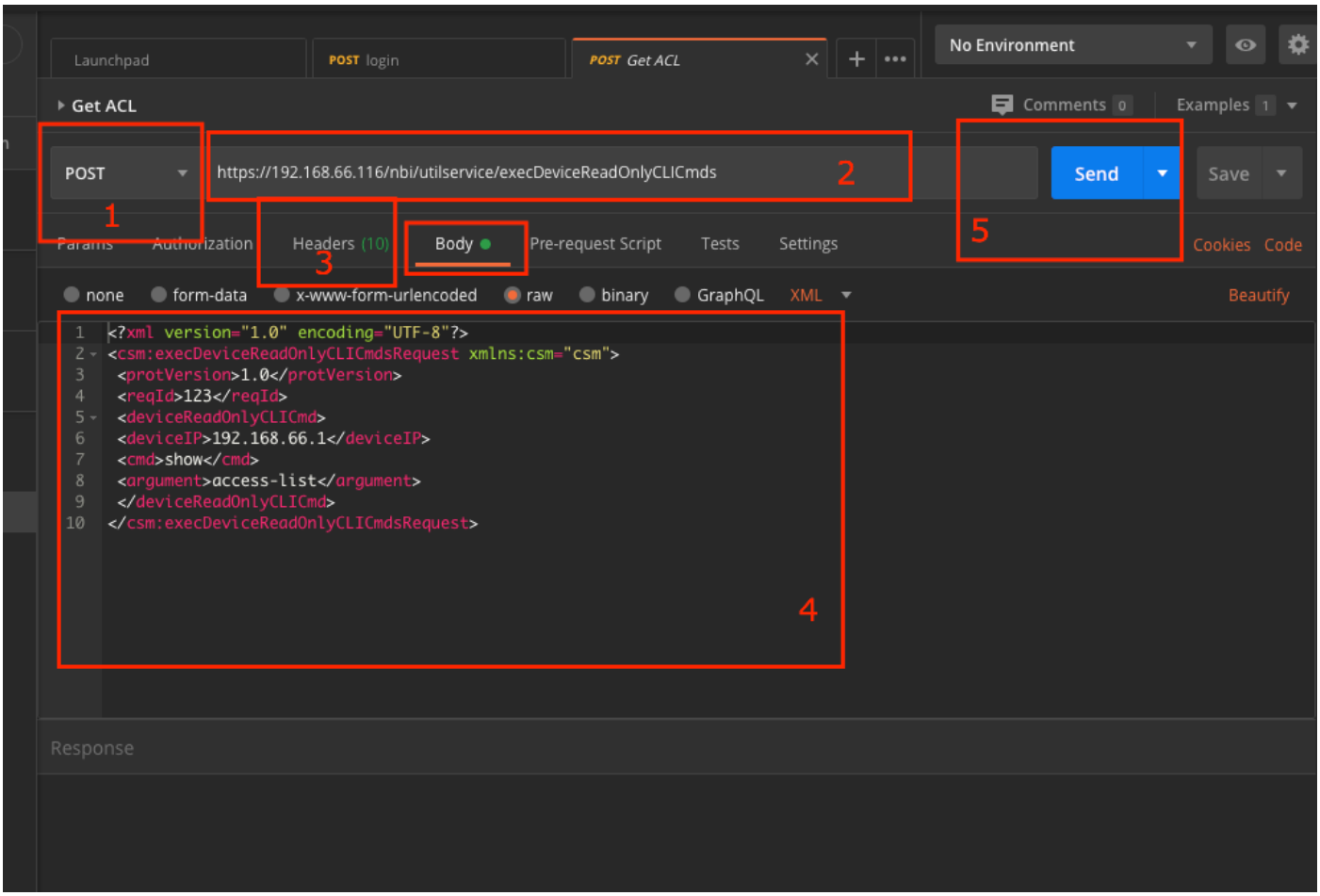
Where:

IP do dispositivo: O endereço IP do dispositivo com o qual o comando deve ser executado.

cmd: Comando fixo **"show".** O regex permite maiúsculas/minúsculas [sS][hH][oO][wW]

argumento: Os argumentos do comando show. Como "executar" para mostrar a configuração atual do dispositivo ou **"lista de acesso"** para mostrar os detalhes da lista de acesso.

5. Enviar

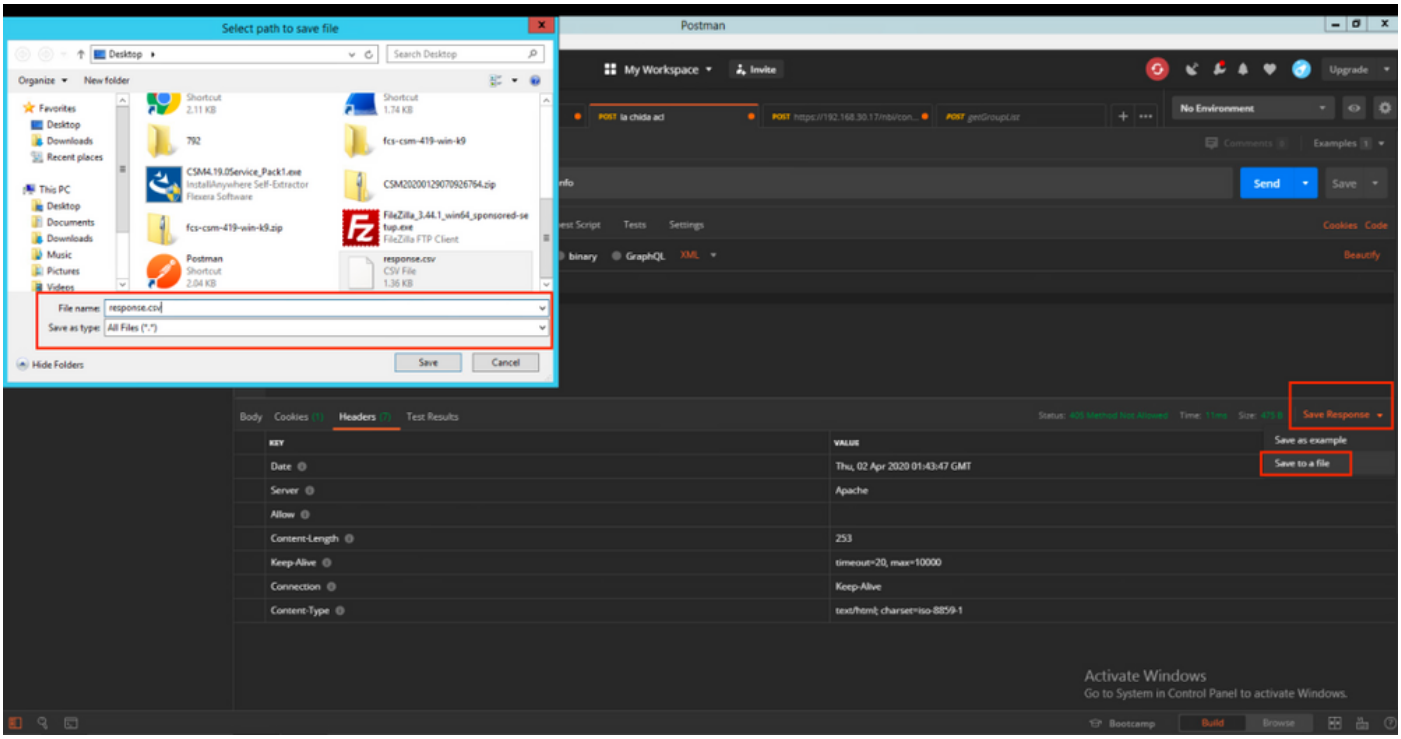


Resposta

```
<?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>
```

Verificar

Você tem a opção Salvar resposta como um arquivo. Navegue até **Salvar resposta > Salvar em um arquivo.** Em seguida, selecione o local do arquivo e salve-o como um tipo .csv.



Em seguida, você deve ser capaz de abrir esse arquivo .csv com o aplicativo Excel, por exemplo. No tipo de arquivo .csv, você pode salvar a saída como outros tipos de arquivo, como PDF, TXT etc.

Troubleshoot

Possíveis respostas de falha usando API.

1. Nenhuma licença de API instalada.

Causa: Licença de API expirada, não instalada ou não habilitada.

Possível solução: Verifique a data de validade da licença, em **Ferramentas > Administração do Security Manager > Página de Licenciamento**

Verifique se o recurso API está habilitado em **Ferramentas > Administração do Security Manager > API**

Confirme as configurações da seção **Instalação/Verificação de Licenças de API CSM** acima deste guia.

2. Uso de endereço IP CSM inválido para o login da API.

Causa: O endereço IP do servidor CSM está incorreto na URL da chamada da API.

Possível solução: Verifique na URL do cliente API se o nome do host é o endereço IP correto do servidor CSM.

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

3. Endereço IP ASA errado.

Causa: O endereço IP definido no corpo entre as marcas <deviceIP></deviceIP> não deve ser o correto.

Possível solução: Confirme se o endereço IP do dispositivo correto está definido na Sintaxe do corpo.

4. Nenhuma conexão com o firewall.

Causa: O dispositivo não tem conexão com o CSM

Possível solução: Execute um teste de conectividade do servidor CSM e solucione problemas de conectividade adicional com o dispositivo.

Para obter mais códigos de erro e descrição, consulte o Guia de especificação da API do Cisco Security Manager no próximo link.