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

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

- Diagramme du réseau

Installation/vérification de la licence CSM API

Étapes de configuration

Utiliser l'API CSM

- Log in, méthode
- Obtenir les règles ACL

Vérifier

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 d'API CSM.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Composants utilisés

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

- Serveur CSM
- Licence d'API CSM

```
Product Name: L-CSMPR-API
Product Description: L-CSMPR-API : Cisco Security Manager Pro - License to enable API Access
```

- Appareil de sécurité adaptatif (ASA) géré par CSM
- Un client API. Vous pouvez utiliser cURL, Python ou Postman. Cet article montre l'ensemble du processus avec Postman.

  L'application cliente CSM doit être fermée. Si une application cliente CSM est ouverte, elle doit l'être par un utilisateur différent de celui qui utilise la méthode API. Sinon, l'API renvoie une erreur. Pour connaître les conditions requises supplémentaires pour utiliser la fonction API, reportez-vous au guide suivant. Conditions préalables 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) offre certaines fonctionnalités pour la configuration des périphériques gérés qui doivent être implémentées 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.

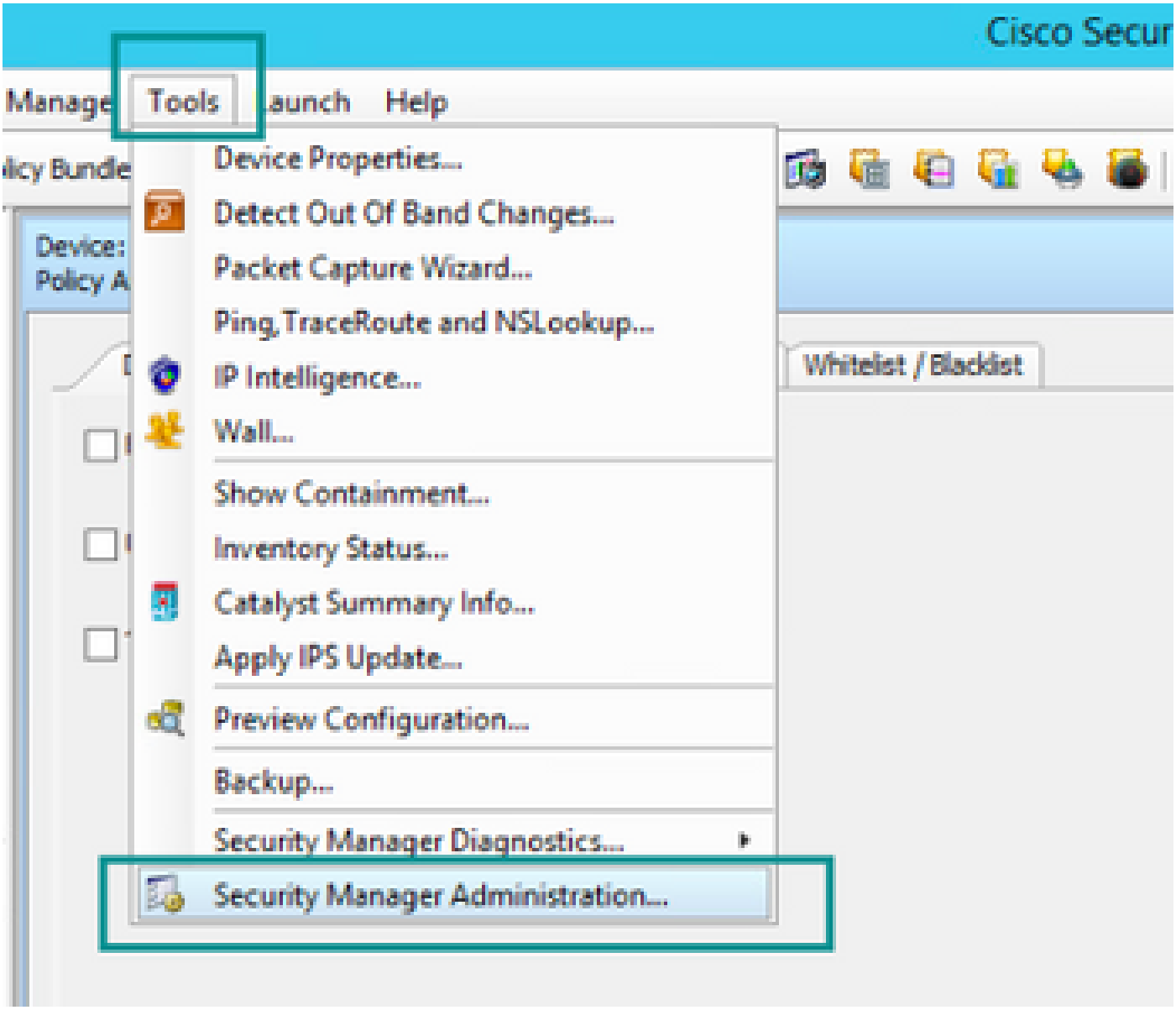
À ces fins, Postman a utilisé comme client API et CSM version 4.19 SP1, ASA 5515 version 9.8(4).

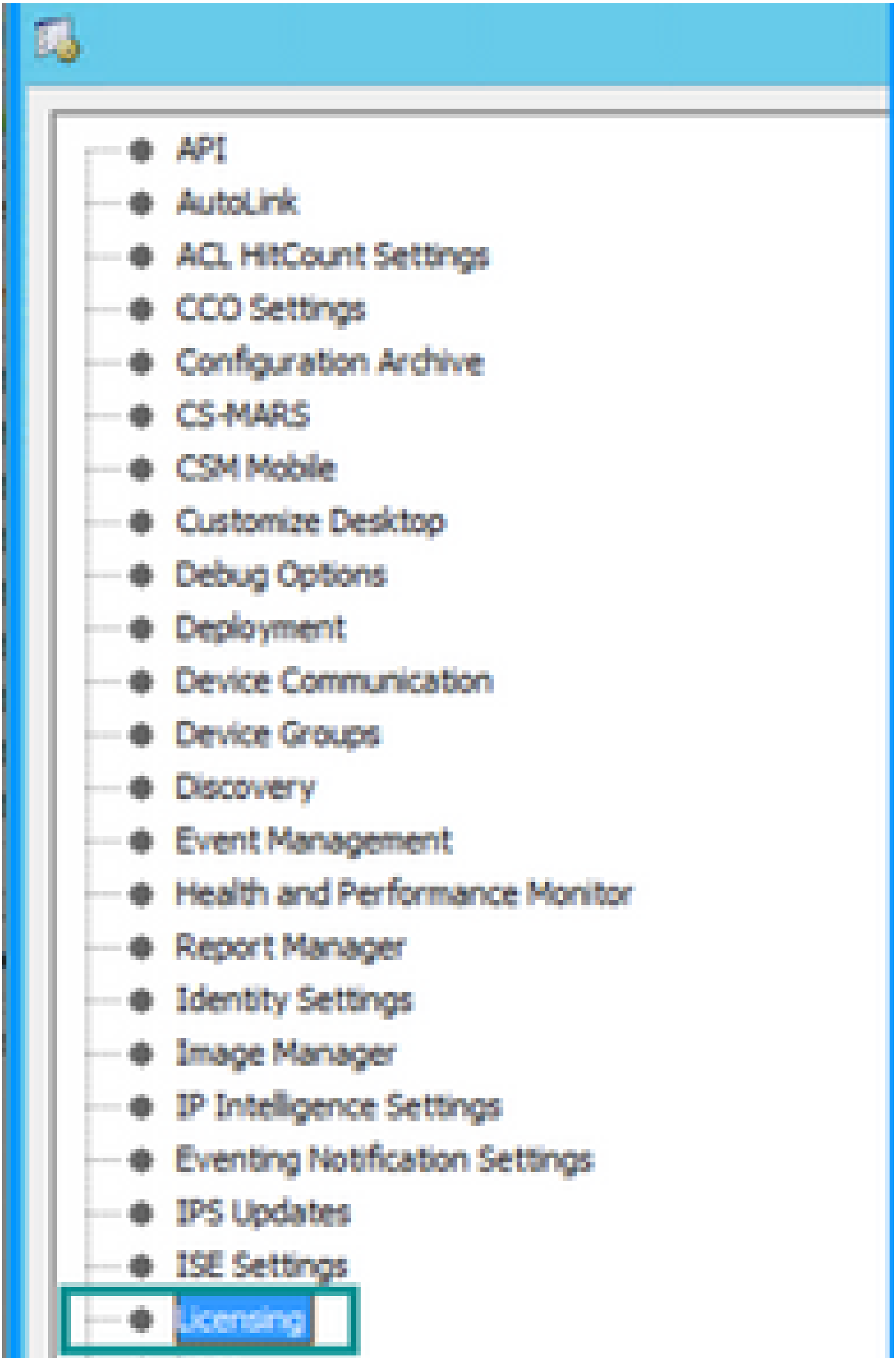
Diagramme du réseau



Installation/vérification de la licence CSM API

CSM API est une fonction sous licence, vous pouvez vérifier que CSM a une licence d'API, dans le client CSM, naviguez à Outils > Administration de Security Manager > Licence page pour confirmer que vous avez une licence déjà installée.


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

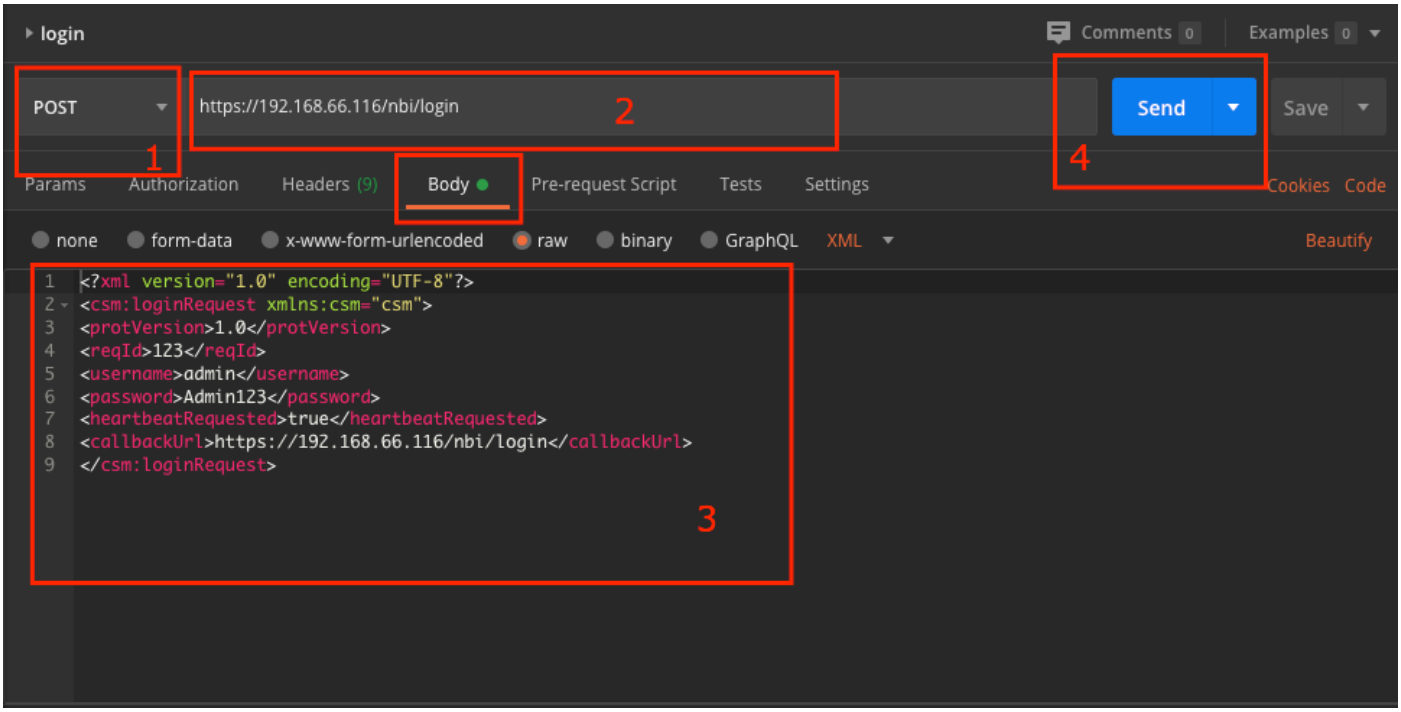

API
AutoLink
ACL HitCount Settings
CCO Settings
Configuration Archive
CS-MARS
CSM Mobile
Customize Desktop
Debug Options
Deployment
Device Communication
Device Groups
Discovery
Event Management
Health and Performance Monitor
Report Manager
Identity Settings
Image Manager
IP Intelligence Settings
Eventing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

: 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 paramétré sur tout ce que l'utilisateur souhaite utiliser comme identifiant.

heartbeatRequested : Cet attribut peut être éventuellement défini. Si l'attribut est défini sur true, le client CSM reçoit un rappel heartbeat 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 au heartbeat, l'API le réessaie 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. Cette valeur doit être spécifiée si heartbeatRequested a la valeur true. Seules les URL de rappel HTTPS sont autorisées

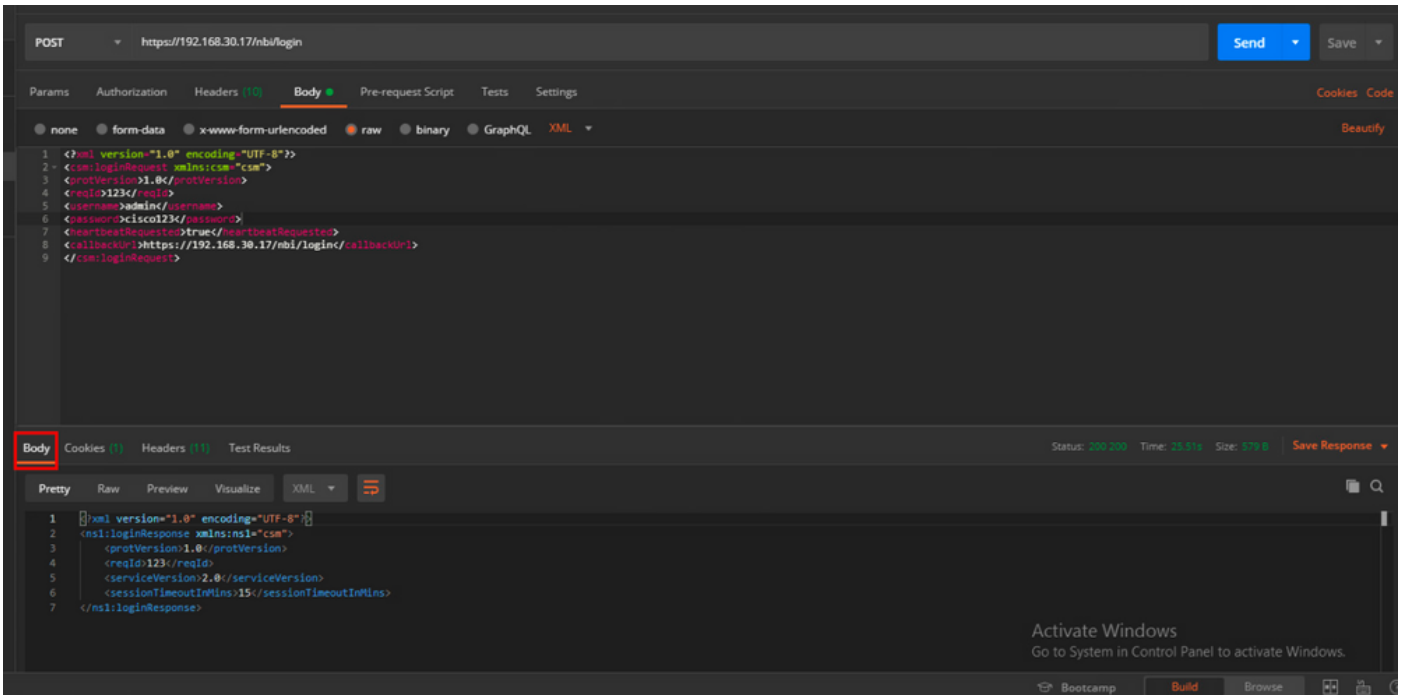
4. Envoyer



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

Réponse

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





Obtenir les règles ACL

Méthode execDeviceReadOnlyCLICmds. L'ensemble des commandes pouvant être exécutées par cette méthode est constitué de commandes en lecture seule telles que des statistiques, des 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

Demande

1. Méthode HTTP : POST

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

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

Entrez la valeur asCookie obtenue précédemment à partir de Method Login.

Clé : Entrez « asCookie ».

Valeur: Valeur d'entrée obtenue.

Cochez cette case pour l'activer.

4. Corps :

```
1.0

123

 192.168.66.1

 show

 access-list
```

Remarque : 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.

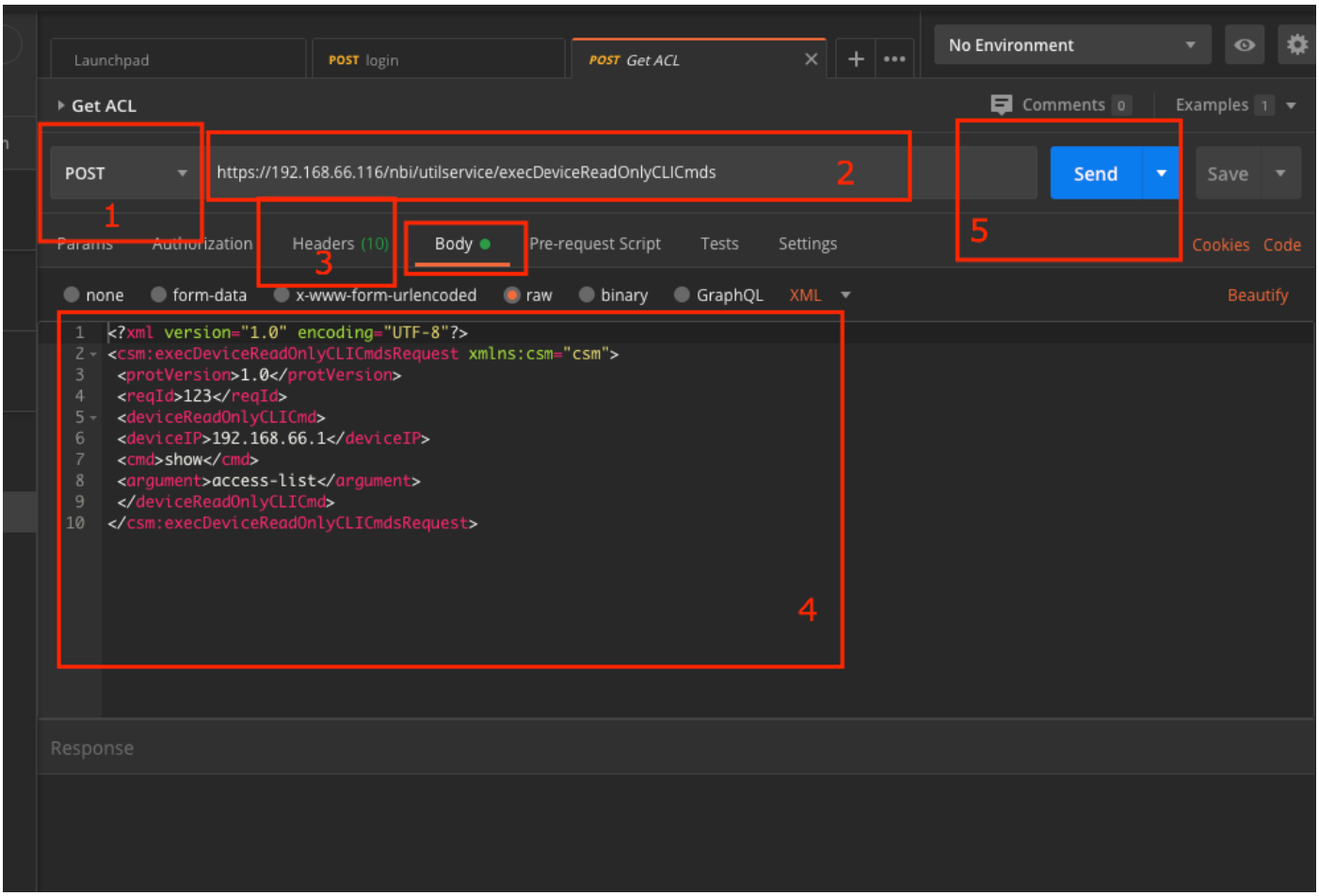
Where:

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

cmd : Commande fixe « show ». L'expression régulière autorise les cas mixtes [sS][hH][oO][wW]

argument : Arguments de la commande show. Comme « run » pour afficher la configuration en cours du périphérique ou « access-list » pour afficher les détails de la liste d'accès.

5. Envoyer

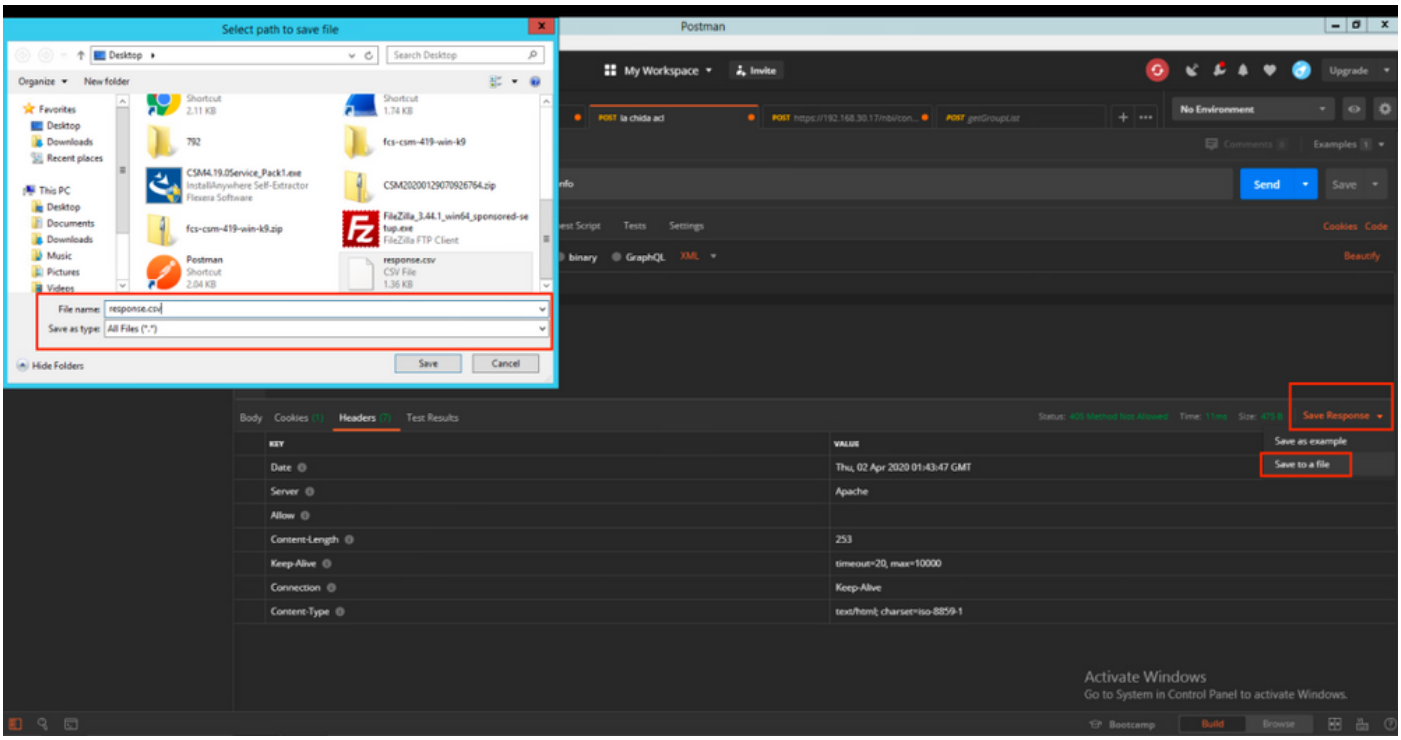


Réponse



Vérifier

Vous avez la possibilité d'enregistrer la réponse en tant que fichier. Naviguez jusqu'à Save Response > Save to a file. Sélectionnez ensuite l'emplacement du fichier et enregistrez-le en tant que type .csv.



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

Dépannage

Réponses possibles en cas d'échec via 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 Licence

Vérifiez que la fonction API est activée sous Outils > Administration de Security Manager > 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 la bonne adresse IP 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 du corps.

4. Aucune connexion au pare-feu.

Motif: Le périphérique n'est pas connecté au CSM

Solution possible : Exécutez un test de connectivité à partir du serveur CSM et dépannez d'autres problèmes de connectivité au périphérique.

Pour plus d'informations sur les codes d'erreur et la description, reportez-vous au guide des spécifications de l'API Cisco Security Manager, disponible sur le lien suivant.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.