

# Extraire la liste de contrôle d'accès de CSM au format CSV via la méthode API

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Diagramme du réseau](#)

[Installation/vérification de la licence de l'API CSM](#)

[Configuration Steps](#)

[Utilisation de l'API CSM](#)

[Méthode de connexion](#)

[Obtenir les règles ACL](#)

[Vérification](#)

[Dépannage](#)

## Introduction

Ce document décrit comment extraire les listes de contrôle d'accès (ACL), au format CSV (Comma-Separated Values), d'un périphérique géré par Cisco Security Manager (CSM) via la méthode API CSM.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Security Manager (CSM)
- API CSM
- Connaissances de base de l'API

### Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Serveur CSM
- Licence API CSM  
Product Name: L-CSMPR-API  
Product Description: L-CSMPR-API : Cisco Security Manager Pro - License to enable API Access
- Dispositif de sécurité adaptatif (ASA) géré par CSM

- Un client API. Vous pouvez utiliser cURL, Python ou Postman. Cet article démontre tout le processus avec Postman. L'application cliente CSM doit être fermée. Si une application cliente CSM est ouverte, doit être effectuée par un utilisateur différent de celui qui utilise la méthode API. Sinon, l'API renvoie une erreur. Pour connaître les conditions préalables supplémentaires à l'utilisation de la fonction API, reportez-vous au guide suivant. [Conditions requises pour l'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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

Cisco Security Manager (CSM) possède certaines fonctionnalités pour la configuration des périphériques gérés qui doivent être mises en oeuvre via l'API.

L'une de ces options de configuration est la méthode d'extraction d'une liste de la liste de contrôle d'accès (ACL) configurée dans chaque périphérique géré par CSM. L'utilisation de l'API CSM est le seul moyen d'atteindre cette exigence jusqu'à présent.

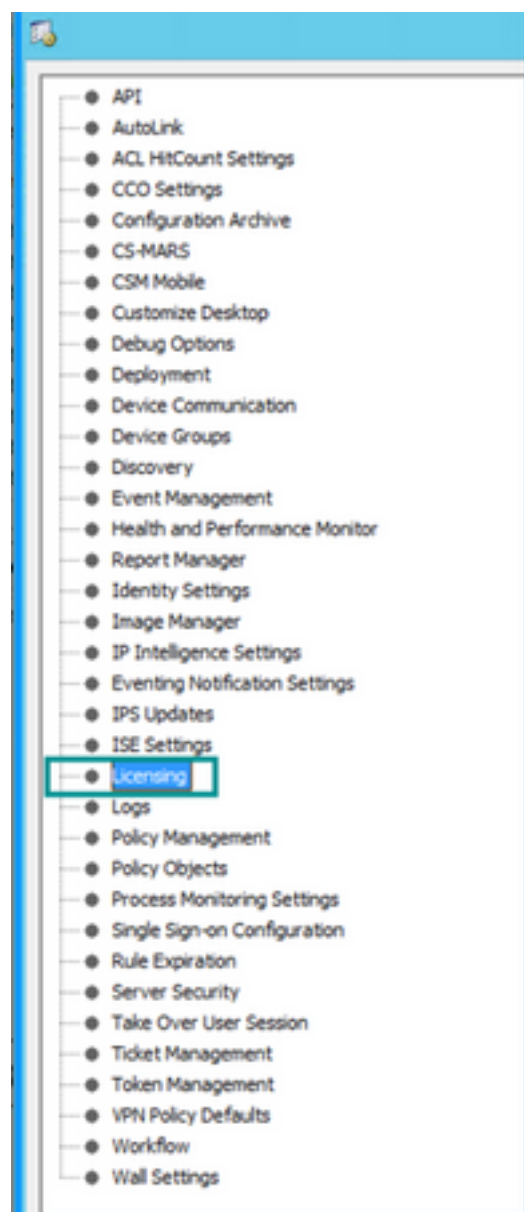
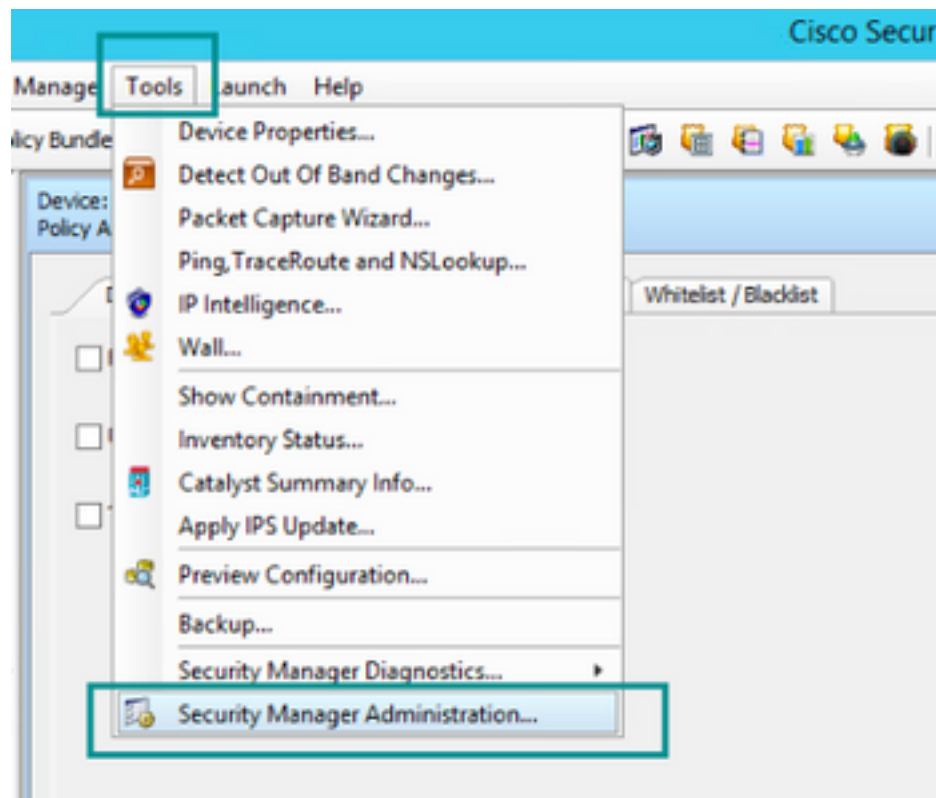
À ces fins, Postman a utilisé comme client API et CSM version 4.19 SP1, ASA 5515 version 9.8(4).

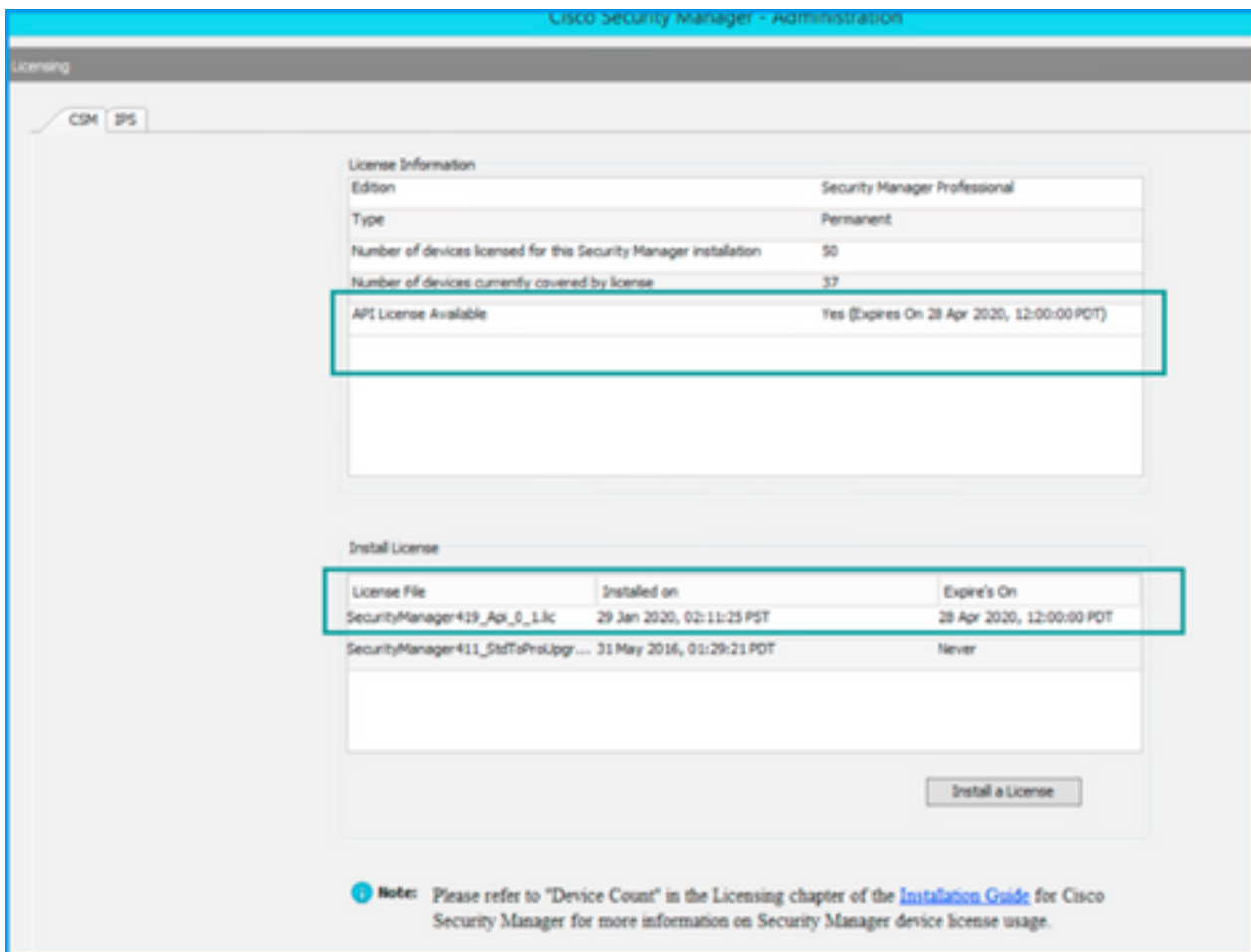
## Diagramme du réseau



## Installation/vérification de la licence de l'API CSM

L'API CSM est une fonctionnalité sous licence. Vous pouvez vérifier que le CSM dispose d'une licence API, dans le client CSM, accédez à **Outils > Administration du Gestionnaire de sécurité > Licence** pour confirmer que vous avez déjà installé une licence.





License Information

Edition	Security Manager Professional
Type	Permanent
Number of devices licensed for this Security Manager installation	50
Number of devices currently covered by license	37
API License Available	Yes (Expires On 28 Apr 2020, 12:00:00 PDT)

Install License

License File	Installed on	Expires On
SecurityManager419_Ap1_0_L.lic	29 Jan 2020, 02:11:25 PST	28 Apr 2020, 12:00:00 PDT
SecurityManager411_StdToProUpgr...	31 May 2016, 01:29:21 PDT	Never

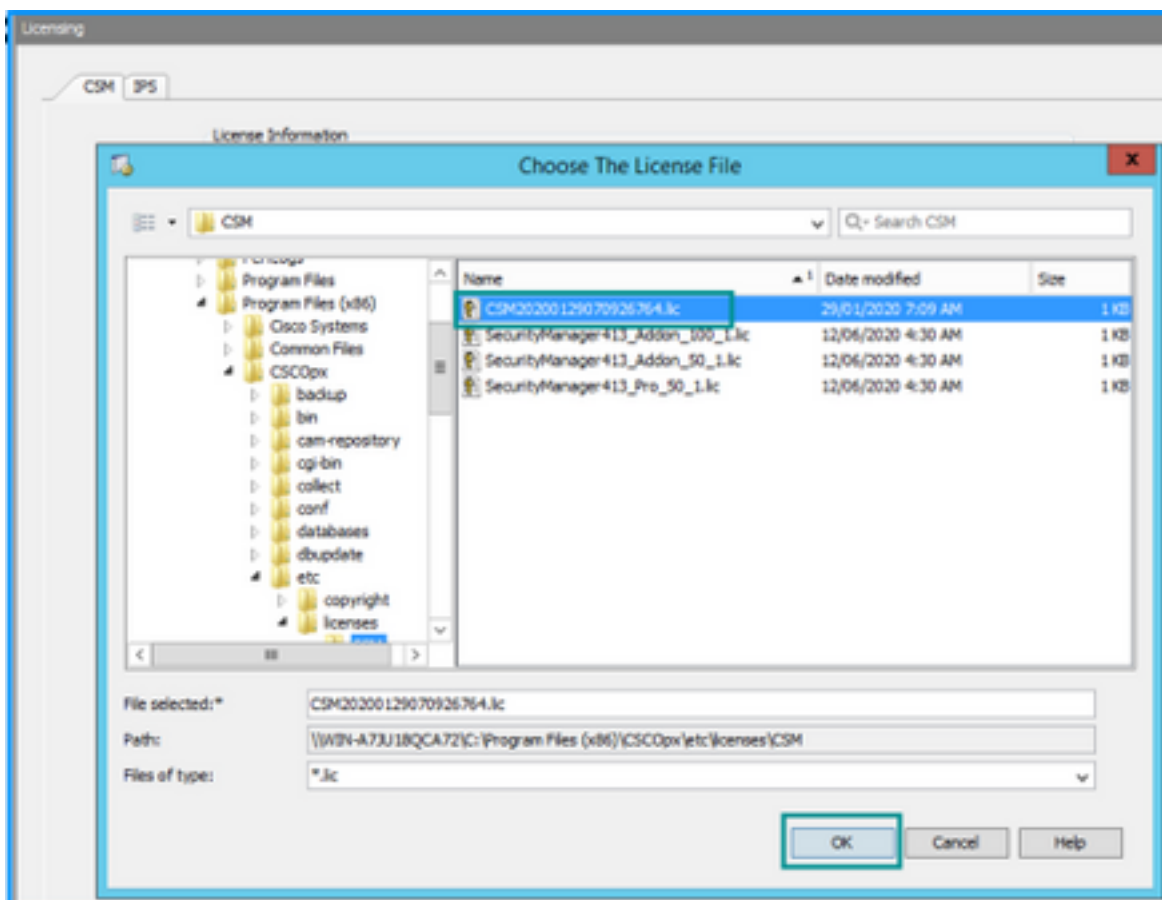
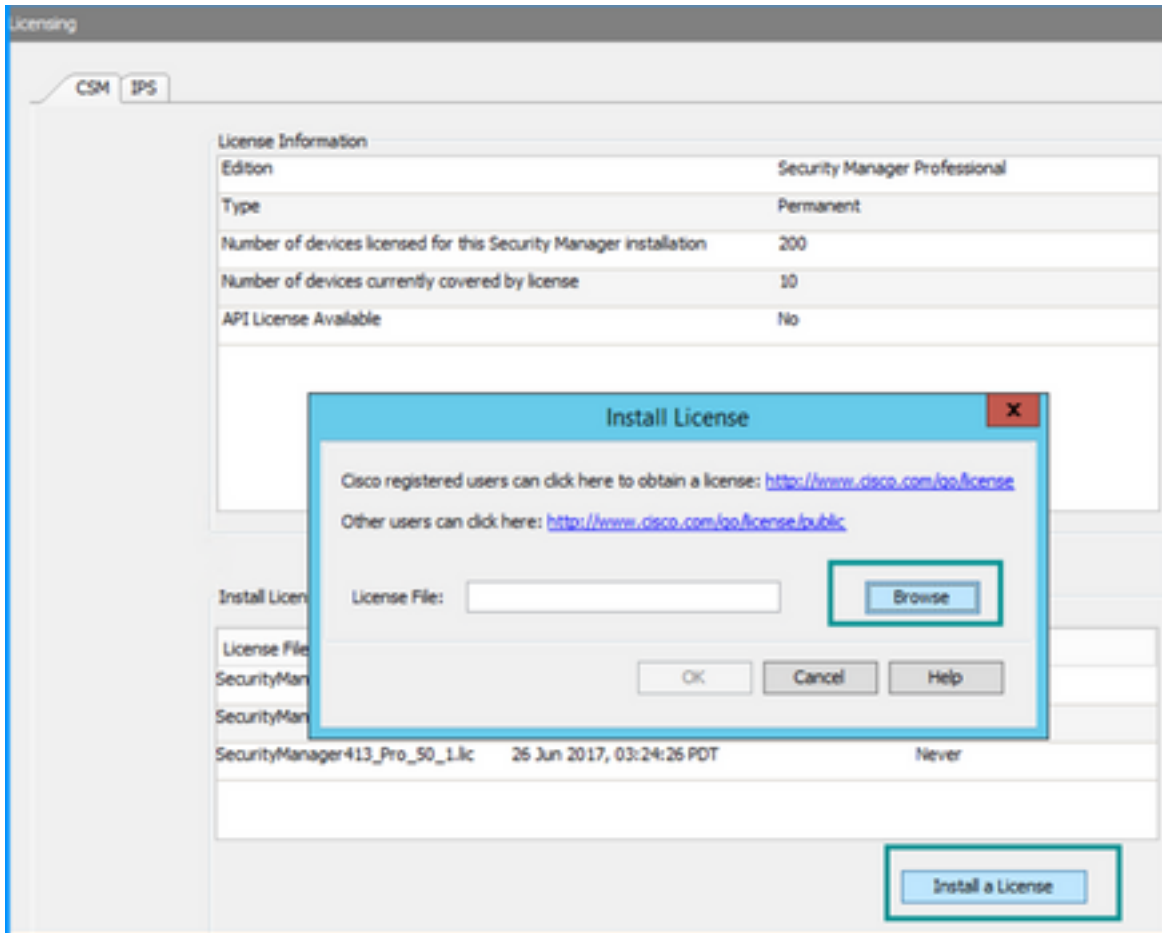
Install a License

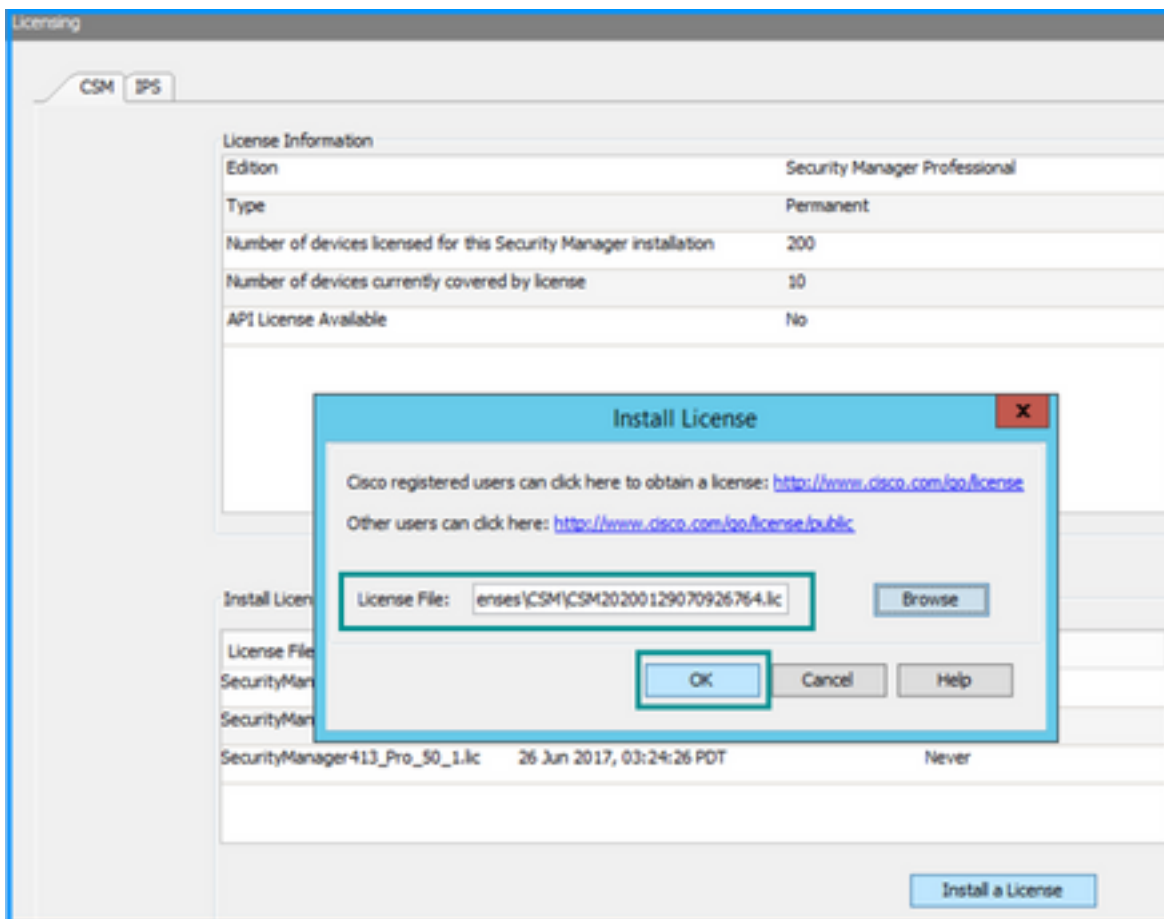
Note: Please refer to "Device Count" in the Licensing chapter of the [Installation Guide](#) for Cisco Security Manager for more information on Security Manager device license usage.

Si aucune licence API n'est appliquée mais que vous disposez déjà du fichier .lic que vous pouvez installer votre licence, cliquez sur le bouton **Installer une licence**, vous devez stocker le fichier de licence sous le même disque où se trouve le serveur CSM.

Pour installer une nouvelle licence Cisco Security Manager, procédez comme suit :

- Étape 1. Enregistrez le fichier de licence joint (.lic) à partir de l'e-mail que vous avez reçu dans votre système de fichiers.
- Étape 2. Copiez le fichier de licence enregistré à un emplacement connu sur le système de fichiers du serveur Cisco Security Manager.
- Étape 3. Lancez le client Cisco Security Manager.
- Étape 4. Accédez à **Outils->Administration de Security Manager...**
- Étape 5. Dans la fenêtre **Cisco Security Manager - Administration**, sélectionnez **Licensing**
- Étape 6. Cliquez sur le bouton **Installer une licence**.
- Étape 7. Dans la boîte de dialogue **Installer la licence**, sélectionnez le bouton **Parcourir**.
- Étape 8. Accédez au fichier de licence enregistré sur le système de fichiers du serveur Cisco Security Manager et sélectionnez le bouton **OK**.
- Étape 9. Dans la boîte de dialogue **Installer la licence**, cliquez sur le bouton **OK**.
- Étape 10. Confirmez les informations de résumé de licence affichées et cliquez sur le bouton **Fermer**.





La licence API ne peut être appliquée que sur un serveur sous licence pour l'édition professionnelle CSM. La licence ne peut pas être appliquée à CSM exécutant une édition Standard de la licence. [Exigences de licence API](#)

## Configuration Steps

### Paramètres du client API

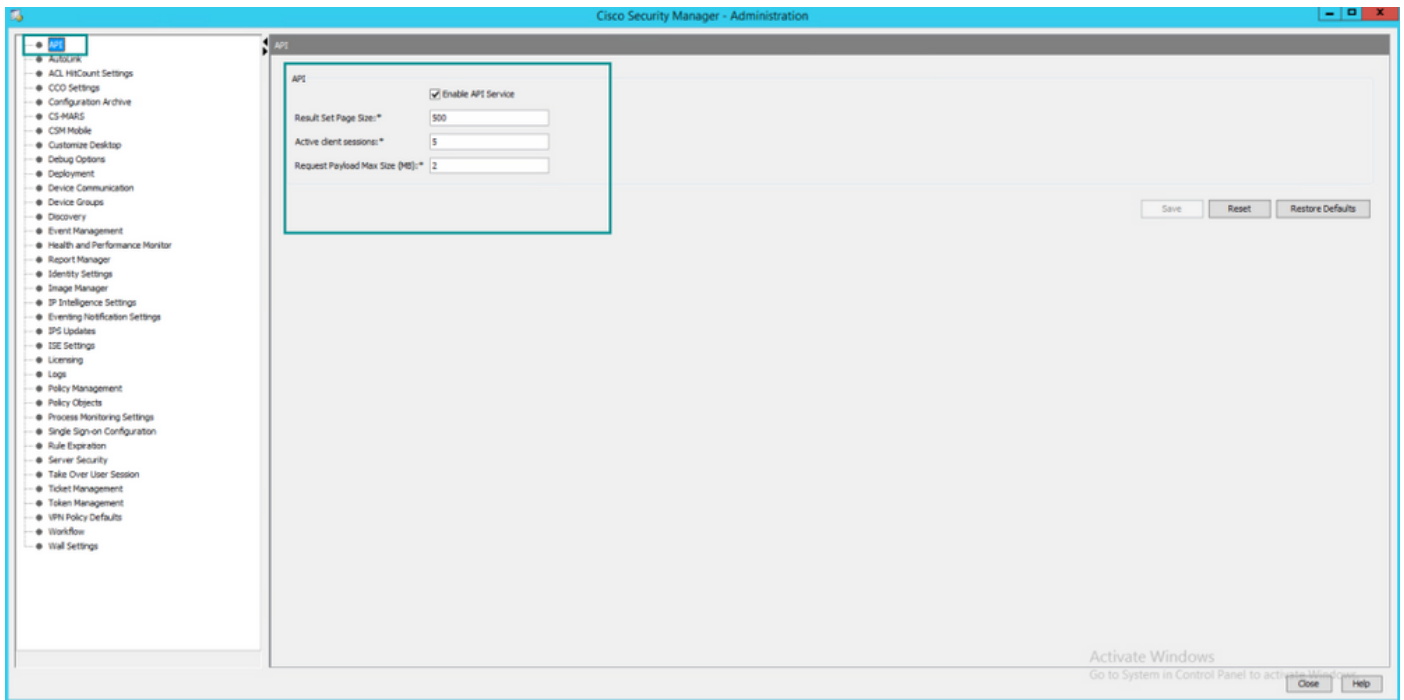
Si vous utilisez Postman, il y a des paramètres que vous devez configurer, cela dépend de chaque client d'API mais doit être similaire.

- Proxy désactivé
- Vérification SSL - DÉSACTIVÉ

### Paramètres CSM

- API activée. Sous **Outils > Administration de Security Manager > API**

[Paramètres API](#)



## Utilisation de l'API CSM

Vous devez configurer dans le client API les deux appels suivants :

1. Méthode de connexion
2. Obtenir les valeurs ACL

Pour référence au cours du processus :

Détails d'accès CSM utilisés dans ces travaux pratiques :

Nom d'hôte CSM (adresse IP) : **192.168.66.116** . Dans l'API, nous utilisons le nom d'hôte dans l'URL.

Utilisateur : **admin**

Mot de passe : **Admin123**

### Méthode de connexion

Cette méthode doit être appelée avant toute autre méthode appelée sur d'autres services.

[Guide d'API CSM : Méthode de connexion](#)

### Demander

1. Méthode HTTP : **POST**
2. URL: **https://<hostname>/nbi/login**
3. Body (Corps) :

Where:

**username (nom d'utilisateur)** : Nom d'utilisateur du client CSM associé à la session

**Mot de passe** : Mot de passe client CSM associé à la session.

**reqId** : Cet attribut identifie de manière unique une requête effectuée par le client. Cette valeur est reprise par le serveur CSM dans la réponse associée. Il peut être défini sur tout ce que l'utilisateur souhaite utiliser comme identificateur.

**heartbeatRequested** : Cet attribut peut être éventuellement défini. Si l'attribut est défini sur true, le client CSM reçoit un rappel de pulsation du serveur CSM. Le serveur tente d'envoyer une requête ping au client avec une fréquence proche de (délai d'inactivité) / 2 minutes. Si le client ne répond pas à la pulsation, l'API recommence la pulsation au cours de l'intervalle suivant. Si la pulsation réussit, le délai d'inactivité de la session est réinitialisé.

**callbackUrl** : URL à laquelle le serveur CSM effectue le rappel. Ceci doit être spécifié si heartbeatRequested a la valeur true. Seules les URL de rappel basées sur HTTPS sont autorisées

#### 4. Envoyer

The screenshot shows a REST client interface for a 'login' endpoint. The method is set to 'POST' and the URL is 'https://192.168.66.116/nbi/login'. The request body is configured as raw XML with the following content:

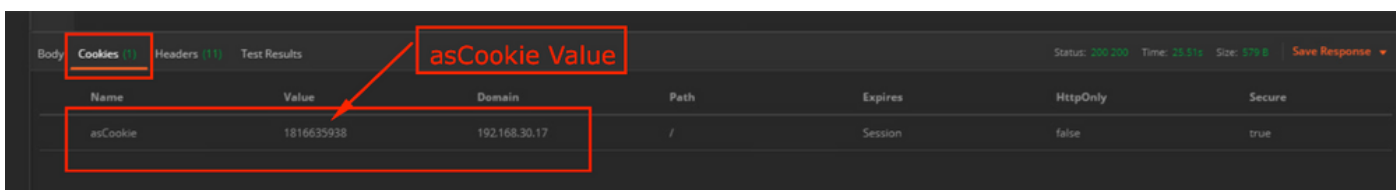
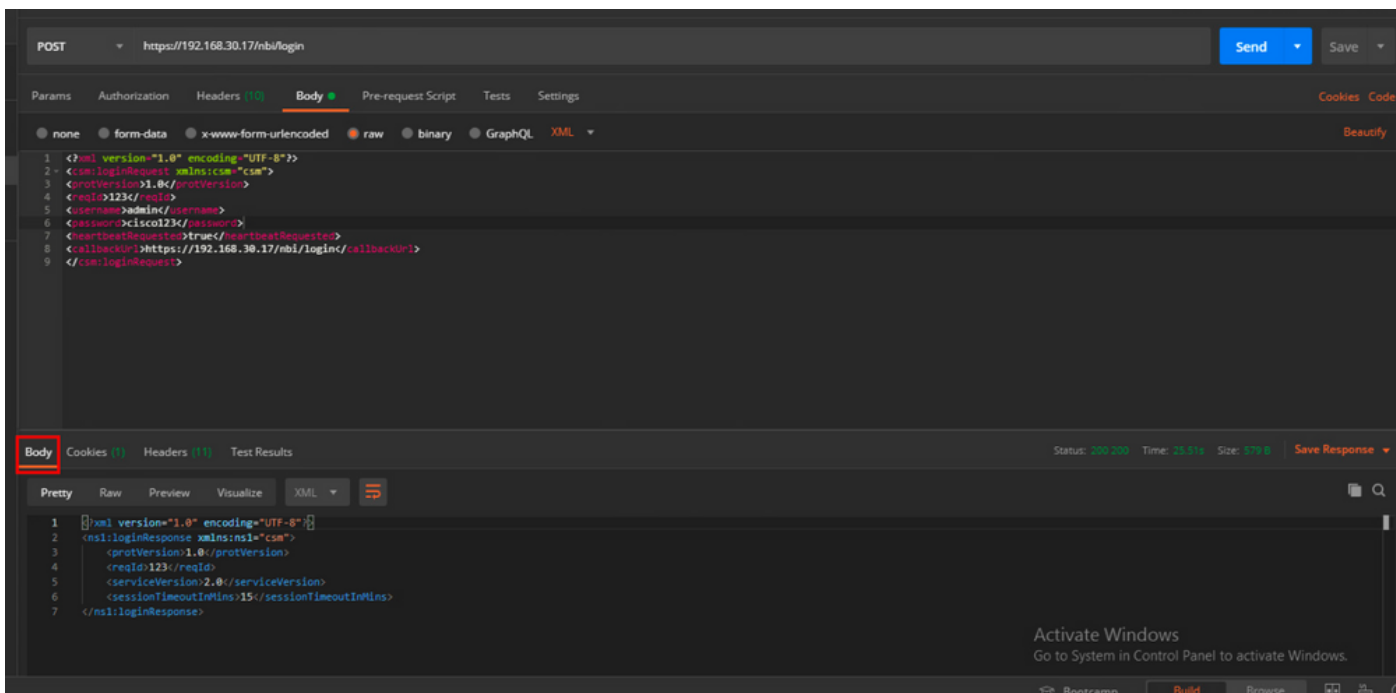
```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <csm:loginRequest xmlns:csm="csm">
3 <protVersion>1.0</protVersion>
4 <reqId>123</reqId>
5 <username>admin</username>
6 <password>Admin123</password>
7 <heartbeatRequested>true</heartbeatRequested>
8 <callbackUrl>https://192.168.66.116/nbi/login</callbackUrl>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

Sélectionnez l'option brute à afficher comme dans cet exemple.

#### Réponse

L'API de connexion valide les informations d'identification de l'utilisateur et renvoie un jeton de session sous la forme d'un cookie sécurisé. La valeur de session est stockée sous la clé **asCookie**, vous devez enregistrer cette **valeur asCookie**.





## Obtenir les règles ACL

**Méthode execDeviceReadOnlyCLICmds.** Le jeu de commandes qui peut être exécuté par cette méthode est constitué de commandes en lecture seule telles que les statistiques, les commandes de surveillance qui fournissent des informations supplémentaires sur le fonctionnement du périphérique particulier.

[Détails de la méthode du guide de l'utilisateur de l'API CSM](#)

### Demander

1. Méthode HTTP : **POST**

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

3. En-tête HTTP : Le cookie retourné par la méthode de connexion qui identifie la session d'authentification.

Entrez **asCookie** valeur obtenue précédemment à partir de la connexion de méthode.

Clé : " de " d'entrée asCookie

Valeur: Valeur d'entrée obtenue.

Cochez cette case pour l'activer.

4. Body (Corps) :

**Note:** Le corps XML ci-dessus peut être utilisé pour exécuter n'importe quelle commande « show », par exemple : « show run all », « show run object », « show run nat », etc.

L'élément XML "<deviceReadOnlyCLICmd>" indique que la commande spécifiée dans "<cmd>" et "<argument>" DOIT être en lecture seule.

Where:

**deviceIP** : Adresse IP du périphérique sur laquelle la commande doit être exécutée.

**cmd** : Commande fixe " show ". Le regex autorise la combinaison de majuscules [sS][hH][oO][wW]

**argument** : Arguments de la commande show. Comme " exécuter " pour afficher la configuration en cours du périphérique ou la " liste d'accès " pour afficher les détails de la liste d'accès.

## 5. Envoyer

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 "Body" tab in the request configuration panel.
- 4:** The XML request body content, which is: 

```
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, used to execute the request.

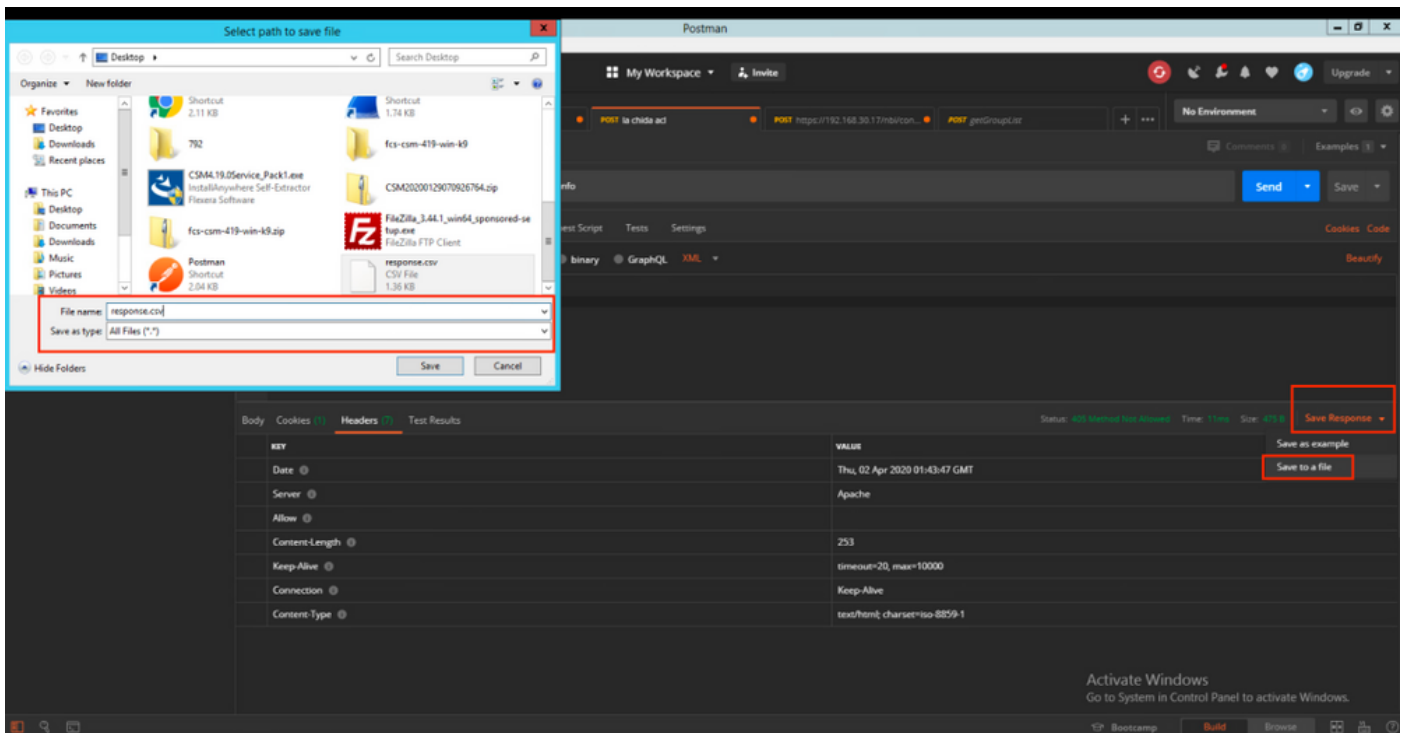
The interface also shows a "Response" section at the bottom, which is currently empty.

## Réponse

```
<?xml version="1.0" encoding="UTF-8"?>
<ns1:execDeviceReadOnlyCLICommandsResponse 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:execDeviceReadOnlyCLICommandsResponse>
```

## Vérification

Vous pouvez enregistrer la réponse sous forme de fichier. Accédez à **Enregistrer la réponse** > **Enregistrer dans un fichier**. Sélectionnez ensuite l'emplacement du fichier et enregistrez-le en tant que type .csv.



Vous devez ensuite pouvoir ouvrir ce fichier .csv avec Excel Application, par exemple. À partir du type de fichier .csv, vous pouvez enregistrer la sortie sous d'autres types de fichier, tels que PDF, TXT, etc.

## Dépannage

Réponses possibles en cas d'échec à l'aide de l'API.

1. Aucune licence API installée.

Motif: Licence API expirée, non installée ou non activée.

Solution possible : Vérifiez la date d'expiration de la licence, sous **Outils > Administration du Gestionnaire de sécurité > Page Licences**.

Vérifiez que la fonctionnalité API est activée sous **Outils > Administration du gestionnaire de sécurité > API**

Confirmez les paramètres de la section **Installation/Vérification de la licence de l'API CSM** ci-dessus de ce guide.

2. Mauvaise utilisation de l'adresse IP CSM pour la connexion à l'API.

Motif: L'adresse IP du serveur CSM est incorrecte dans l'URL de l'appel API.

Solution possible : Vérifiez dans l'URL du client API que le nom d'hôte est l'adresse IP correcte du serveur CSM.

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

3. Adresse IP ASA incorrecte.

Motif: L'adresse IP définie sur le corps entre les balises `<deviceIP></deviceIP>` ne doit pas être la bonne.

Solution possible : Vérifiez que l'adresse IP du périphérique approprié est définie dans la syntaxe Body.

4. Aucune connexion au pare-feu.

Motif: Le périphérique n'a aucune connexion avec le CSM

Solution possible : Exécutez un test de connectivité à partir du serveur CSM et dépannez une connectivité supplémentaire au périphérique.

Pour plus d'informations sur les codes d'erreur et la description, reportez-vous au Guide de spécification de l'API de Cisco Security Manager dans le [lien](#) suivant.