Estrai ACL dal CSM in formato CSV tramite metodo API

Sommario

Introduzione

In questo documento viene descritto come estrarre gli Access Control Lists (ACL), in formato CSV (Comma-Separated Values), di un dispositivo gestito da Cisco Security Manager (CSM) tramite il metodo API del CSM.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Security Manager (CSM)
- API CSM
- Conoscenze base API

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Server CSM
- Licenza API CSM
  ```
  Product Name: L-CSMPR-API
  Product Description: L-CSMPR-API : Cisco Security Manager Pro - License to enable API Access
  ```
- Appliance Adaptive Security (ASA) gestita da CSM

- Un client API. È possibile utilizzare cURL, Python o Postman. Questo articolo mostra l'intero processo con Postman. L'applicazione client CSM deve essere chiusa. Se un'applicazione client CSM è aperta, deve essere utilizzata da un utente diverso da quello che utilizza il metodo API. In caso contrario, l'API restituisce un errore. Per ulteriori prerequisiti per l'utilizzo della funzione API, consultare la guida successiva. Prerequisiti API

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Cisco Security Manager (CSM) dispone di alcune funzionalità per la configurazione dei dispositivi gestiti che devono essere implementate tramite l'API.

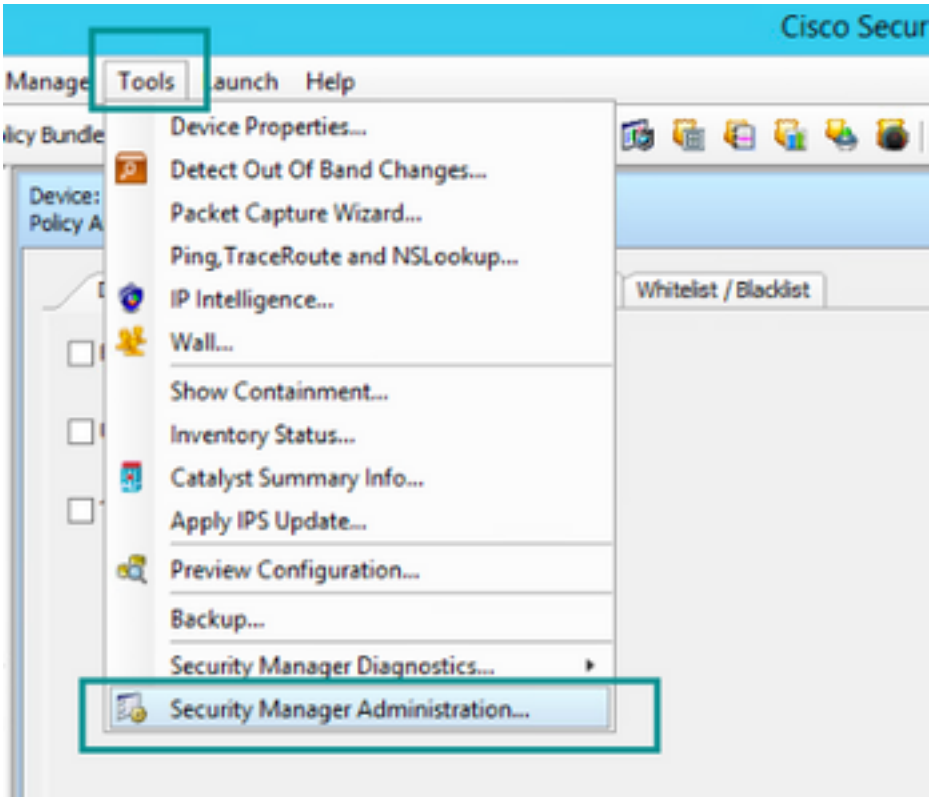
Una di queste opzioni di configurazione è il metodo per estrarre un elenco degli Access Control List (ACL) configurati in ciascun dispositivo gestito da CSM. L'uso dell'API del CSM è l'unico modo finora per soddisfare tale requisito.

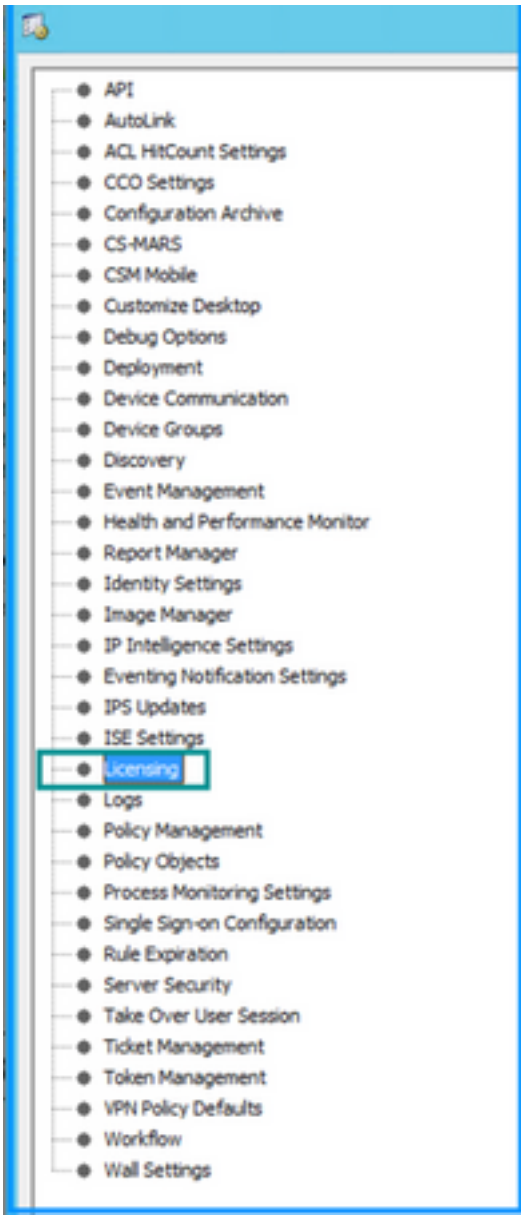
Per questi scopi, Postman ha usato come client API e CSM versione 4.19 SP1, ASA 5515 versione 9.8(4).

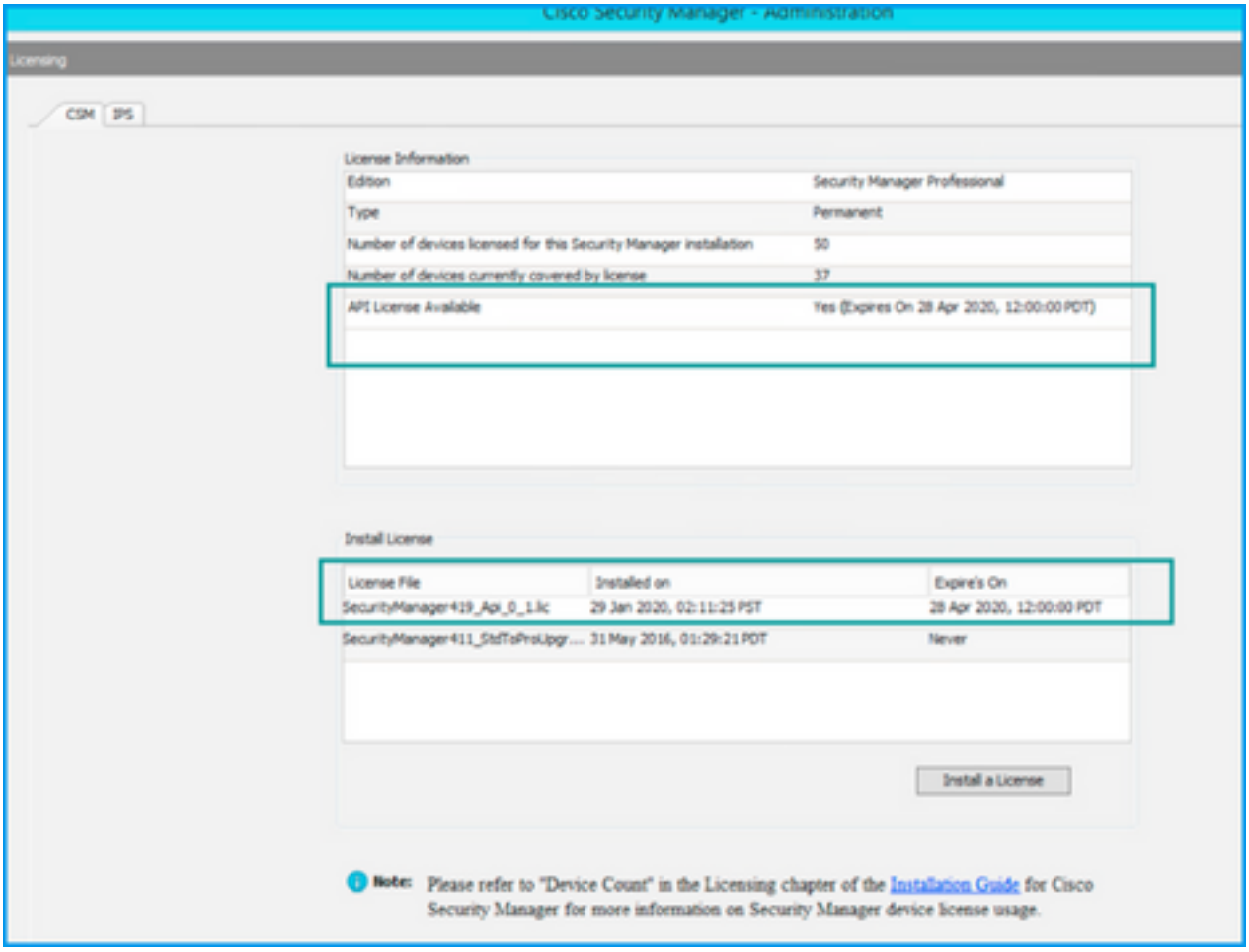
Esempio di rete

Installazione/verifica licenza API CSM

L'API CSM è una funzionalità concessa in licenza. È possibile verificare che il CSM disponga di una licenza API. Nel client CSM, selezionare **Strumenti > Amministrazione Security Manager > Pagina Gestione licenze** per confermare che la licenza è già installata.


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

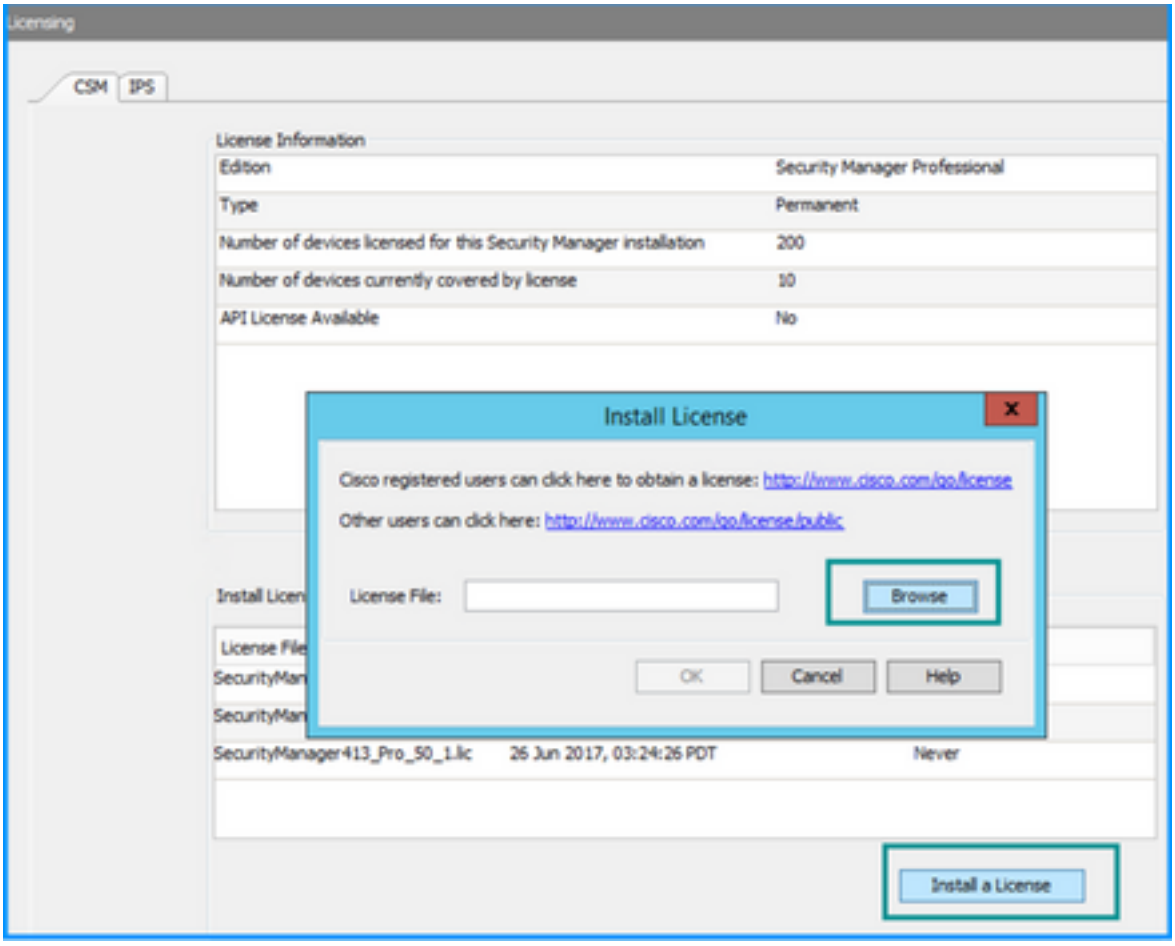

API
AutoLink
ACL HitCount Settings
CCO Settings
Configuration Archive
CS-MARS
CSM Mobile
Customize Desktop
Debug Options
Deployment
Device Communication
Device Groups
Discovery
Event Management
Health and Performance Monitor
Report Manager
Identity Settings
Image Manager
IP Intelligence Settings
Eventing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

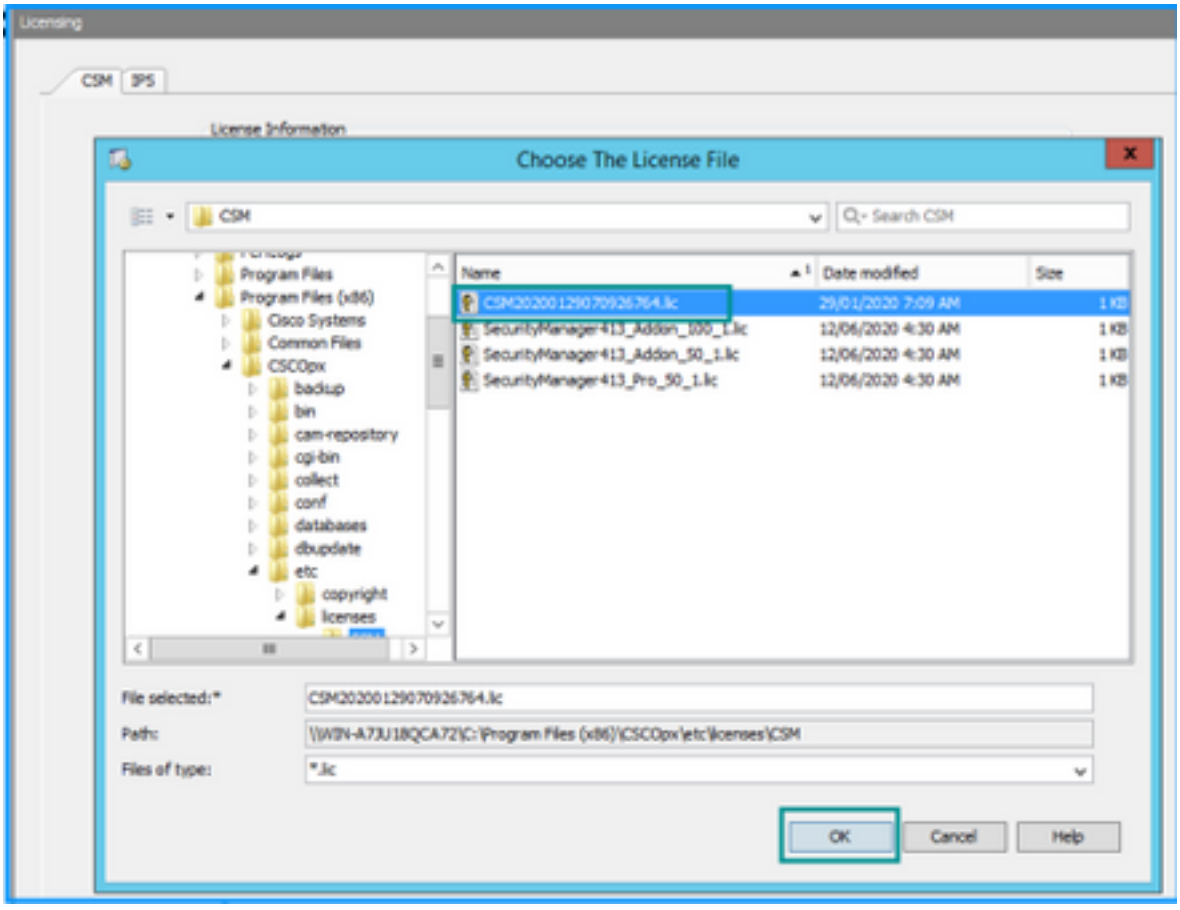


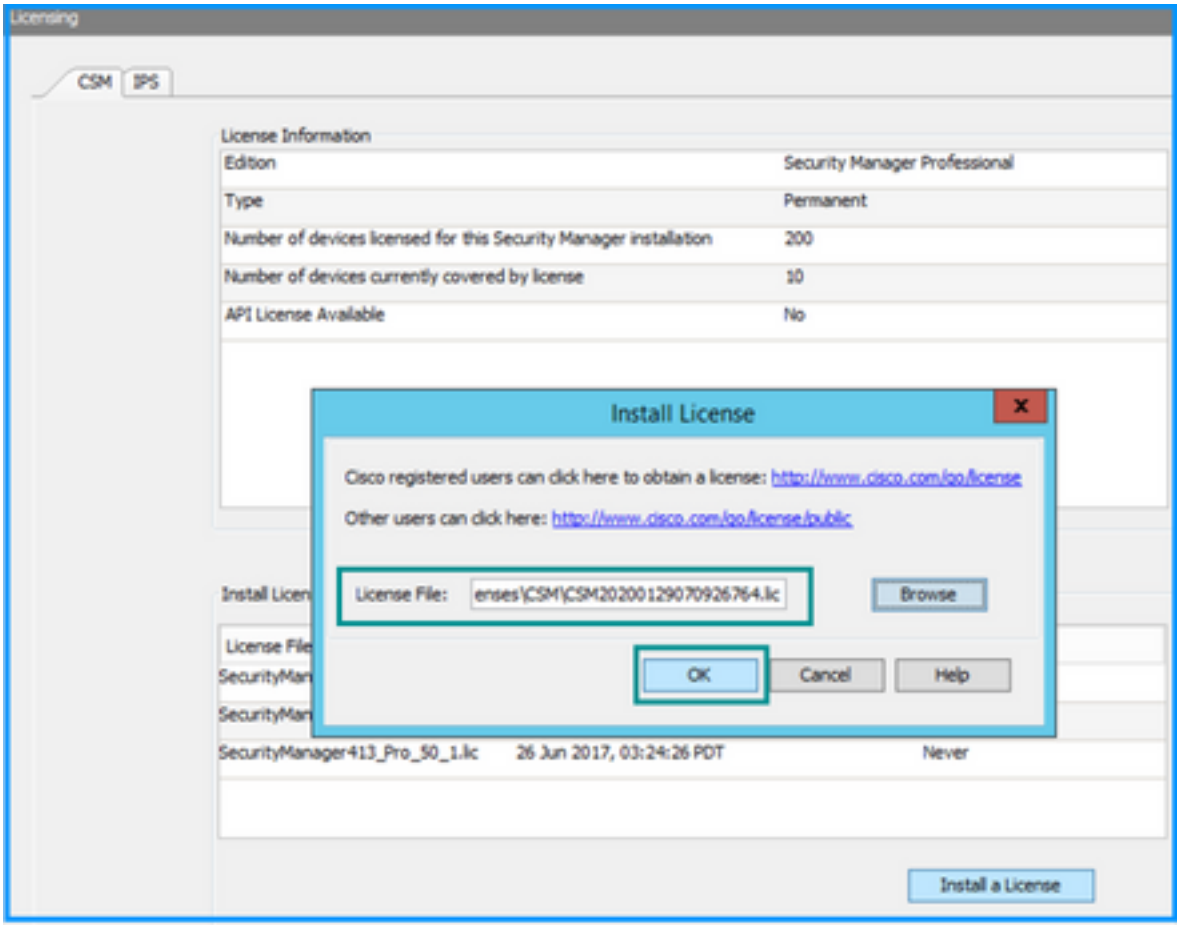
Se non è stata applicata alcuna licenza API ma si dispone già del file .lic su cui è possibile installare la licenza, fare clic sul pulsante **Installa licenza**, quindi memorizzare il file della licenza nello stesso disco in cui si trova il server CSM.

Per installare una nuova licenza di Cisco Security Manager, attenersi alla seguente procedura:

Passaggio 1. Salvare il file di licenza allegato (.lic) dall'e-mail ricevuta nel file system.
Passaggio 2. Copiare il file di licenza salvato in una posizione nota nel file system del server Cisco Security Manager.
Passaggio 3. Avviare il client Cisco Security Manager.
Passaggio 4. Passare a **Strumenti->Amministrazione Security Manager...**
Passaggio 5. Dalla finestra **Cisco Security Manager - Amministrazione**, selezionare **Licensing**
Passaggio 6. Fare clic sul pulsante **Installa licenza**.
Passaggio 7. Dalla finestra di dialogo **Install License**, selezionare il pulsante **Browse** (Sfoglia).
Passaggio 8. Individuare il file della licenza salvato nel file system del server Cisco Security Manager e selezionarlo, quindi fare clic sul pulsante **OK**.
Passaggio 9. Dalla finestra di dialogo **Install License**, fare clic sul pulsante **OK**.
Passaggio 10. Confermare le informazioni sul Riepilogo licenze visualizzate e fare clic sul pulsante **Chiudi**.


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



La licenza API può essere applicata solo su un server con licenza CSM Professional Edition. La licenza non può essere applicata al CSM che esegue un'edizione Standard della licenza. Requisiti licenza API

Fasi della configurazione

Impostazioni client API

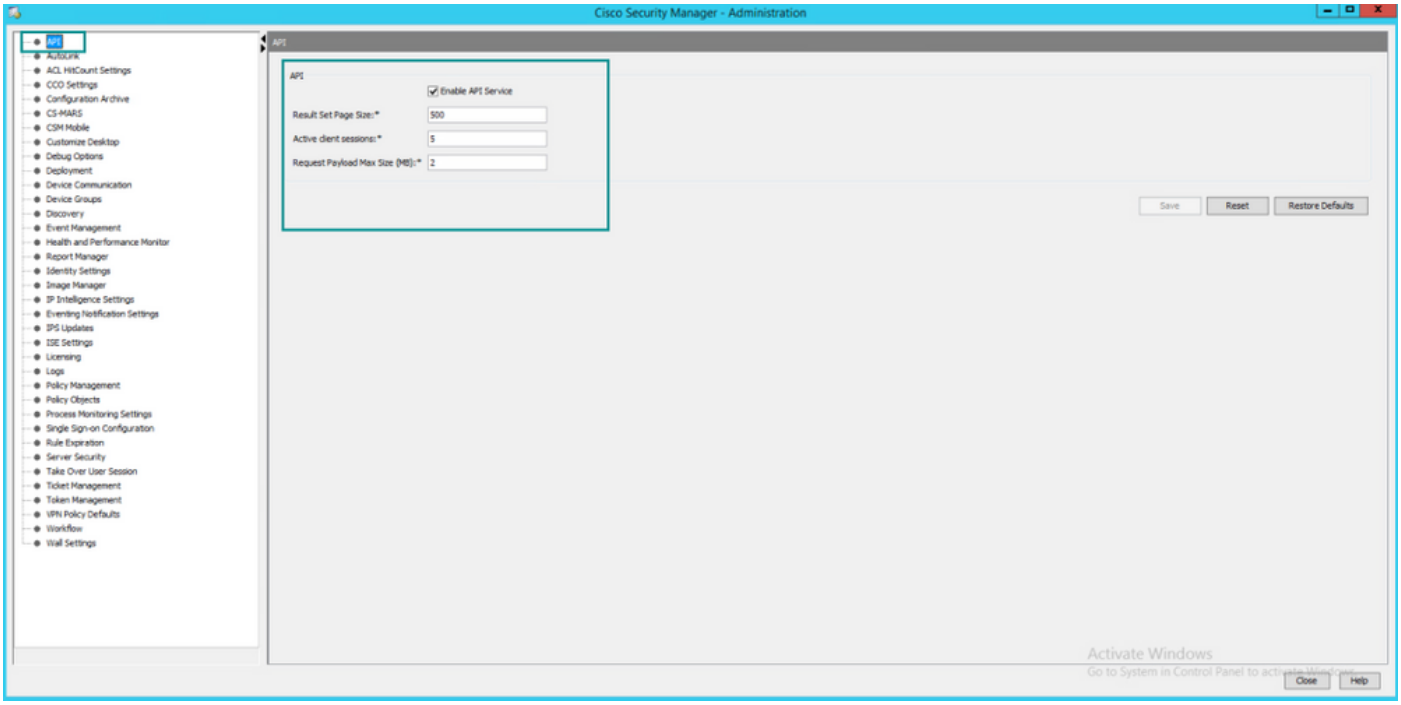
Se si usa Postman ci sono alcune impostazioni che è necessario configurare, dipende da ogni client API, ma deve essere simile.

- Proxy disattivato
- Verifica SSL - DISATTIVATA

Impostazioni CSM

- API abilitata. In **Strumenti > Amministrazione di Security Manager > API**

Impostazioni
API



Uso dell'API CSM

Ènecessario configurare nel client API le due chiamate seguenti:

1. Metodo di login

2. Recupero dei valori ACL

Per riferimento nel processo:

Dettagli di accesso CSM utilizzati in questa esercitazione:

Nome host CSM (indirizzo IP): **192.168.66.116**. Nell'API viene utilizzato il nome host nell'URL.

Utente: **admin**

Password: **Admin123**

Metodo di accesso

Questo metodo deve essere chiamato prima di qualsiasi altro metodo chiamato su altri servizi.

Guida API CSM: Metodo Log in

Richiesta

1. Metodo HTTP: **POST**

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

3. Corpo:

Dove:

Username: Nome utente del client CSM associato alla sessione

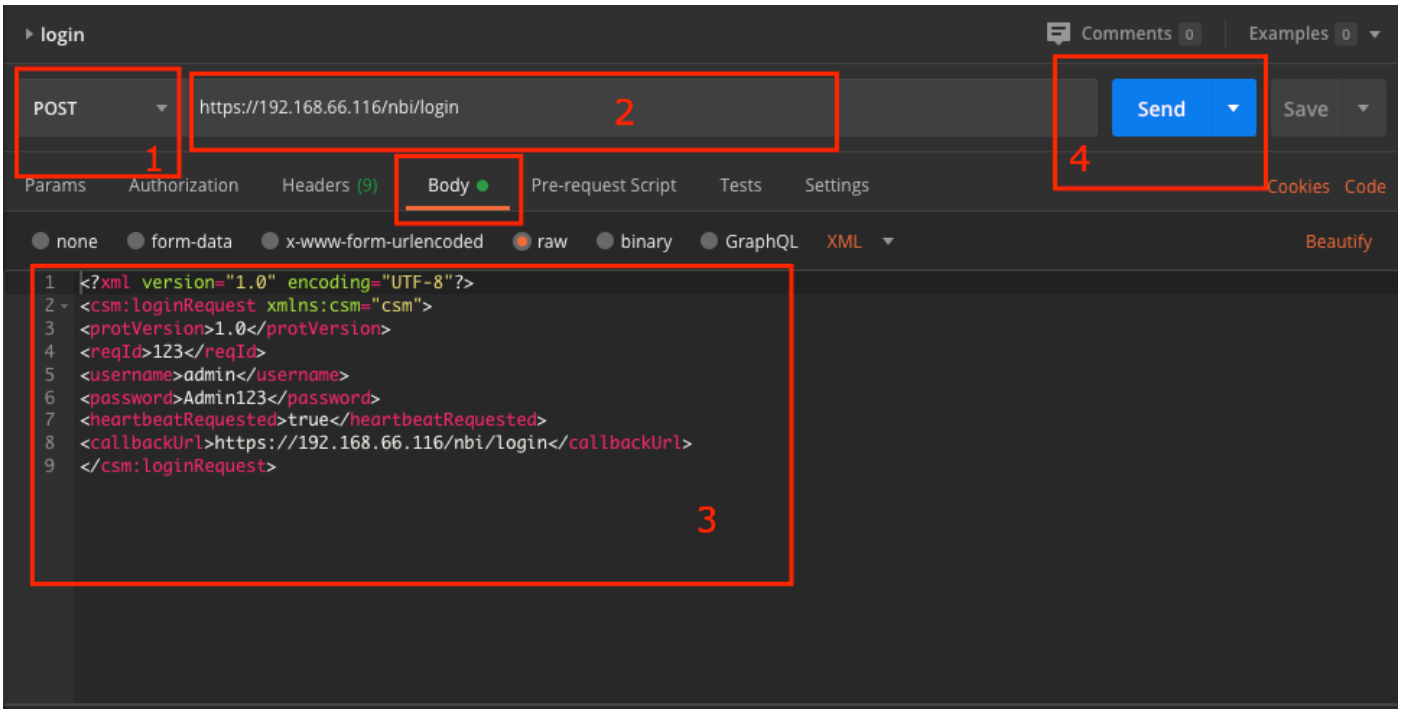
Password: Password del client CSM associata alla sessione.

ID richiesta: Questo attributo identifica in modo univoco una richiesta eseguita dal client. Questo valore viene ripetuto dal server CSM nella risposta associata. Può essere impostato su qualsiasi elemento che l'utente desidera utilizzare come identificatore.

heartbeatRichiesto: Questo attributo può essere definito facoltativamente. Se l'attributo è impostato su true, il client CSM riceve un callback heartbeat dal server CSM. Il server tenta di eseguire il ping sul client con una frequenza vicina a (timeout di inattività) / 2 minuti. Se il client non risponde all'heartbeat, l'API ritenta l'heartbeat durante l'intervallo successivo. Se l'heartbeat ha esito positivo, il timeout di inattività della sessione viene reimpostato.

callbackUrl: URL in cui il server CSM esegue il callback. È necessario specificare questa proprietà se l'elemento heartbeatRequested è true. Sono consentiti solo URL di callback basati su HTTPS

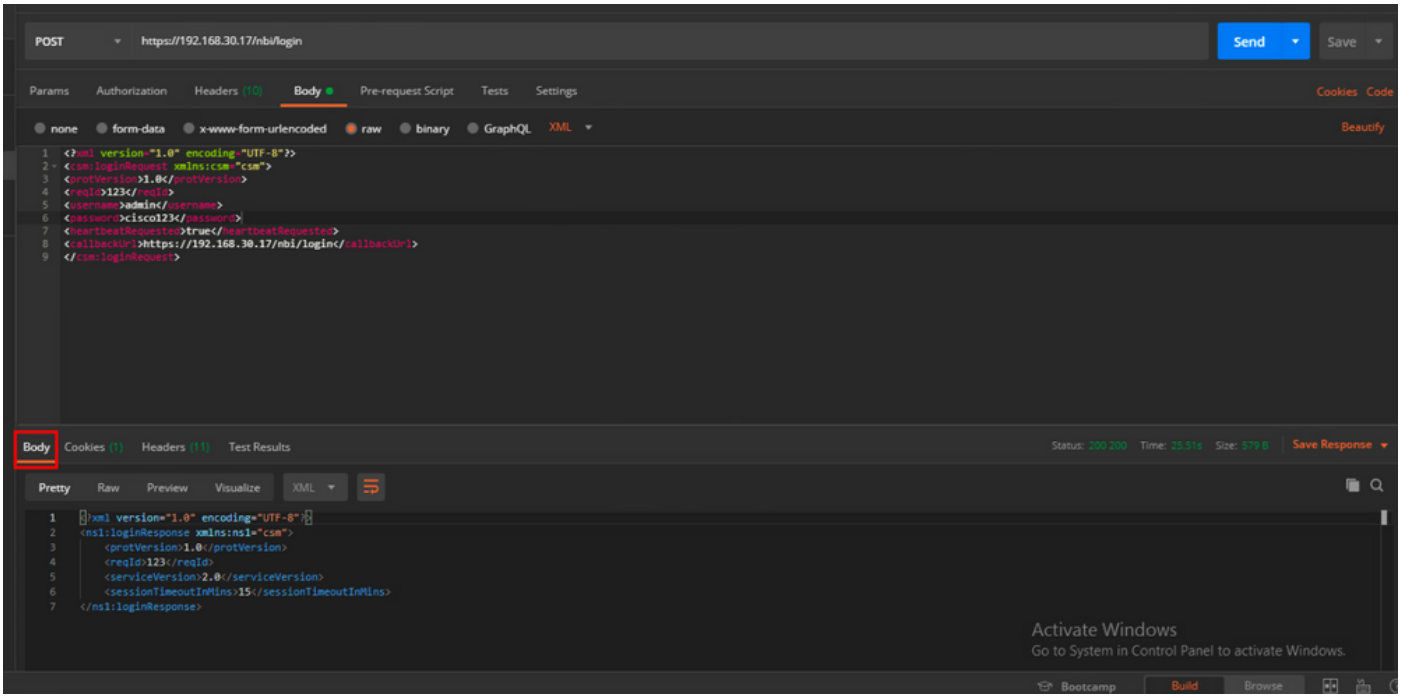
4. Invio



Selezionare l'opzione raw da visualizzare come in questo esempio.

Risposta

L'API di accesso convalida le credenziali utente e restituisce un token di sessione come cookie protetto. Il valore della sessione viene memorizzato nella chiave **asCookie**. È necessario salvare il **valore asCookie**.



Ottieni regole ACL

Metodo execDeviceReadOnlyCLICmds. Il set di comandi che può essere eseguito da questo metodo è di sola lettura, ad esempio le statistiche, i comandi di monitoraggio che forniscono informazioni aggiuntive sul funzionamento del dispositivo specifico.

[Dettagli sul metodo dalla Guida dell'utente dell'API CSM]

Richiesta

1. Metodo HTTP: **POST**

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

3. Intestazione HTTP: Cookie restituito dal metodo di accesso che identifica la sessione di autenticazione.

Immettere il valore asCookie ottenuto in precedenza da Method Login.

Chiave: Immettere "asCookie"

Valore: Valore di input ottenuto.

Fare clic sulla casella di controllo per attivarla.

4. Corpo:

Nota: Il corpo XML sopra riportato può essere utilizzato per eseguire qualsiasi comando "show", ad esempio: "show run all", "show run object", "show run nat" e così via.
L'elemento "<deviceReadOnlyCLICmd>" XML indica che il comando specificato in "<cmd>" e "<topic>" DEVE essere di sola lettura.

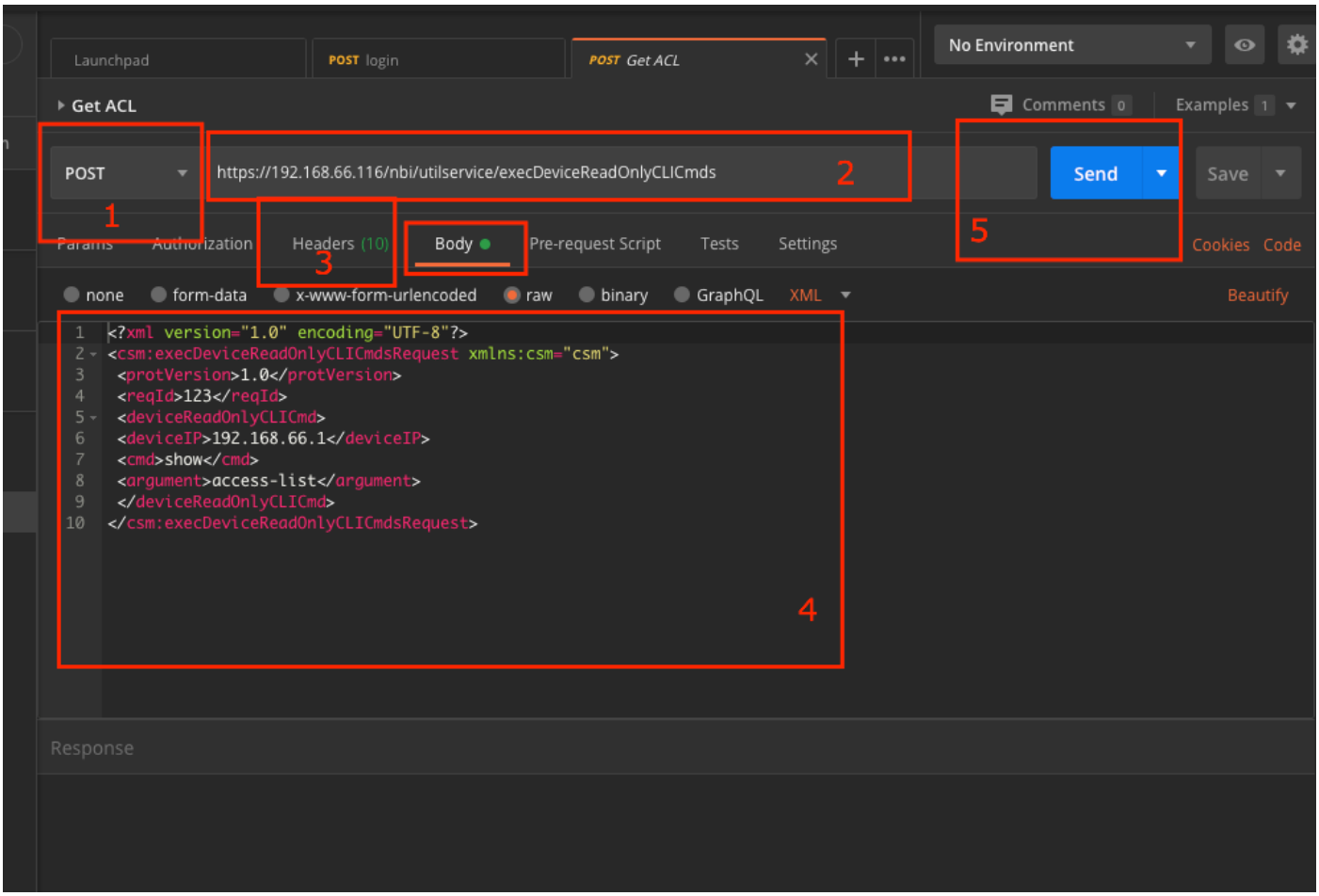
Dove:

IP dispositivo: L'indirizzo IP del dispositivo su cui deve essere eseguito il comando.

cmd: Comando fisso **"show".** Il regex consente l'uso di lettere maiuscole e minuscole miste [sS][hH][oO][wW]

argomento: Gli argomenti del comando show. Simile a "run" per visualizzare la configurazione corrente del dispositivo o a **"access-list"** per visualizzare i dettagli dell'elenco degli accessi.

5. Invia

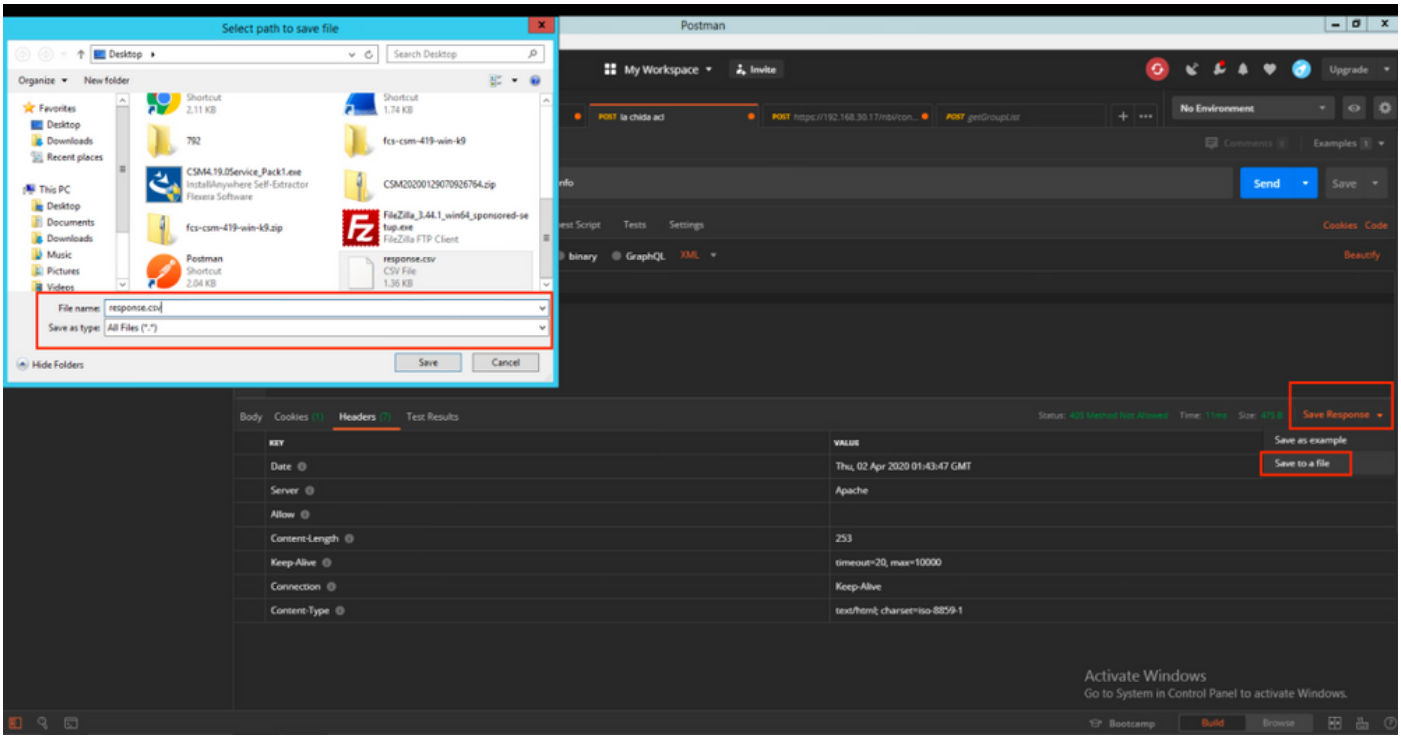


Risposta

<?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>

Verifica

Èpossibile scegliere Salva risposta come file. Passare a **Salva risposta > Salva in un file.** Selezionare il percorso del file e salvarlo come tipo .csv.



Quindi è necessario essere in grado di aprire questo file .csv con l'applicazione Excel, ad esempio. Dal tipo di file .csv, è possibile salvare l'output come altri tipi di file, ad esempio PDF, TXT, ecc.

Risoluzione dei problemi

Possibili risposte di errore tramite API.

1. Nessuna licenza API installata.

Causa: Licenza API scaduta, non installata o non abilitata.

Soluzione possibile: Verificare la data di scadenza della licenza, in **Strumenti > Amministrazione Security Manager > Pagina Gestione licenze**

Verificare che la funzionalità API sia abilitata in **Strumenti > Amministrazione Security Manager > API**

Confermare le impostazioni della sezione **Installazione/verifica licenza API CSM** in alto in questa guida.

2. Indirizzo IP CSM non valido utilizzato per l'accesso API.

Causa: L'indirizzo IP del server CSM non è corretto nell'URL della chiamata API.

Soluzione possibile: Verificare nell'URL del client API che il nome host sia l'indirizzo IP corretto del server CSM.

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

3. Indirizzo IP ASA errato.

Causa: L'indirizzo IP definito nel corpo tra i tag <deviceIP></deviceIP> non deve essere quello corretto.

Soluzione possibile: Verificare che l'indirizzo IP del dispositivo corretto sia definito nella sintassi del corpo.

4. Nessuna connessione al firewall.

Causa: Il dispositivo non è collegato al CSM

Soluzione possibile: Eseguire un test della connettività dal server CSM e risolvere i problemi di ulteriore connettività al dispositivo.

Per ulteriori dettagli sui codici di errore e la descrizione, consultare la guida alle specifiche dell'API Cisco Security Manager nel collegamento successivo.