

Extraer ACL de CSM en formato CSV a través del método API

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Diagrama de la red](#)

[Instalación/Verificación de la licencia de la API CSM](#)

[Configuration Steps](#)

[Trabajar con la API CSM](#)

[Método de inicio de sesión](#)

[Obtener reglas de ACL](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo extraer las listas de control de acceso (ACL), en formato CSV (valores separados por comas), de un dispositivo administrado por Cisco Security Manager (CSM) a través del método de la API CSM.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

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

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Servidor CSM
- licencia de API CSM
Product Name: L-CSMPR-API
Product Description: L-CSMPR-API : Cisco Security Manager Pro - License to enable API Access
- Dispositivo de seguridad adaptativo (ASA) administrado por CSM

- Un cliente API. Puede utilizar cURL, Python o Postman. Este artículo demuestra todo el proceso con Postman. La aplicación cliente CSM debe estar cerrada. Si una aplicación cliente CSM está abierta, debe estar a cargo de un usuario diferente al que utiliza el método API. De lo contrario, la API devuelve un error. Para obtener requisitos previos adicionales para utilizar la función API, puede utilizar la siguiente guía. [Requisitos previos 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Cisco Security Manager (CSM) cuenta con algunas funcionalidades para la configuración de dispositivos administrados que deben implementarse a través de la API.

Una de estas opciones de configuración es el método para extraer una lista de la lista de control de acceso (ACL) configurada en cada dispositivo administrado por CSM. El uso de la API CSM es la única manera de lograr este requisito hasta ahora.

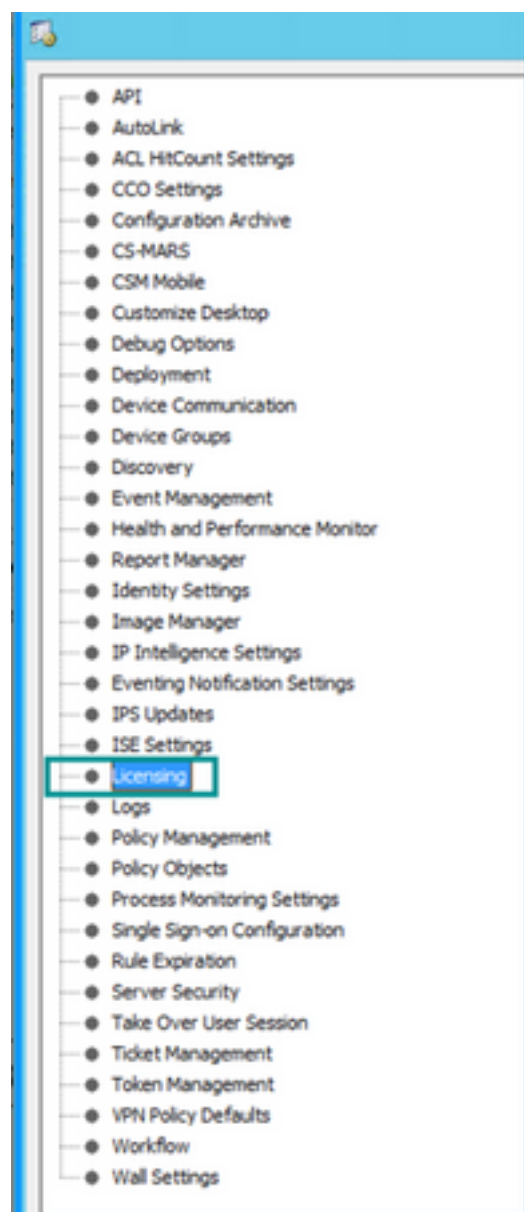
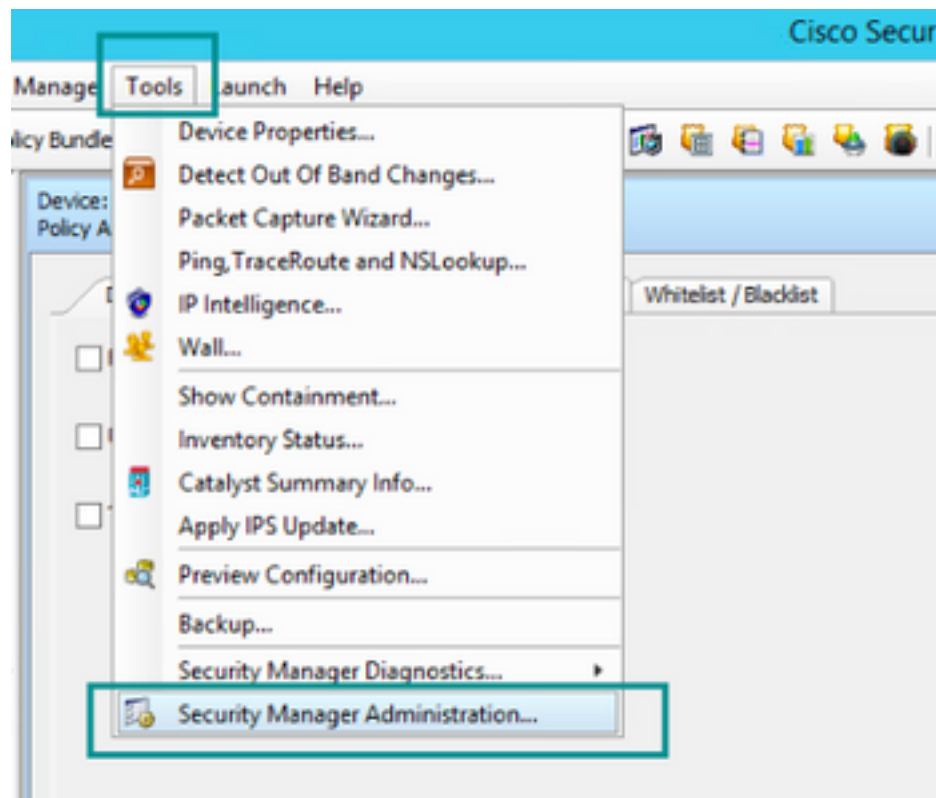
Para estos fines, Postman se utiliza como API Client y CSM versión 4.19 SP1, ASA 5515 versión 9.8(4).

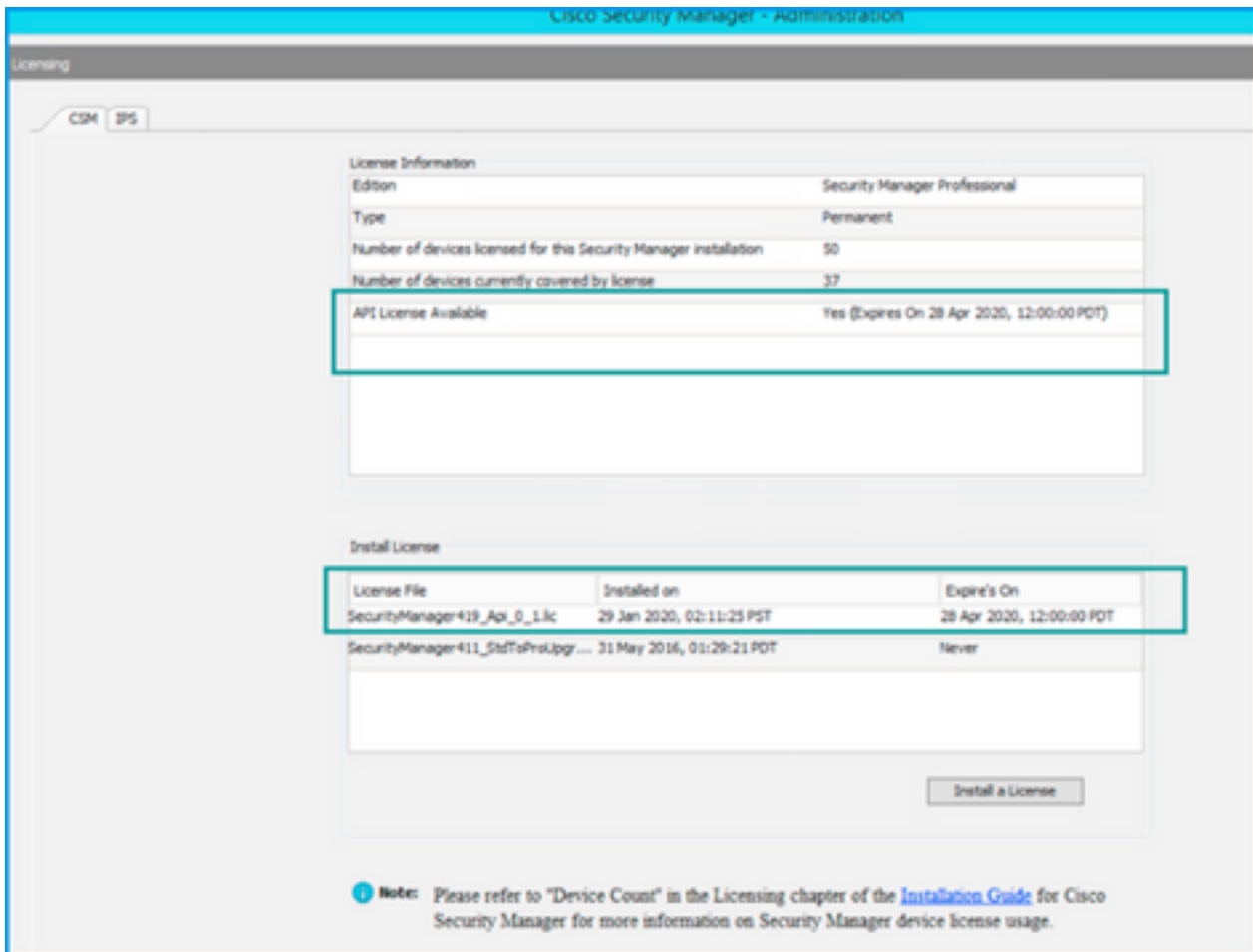
Diagrama de la red



Instalación/Verificación de la licencia de la API CSM

La API CSM es una función con licencia, puede verificar que el CSM tenga una licencia API, en el cliente CSM, navegue hasta **Herramientas > Administración del administrador de seguridad > Página de licencias** para confirmar que ya tiene instalada una licencia.

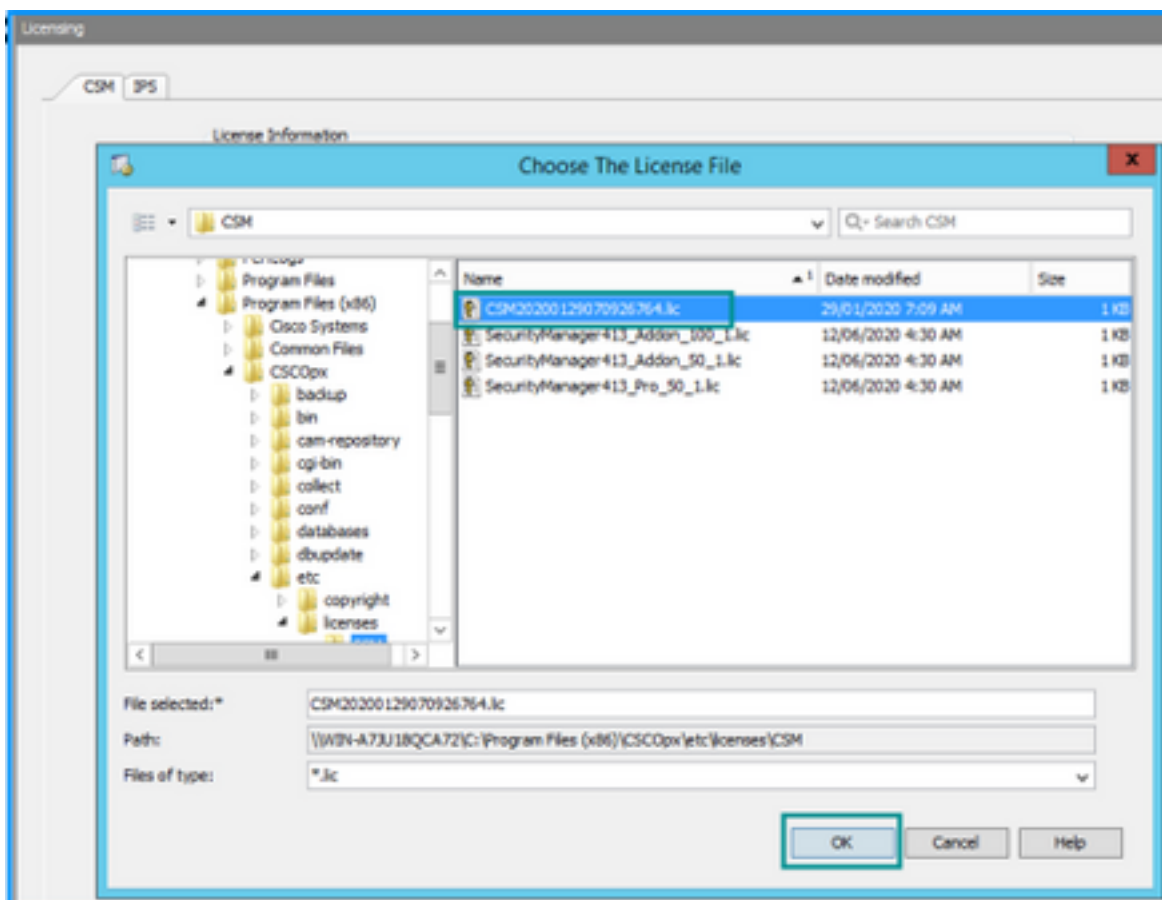
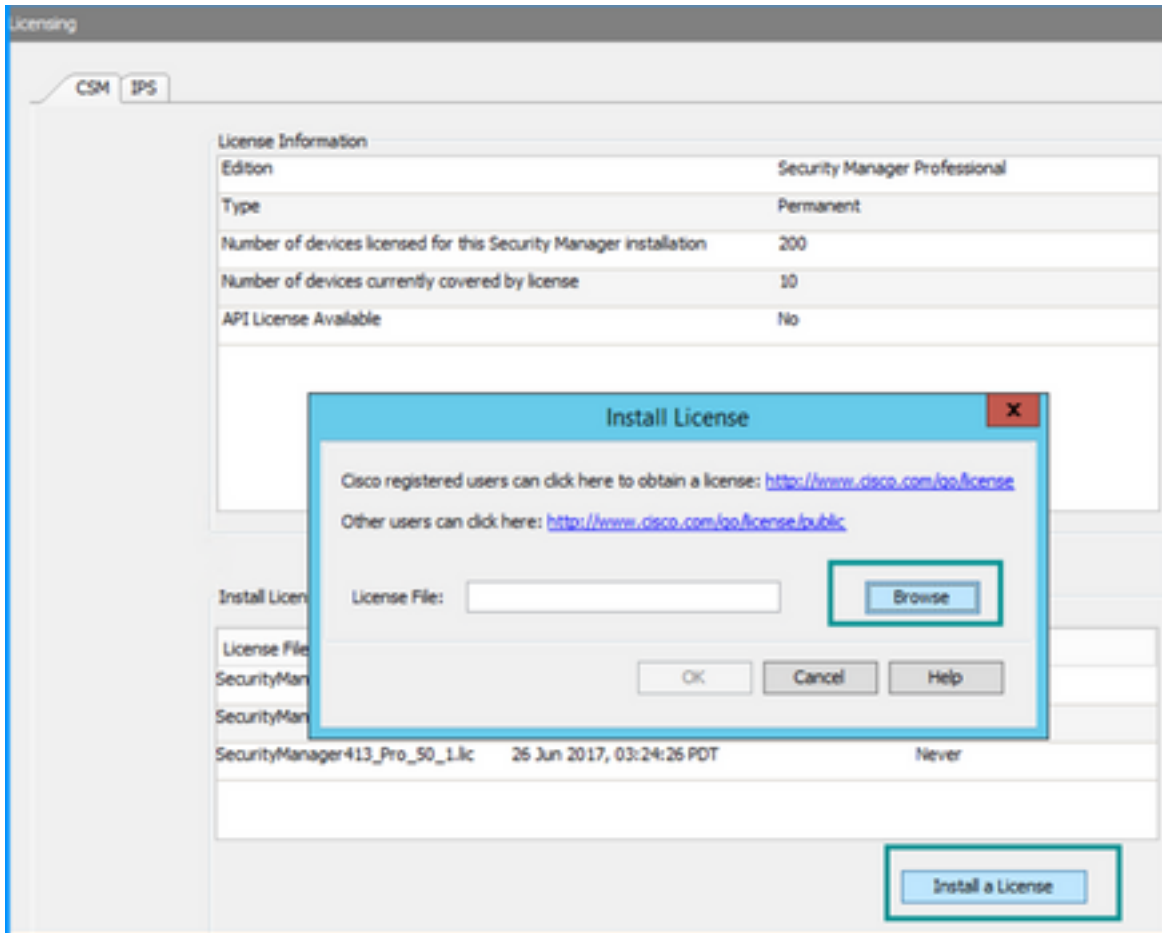


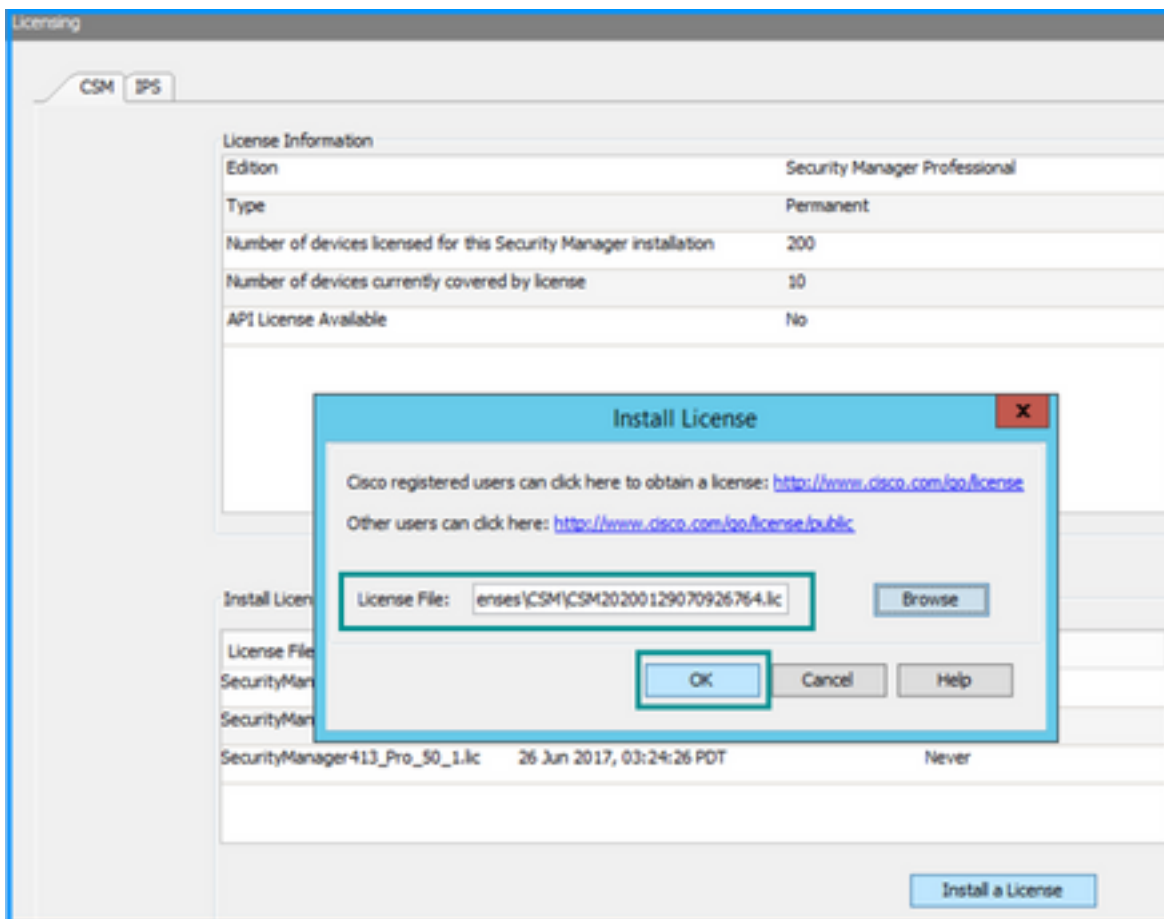


Si no se ha aplicado ninguna licencia de API pero ya tiene el archivo .lic que puede instalar, haga clic en el botón **Install a License** (Instalar una licencia), debe almacenar el archivo de licencia en el mismo disco donde se encuentra el servidor CSM.

Para instalar una nueva licencia de Cisco Security Manager, siga estos pasos:

- Paso 1. Guarde el archivo de licencia adjunto (.lic) del correo electrónico que ha recibido en el sistema de archivos.
- Paso 2. Copie el archivo de licencia guardado en una ubicación conocida del sistema de archivos del servidor de Cisco Security Manager.
- Paso 3. Inicie Cisco Security Manager Client.
- Paso 4. Vaya a **Herramientas->Administración del administrador de seguridad...**
- Paso 5. En la ventana **Cisco Security Manager - Administration**, seleccione **Licensing**
- Paso 6. Haga clic en el botón **Install a License** .
- Paso 7. En el diálogo **Instalar licencia**, seleccione el botón **Examinar**.
- Paso 8. Navegue hasta y seleccione el archivo de licencia guardado en el sistema de archivos del servidor de Cisco Security Manager y seleccione el botón **Aceptar**.
- Paso 9. En el cuadro de diálogo **Install License**, haga clic en el botón **OK**.
- Paso 10. Confirme la información de Resumen de licencia mostrada y haga clic en el botón **Cerrar**.





La licencia de API sólo se puede aplicar en un servidor con licencia para la edición profesional de CSM. La licencia no se puede aplicar a CSM que ejecuta una edición estándar de la licencia.

[Requisitos de licencia de API](#)

Configuration Steps

Configuración del cliente API

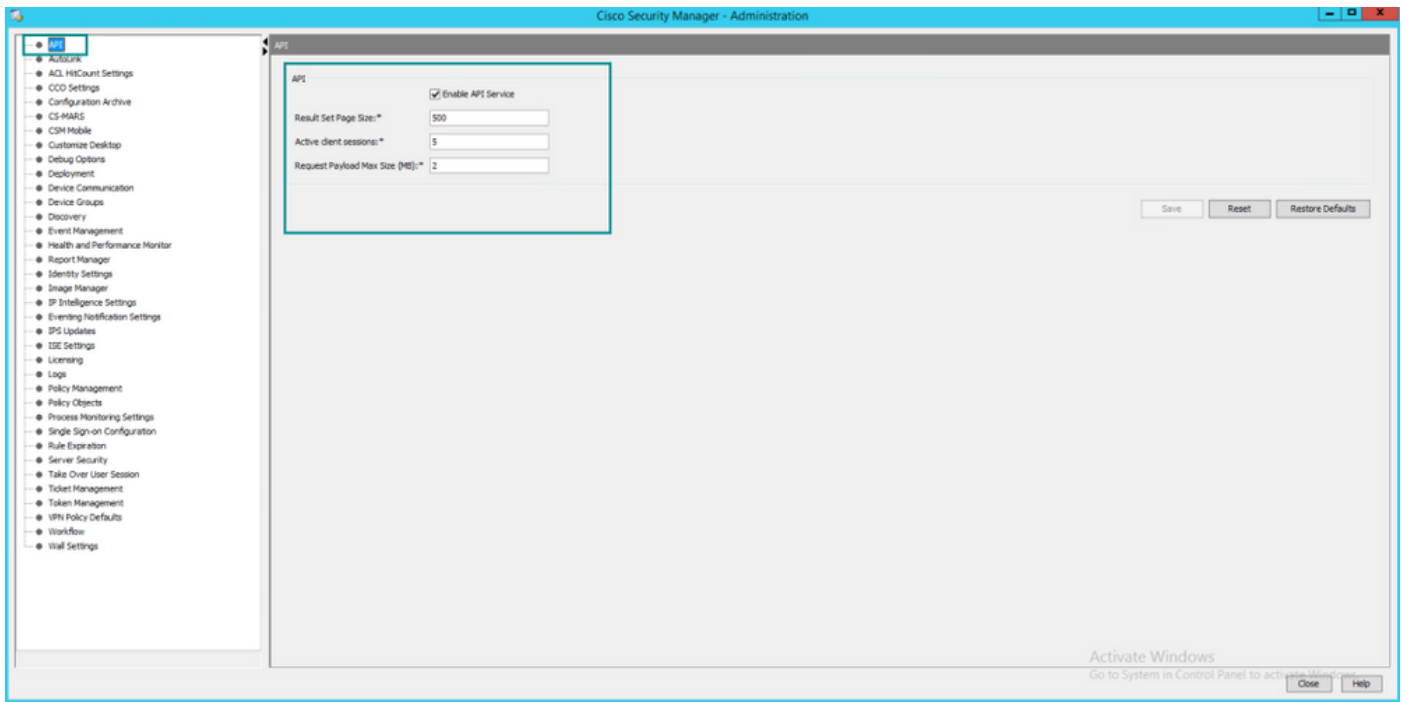
Si utiliza Postman hay algunos ajustes que necesita configurar, depende de cada cliente de API pero debe ser similar.

- Proxy deshabilitado
- Verificación SSL - OFF

Configuración de CSM

- API habilitada. En **Herramientas > Administración del Administrador de seguridad > API**

[Configuración de API](#)



Trabajar con la API CSM

Debe configurar en el cliente API las dos llamadas siguientes:

1. Método de inicio de sesión
2. Obtener valores de ACL

Para obtener referencia a través del proceso:

Detalles de acceso a CSM utilizados en este laboratorio:

Nombre de host CSM (dirección IP): **192.168.66.116**. En la API utilizamos el nombre de host en la URL.

Usuario: **admin**

Contraseña **Admin123**

Método de inicio de sesión

Se debe llamar a este método antes de cualquier otro método llamado en otros servicios.

[Guía de la API de CSM: Inicio de sesión de método](#)

Petición

1. Método HTTP: **POST**
2. URL: **https://<hostname>/nbi/login**
3. Cuerpo:

Where:

Nombre de usuario: El nombre de usuario del cliente CSM asociado a la sesión

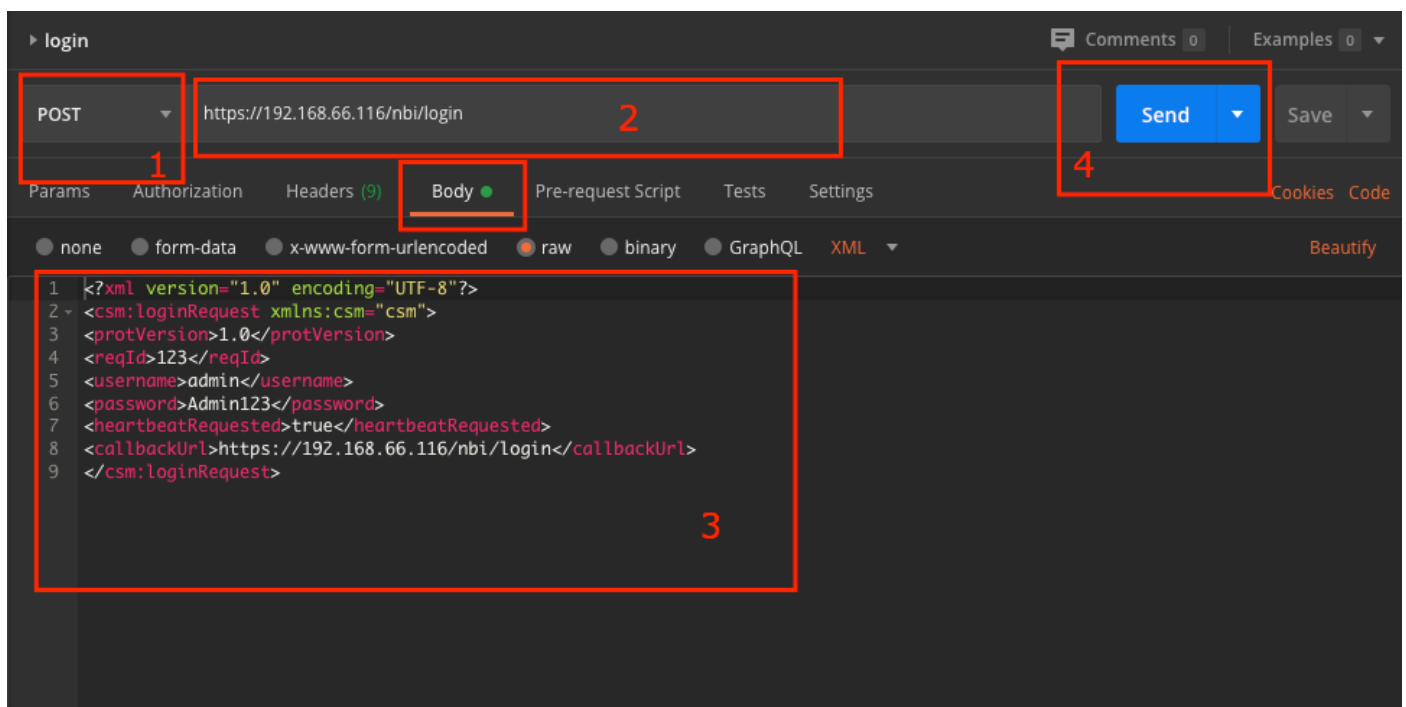
Contraseña La contraseña del cliente CSM asociada a la sesión.

reqId: Este atributo identifica de forma única una solicitud realizada por el cliente, este valor se hace eco por el servidor CSM en la respuesta asociada. Se puede establecer en cualquier cosa que el usuario desee utilizar como identificador.

latidoSolicitado: Este atributo puede definirse opcionalmente. Si el atributo se establece en true, el cliente CSM recibe una devolución de llamada de latido del servidor CSM. El servidor intenta hacer ping al cliente con una frecuencia cercana (tiempo de espera de inactividad) / 2 minutos. Si el cliente no responde al latido, la API reintenta el latido durante el siguiente intervalo. Si el latido del corazón se realiza correctamente, se restablece el tiempo de espera de inactividad de la sesión.

callbackUrl: La URL en la que el servidor CSM realiza la devolución de llamada. Esto debe especificarse si el comando latidoSolicitado es true. Solo se permiten URL de devolución de llamada basadas en HTTPS

4. Enviar



The screenshot shows a REST client interface for a 'login' endpoint. The method is set to 'POST' (1) and the URL is 'https://192.168.66.116/nbi/login' (2). The 'Body' tab is selected (3), and the 'raw' format is chosen. The XML body is as follows:

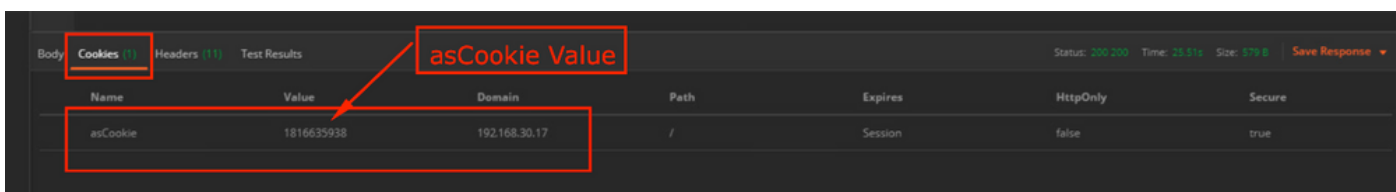
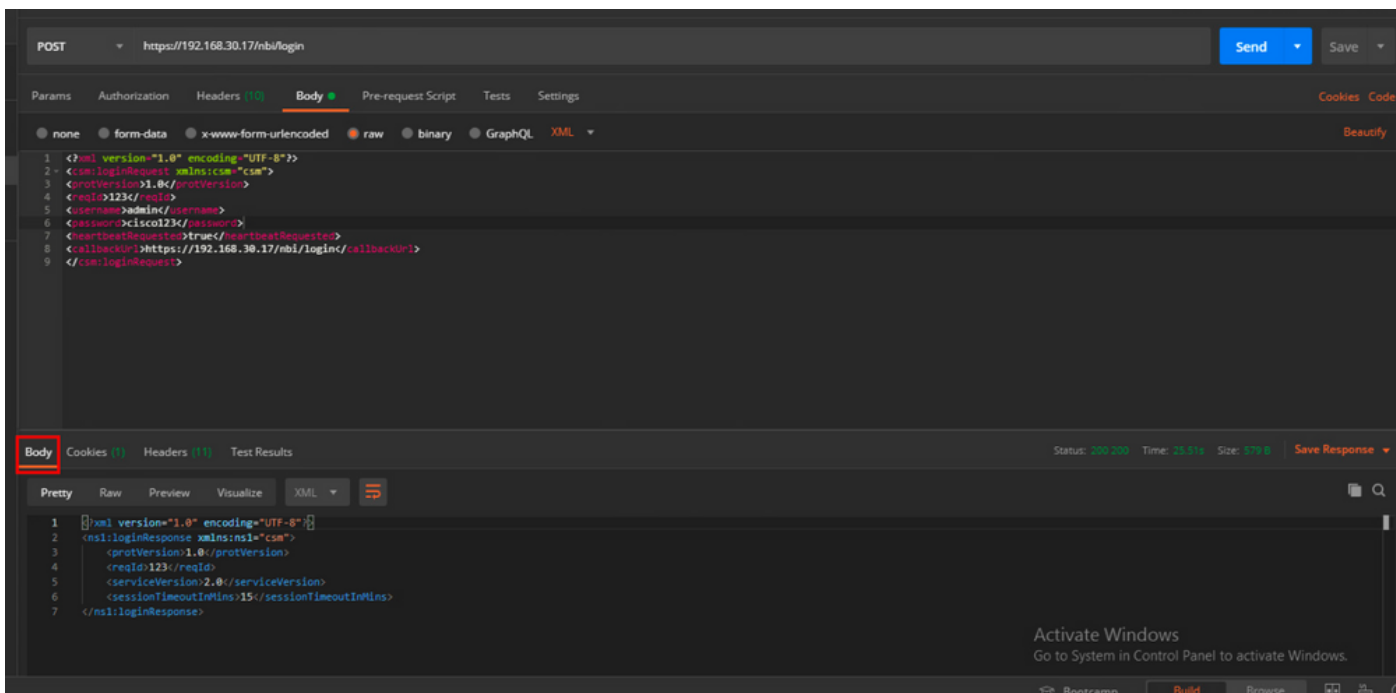
```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <csm:loginRequest xmlns:csm="csm">
3 <protVersion>1.0</protVersion>
4 <reqId>123</reqId>
5 <username>admin</username>
6 <password>Admin123</password>
7 <heartbeatRequested>true</heartbeatRequested>
8 <callbackUrl>https://192.168.66.116/nbi/login</callbackUrl>
9 </csm:loginRequest>
```

The 'Send' button (4) is visible in the top right corner.

Seleccione la opción sin procesar para ver como en este ejemplo.

Respuesta

La API de inicio de sesión valida las credenciales del usuario y devuelve un token de sesión como cookie segura. El valor de sesión se almacena bajo la clave **como Cookie**, debe guardar este valor **como Cookie**.



Obtener reglas de ACL

Method execDeviceReadOnlyCLICmds. El conjunto de comandos que se pueden ejecutar con este método son comandos de sólo lectura como estadísticas, comandos de supervisión que proporcionan información adicional sobre el funcionamiento del dispositivo en particular.

[Detalles del método de la Guía del usuario de la API CSM](#)

Petición

1. Método HTTP: **POST**

2. URL: `https://hostname/nbi/utlilservice/execDeviceReadOnlyCLICmds`

3. Encabezado HTTP: La cookie devuelta por el método de inicio de sesión que identifica la sesión de autenticación.

Introducir **como** valor **Cookie** obtenido previamente de Inicio de sesión de método.

Clave: Entrada "asCookie"

Valor: Valor de entrada obtenido.

Haga clic en la casilla de verificación para activarla.

4. Cuerpo:

Nota: El cuerpo XML anterior se puede utilizar para ejecutar cualquier comando "show", por ejemplo: "show run all", "show run object", "show run nat", etc.

El elemento XML "<deviceReadOnlyCLICmd>" indica que el comando especificado en "<cmd>" y "<argumento>" DEBE ser de sólo lectura.

Where:

DeviceIP: La dirección IP del dispositivo con la que se debe ejecutar el comando.

cmd: Orden fija "show". El regex permite casos [sS][hH][oO][wW] mixtos

argumento: Los argumentos del comando show. Como "ejecutar" para mostrar la configuración en ejecución del dispositivo o "lista de acceso" para mostrar los detalles de la lista de acceso.

5. Enviar

The screenshot shows a REST client interface with the following elements highlighted by red boxes and numbered 1 through 5:

- 1:** The HTTP method dropdown menu, currently set to "POST".
- 2:** The URL input field, containing "https://192.168.66.116/nbi/utlilservice/execDeviceReadOnlyCLICmds".
- 3:** The "Headers" tab, which is currently selected and shows "(10)" headers.
- 4:** The "Body" tab, which is currently selected and shows an XML payload. The XML content is as follows:

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <csm:execDeviceReadOnlyCLICmdsRequest xmlns:csm="csm">
3   <protVersion>1.0</protVersion>
4   <reqId>123</reqId>
5   <deviceReadOnlyCLICmd>
6     <deviceIP>192.168.66.1</deviceIP>
7     <cmd>show</cmd>
8     <argument>access-list</argument>
9   </deviceReadOnlyCLICmd>
10 </csm:execDeviceReadOnlyCLICmdsRequest>
```
- 5:** The "Send" button, which is used to execute the request.

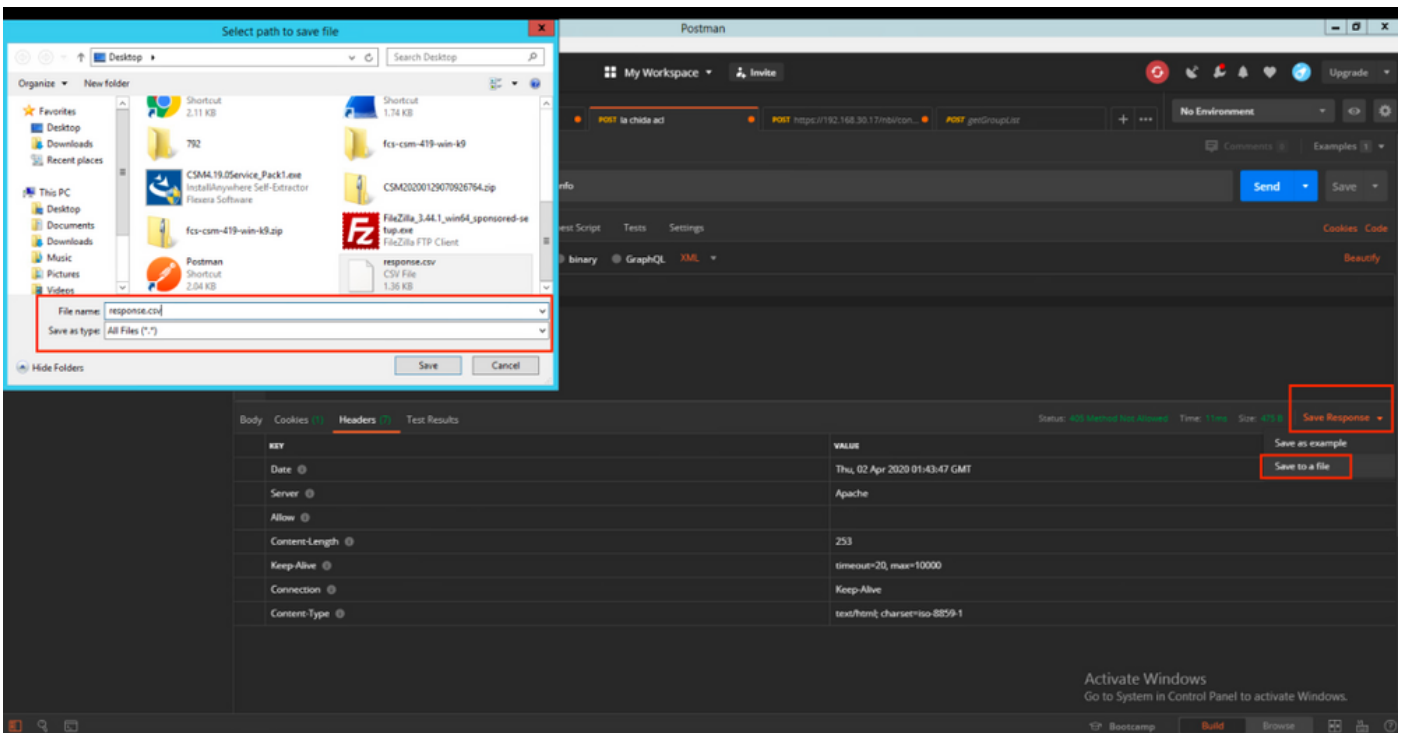
Below the request configuration, the "Response" section is visible but currently empty.

Respuesta

```
<?xml version="1.0" encoding="UTF-8"?>
<ns1:execDeviceReadOnlyCLICmdsResponse xmlns:ns1="csm">
  <protVersion>1.0</protVersion>
  <reqId>1234</reqId>
  <deviceCmdResult>
    <deviceIP>192.168.30.2</deviceIP>
    <deviceID>00000000-0000-0000-0005-360119185746</deviceID>
    <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>
```

Verificación

Puede guardar la respuesta como archivo. Vaya a **Guardar respuesta > Guardar en un archivo**. A continuación, seleccione la ubicación del archivo y guárdelo como un tipo .csv.



Por ejemplo, debe poder abrir este archivo .csv con la aplicación Excel. Desde el tipo de archivo .csv, puede guardar el resultado como otros tipos de archivo, como PDF, TXT, etc.

Troubleshoot

Posibles respuestas a fallos mediante API.

1. No se ha instalado ninguna licencia de API.

Causa: Licencia de API caducada, no instalada o no habilitada.

Posible solución: Verificar la fecha de vencimiento de la licencia, en **Herramientas > Administración del administrador de seguridad > Página Licencias**

Verificar que la función API esté habilitada en **Herramientas > Administración del Administrador de seguridad > API**

Confirme la configuración de la sección **Instalación/Verificación de Licencia de la API CSM** de

esta guía.

2. Uso incorrecto de la dirección IP CSM para el inicio de sesión de la API.

Causa: La dirección IP del servidor CSM es incorrecta en la dirección URL de la llamada API.

Posible solución: Verifique en la URL del cliente API que el nombre de host es la dirección IP correcta del servidor CSM.

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

3. Dirección IP ASA incorrecta.

Causa: La dirección IP definida en Body entre las etiquetas `<deviceIP></deviceIP>` no debe ser la correcta.

Posible solución: Confirme que la dirección IP del dispositivo correcto esté definida dentro de la sintaxis del cuerpo.

4. No hay conexión al firewall.

Causa: El dispositivo no tiene conexión con el CSM

Posible solución: Ejecute una Conectividad de Prueba desde el servidor CSM y resuelva problemas de conectividad adicional con el dispositivo.

Para obtener más información sobre los códigos de error y la descripción, consulte la Guía de especificación de la API de Cisco Security Manager en el siguiente [enlace](#).