

APIメソッドによるCSV形式のCSMからのACLの抽出

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[ネットワーク図](#)

[CSM APIライセンスのインストール/検証](#)

[設定手順](#)

[CSM APIを使用する](#)

[ログイン方法](#)

[ACLルールの取得](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、CSM APIメソッドを介してCisco Security Manager(CSM)によって管理されるデバイスのアクセスコントロールリスト(ACL)をカンマ区切り値(CSV)形式で抽出する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Security Manager(CSM)
- CSM API
- APIの基礎知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CSMサーバ
- CSM APIライセンス
Product Name: L-CSMPR-API
Product Description: L-CSMPR-API : Cisco Security Manager Pro - License to enable API Access
- CSMで管理される適応型セキュリティアプライアンス(ASA)
- APIクライアント。cURL、Python、またはPostmanを使用できます。この記事では、

Postmanのプロセス全体を示します。CSMクライアントアプリケーションを閉じる必要があります。CSMクライアントアプリケーションが開いている場合、はAPIメソッドを使用するユーザとは異なるユーザである必要があります。それ以外の場合、APIはエラーを返します。API機能を使用するための追加の前提条件については、次のガイドを使用できます。[APIの前提条件](#)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Cisco Security Manager(CSM)には、APIを介して実装する必要がある管理対象デバイス設定の機能がいくつかあります。

これらの設定オプションの1つは、CSMによって管理される各デバイスで設定されているアクセスコントロールリスト(ACL)のリストを抽出する方法です。この要件を達成するには、CSM APIを使用する方法しかありません。

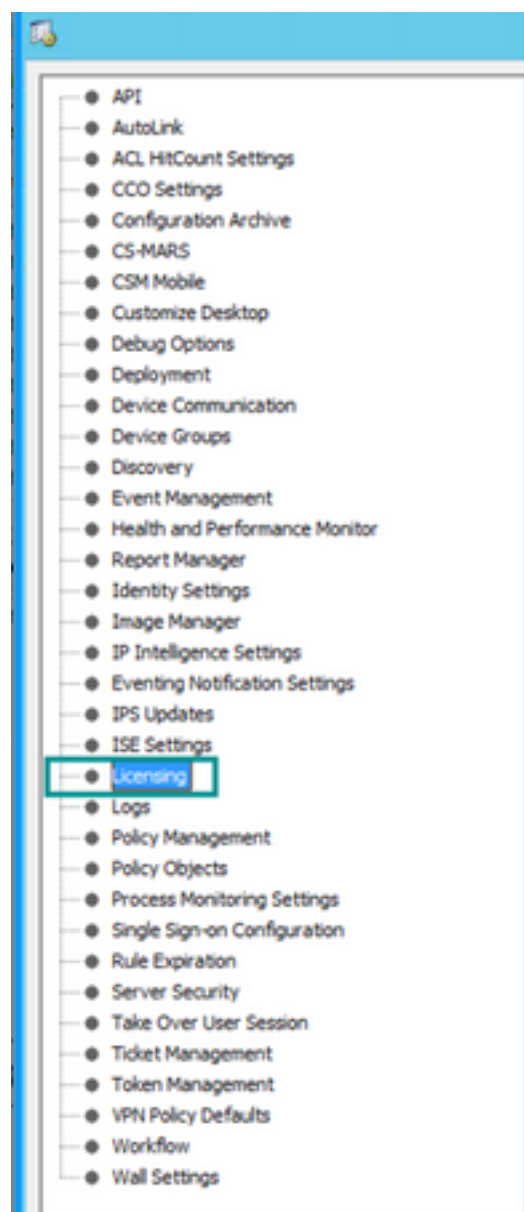
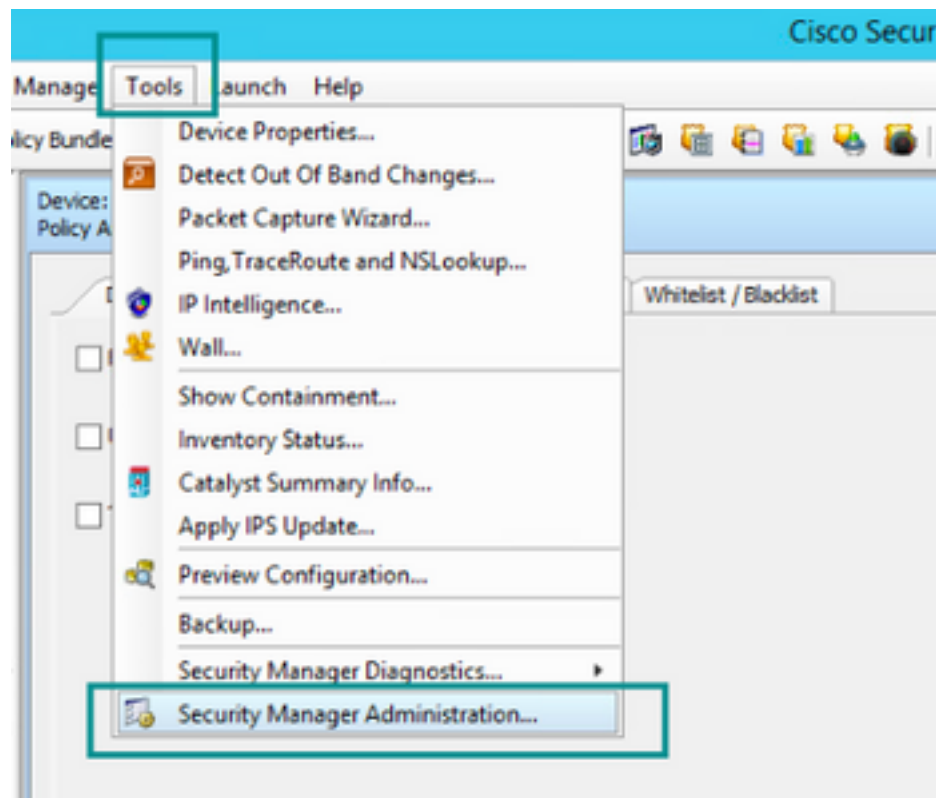
これらの目的のために、PostmanはAPIクライアントおよびCSMバージョン4.19 SP1、ASA 5515バージョン9.8(4)として使用されます。

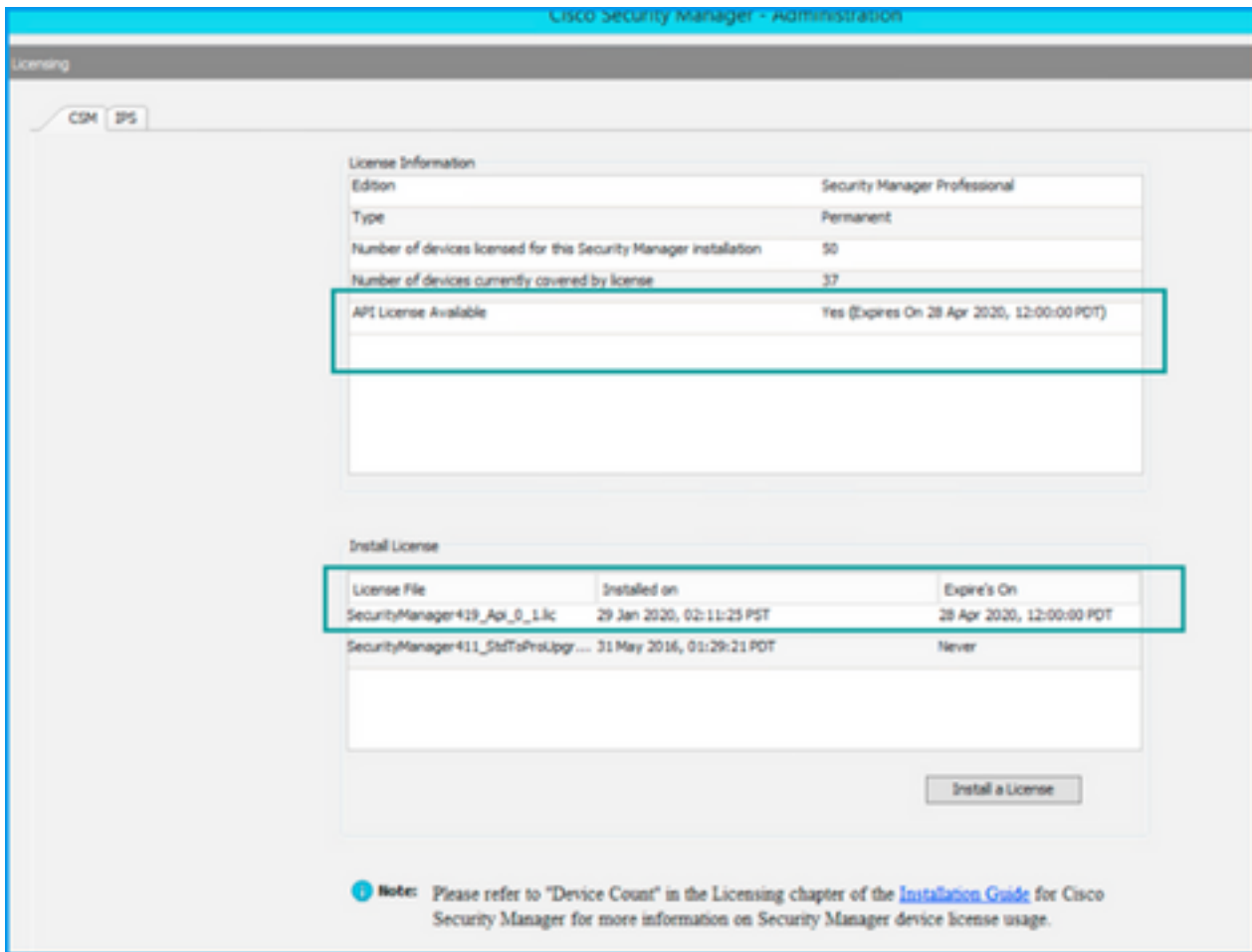
ネットワーク図



CSM APIライセンスのインストール/検証

CSM APIはライセンス済みの機能です。CSMクライアントで、[Tools] > [Security Manager Administration] > [Licensing]ページに移動し、ライセンスがすでにインストールされていることを確認します。





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_Apr_0_Lic	29 Jan 2020, 02:11:25 PST	28 Apr 2020, 12:00:00 PDT
SecurityManager411_StdToPrsUpgr...	31 May 2016, 01:29:21 PDT	Never

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.

APIライセンスが適用されていないが、ライセンスをインストールできる.licファイルがすでに存在する場合は、[Install a License]ボタンをクリックし、CSMサーバがある同じディスクにライセンスファイルを保存する必要があります。

新しいCisco Security Managerライセンスをインストールするには、次の手順を実行します。

ステップ1：受信した電子メールから添付したライセンスファイル(.lic)をファイルシステムに保存します。

ステップ2：保存したライセンスファイルをCisco Security Managerサーバのファイルシステム上の既知の場所にコピーします。

ステップ3: Cisco Security Managerクライアントを起動します。

ステップ4:[Tools] > [Security Manager Administration...]に移動します。

ステップ5:[Cisco Security Manager - Administration]ウィンドウで、[Licensing]を選択します

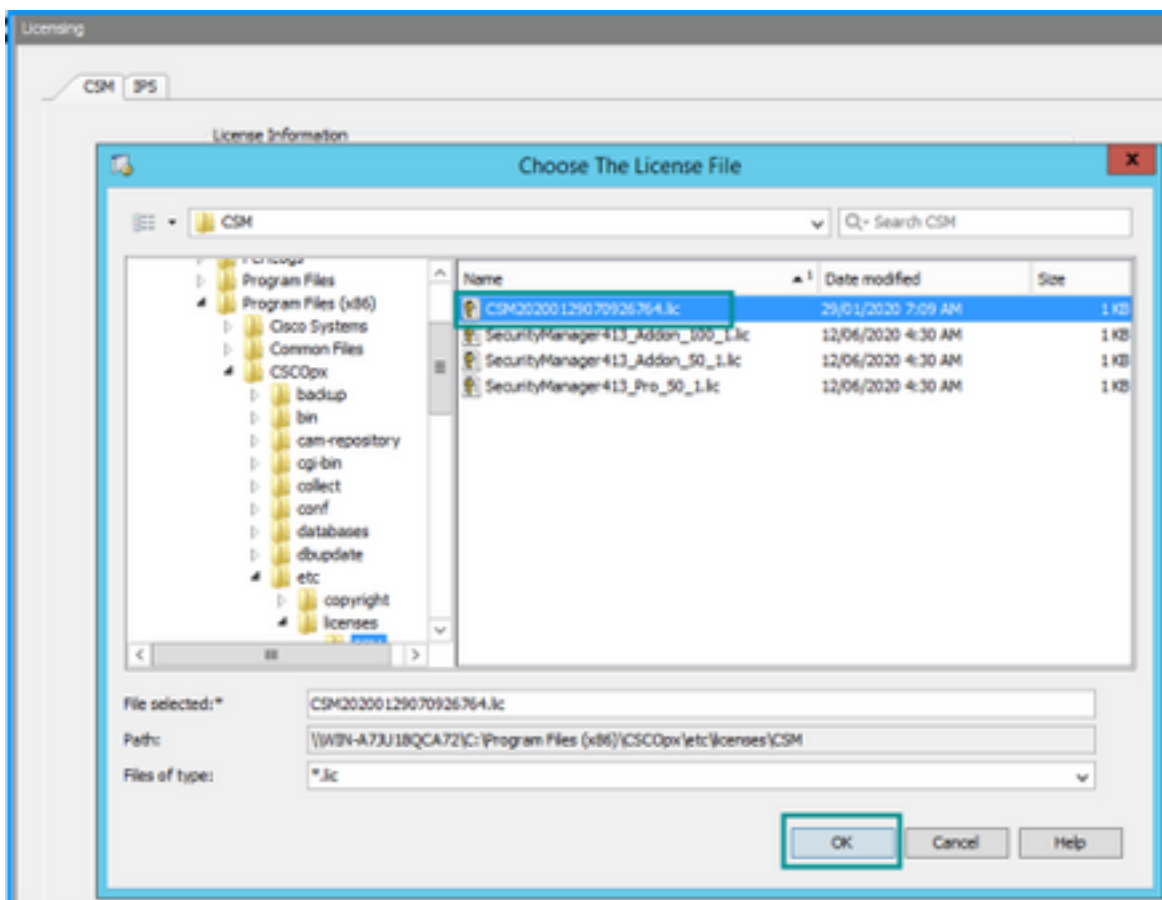
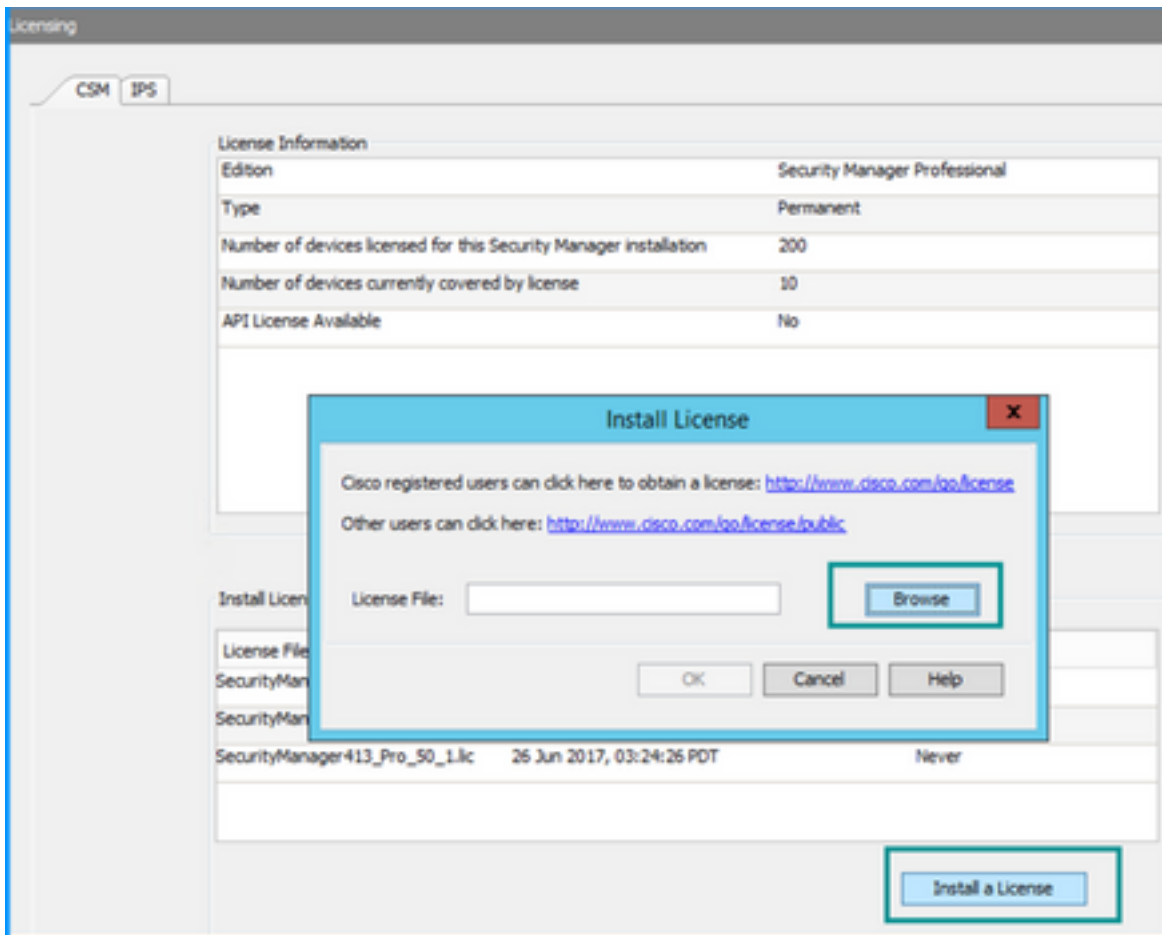
ステップ6:[Install a License]ボタンをクリックします。

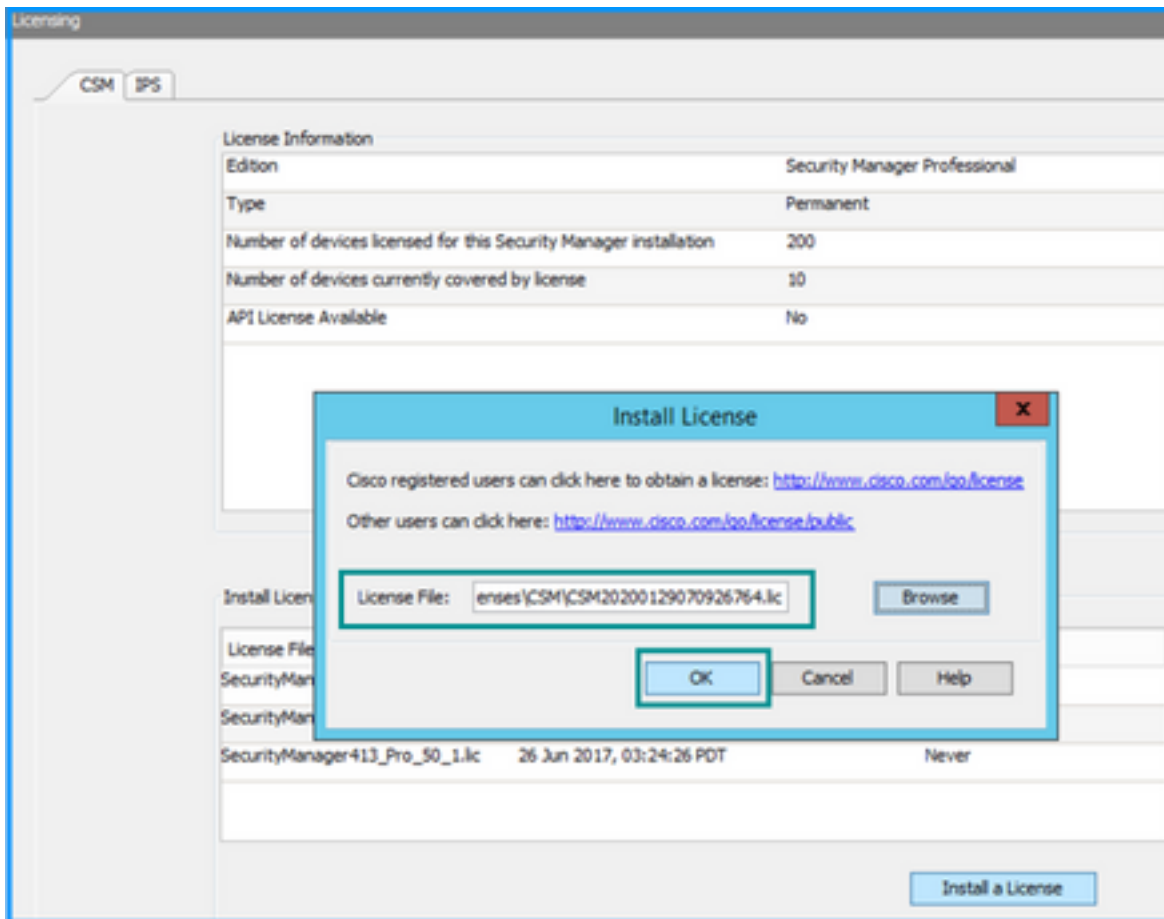
ステップ7:[ライセンスのインストール]ダイアログで、[参照]ボタンを選択します。

ステップ8: Cisco Security Managerサーバのファイルシステムに保存されているライセンスファイルに移動して選択し、[OK]ボタンを選択します。

ステップ9:[Install License]ダイアログボックスで、[OK]ボタンをクリックします。

ステップ10：表示された[License Summary]情報を確認し、[Close]ボタンをクリックします。





APIライセンスは、CSM professional editionのライセンスを受けたサーバにのみ適用できます。ライセンスのStandardエディションを実行しているCSMには、ライセンスを適用できません。

[APIライセンス要件](#)

設定手順

APIクライアントの設定

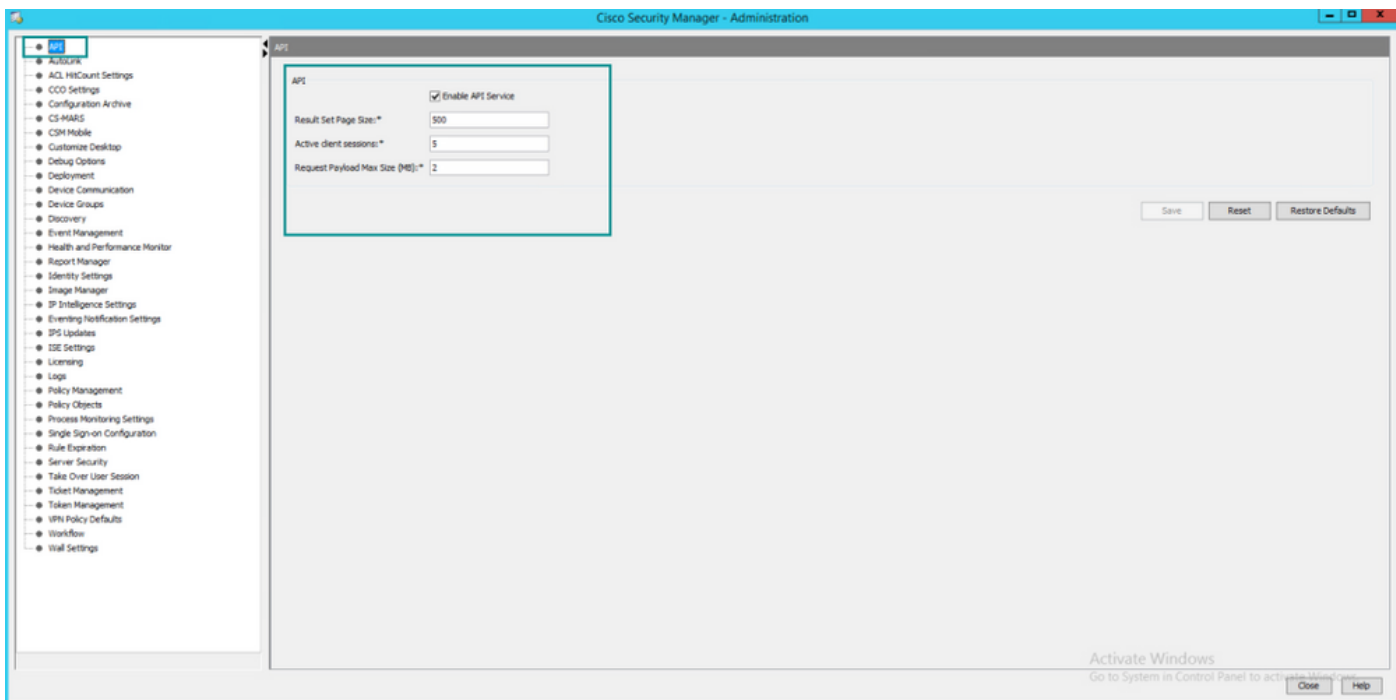
Postmanを使用する場合は、設定が必要な設定があります。これは各APIクライアントによって異なりますが、類似している必要があります。

- プロキシが無効
- SSL検証：オフ

CSMの設定

- 有効なAPI。[Tools] > [Security Manager Administration] > [API]の順に選択します。

[API設定](#)



CSM APIを使用する

APIクライアントで次の2つのコールを設定する必要があります。

1. ログイン方式
2. ACL値の取得

プロセスを参照するには、次の手順を実行します。

この実習で使用するCSMアクセスの詳細：

CSMホスト名 (IPアドレス) :192.168.66.116.APIでは、URLのホスト名を使用します。

User:admin

パスワード : Admin123

ログイン方法

このメソッドは、他のサービスで呼び出される他のメソッドよりも前に呼び出す必要があります。

[CSM APIガイド : メソッドログイン](#)

Request

1. HTTPメソッド : **POST**
2. URL:https://<hostname>/nbi/login
3. 本文 :

場所 :

ユーザ名:セッションに関連付けられたCSMクライアントのユーザ名

パスワード : セッションに関連付けられているCSMクライアントパスワード。

reqId:この属性は、クライアントによって実行された要求を一意に識別します。この値は、関連付けられた応答でCSMサーバによってエコーされます。ユーザがIDとして使用するすべての設定が可能です。

heartbeatRequested:この属性はオプションで定義できます。属性がtrueに設定されている場合、CSMクライアントはCSMサーバからハートビートコールバックを受信します。サーバは、(非アクティビタムアウト)/2分に近い頻度でクライアントにpingを実行しようとします。クライアントがハートビートに回答しない場合、APIは次の間隔でハートビートを再試行します。ハートビートに成功すると、セッションの非アクティビタムアウトがリセットされます。

callbackUrl:CSMサーバがコールバックを行うURL。これは、heartbeatRequestedがtrueの場合に指定する必要があります。HTTPSベースのコールバックURLのみが許可されます

4.送信

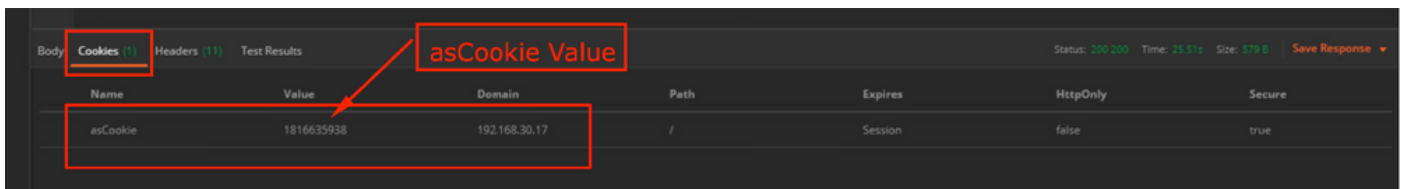
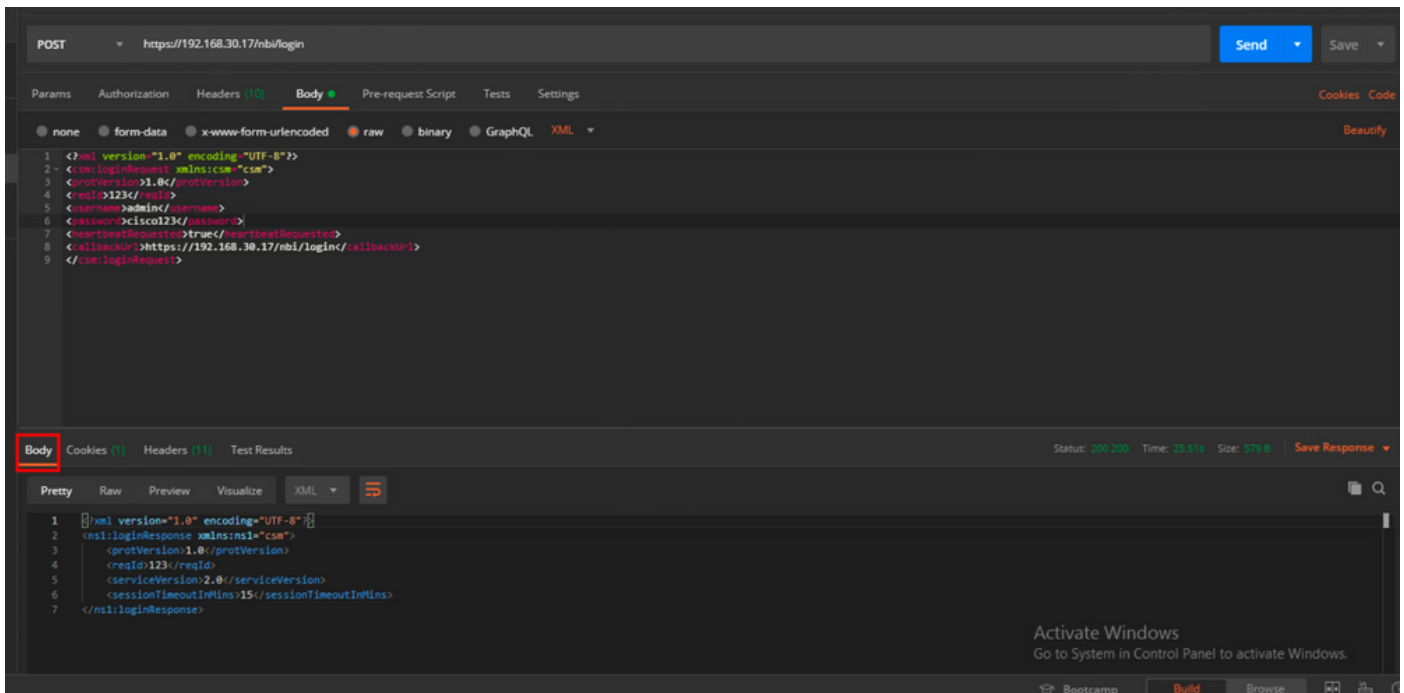
The screenshot shows a REST client interface for a POST request to `https://192.168.66.116/nbi/login`. The request body is an XML document:

```
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>
```

rawオプションを選択すると、この例のように表示されます。

応答

Login APIはユーザクレデンシャルを検証し、セッショントークンをセキュアなcookieとして返します。セッション値はasCookieキーの下に格納され、これをCookie値として保存する必要があります。



ACLルールの取得

メソッド `execDeviceReadOnlyCLICmds`。この方法で実行できるコマンドのセットは、統計情報、監視コマンドなど、特定のデバイスの動作に関する追加情報を提供する読み取り専用コマンドです。

[CSM APIユーザガイドのメソッドの詳細](#)

Request

1. HTTPメソッド : **POST**
2. URL: `https://hostname/nbi/utlilservice/execDeviceReadOnlyCLICmds`
3. HTTPヘッダー : 認証セッションを識別するログイン方式によって返されるcookie。

メソッドログインから取得したasCookie値を入力します。

ポイント : 「asCookie」を入力

[Value] : 入力値を取得しました。

チェックボックスをクリックして有効にします。

4.本文 :

注：上記のXML本文を使用すると、次のような「show」コマンドを実行できます。「show run all」、「show run object」、「show run nat」など

XML "<deviceReadOnlyCLICmd>"要素は、「<cmd>」および「<argument>」で指定されたコマンドが読み取り専用であることを示します。

場所：

deviceIP: コマンドを実行する必要があるデバイスのIPアドレス。

cmd: コマンド「show」を修正。regexでは、大文字と小文字を混在させることができます [sS][hH][oO][wW]

引数: showコマンドの引数。デバイスの実行コンフィギュレーションを表示する「run」や、アクセスリストの詳細を表示する「access-list」と同様に使用します。

5.送信

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

- 1: Method dropdown menu set to POST.
- 2: URL field containing https://192.168.66.116/nbi/utl/service/execDeviceReadOnlyCLICmds.
- 3: Headers tab selected, showing 10 headers.
- 4: Body tab selected, containing XML content for a device read-only CLI command request.
- 5: Send button.

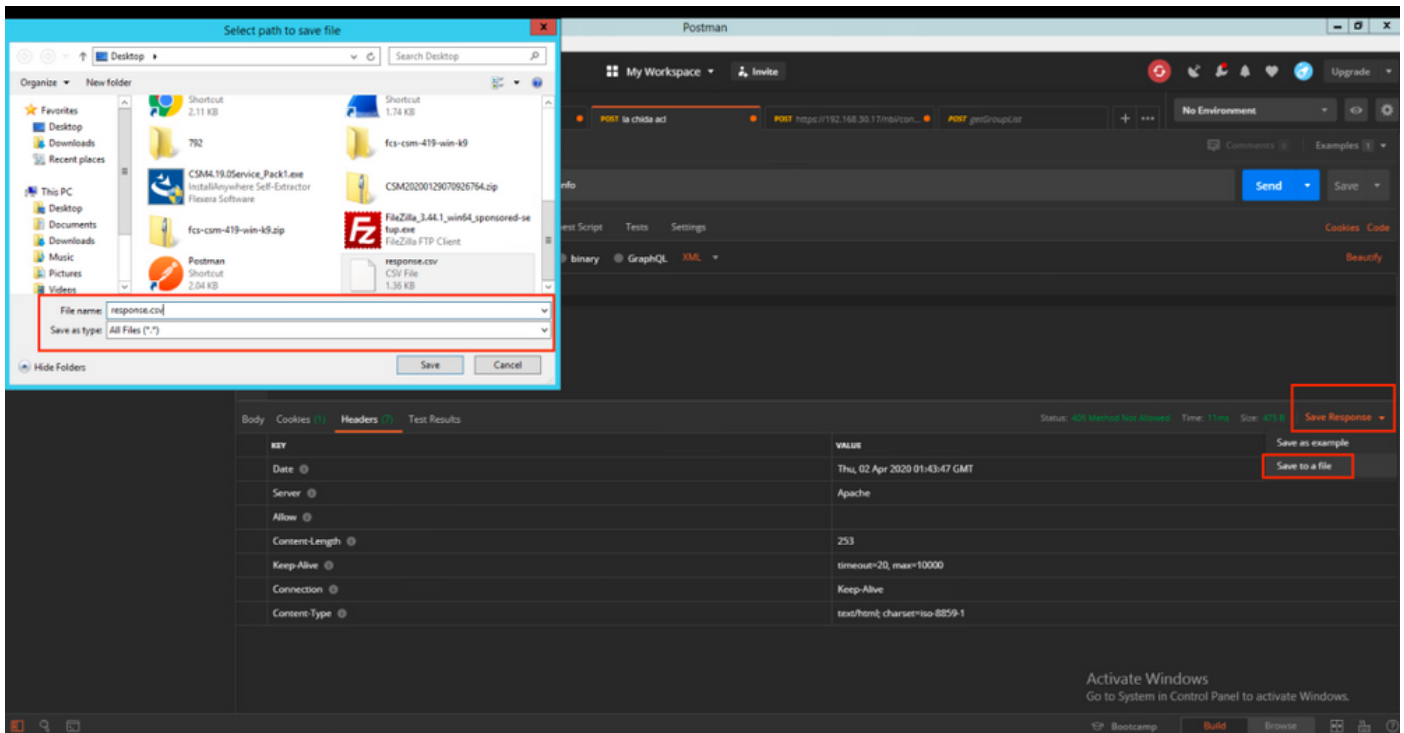
```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <csm:execDeviceReadOnlyCLICmdsRequest xmlns:csm="csm">
3   <protVersion>1.0</protVersion>
4   <reqId>123</reqId>
5   <deviceReadOnlyCLICmd>
6     <deviceIP>192.168.66.1</deviceIP>
7     <cmd>show</cmd>
8     <argument>access-list</argument>
9   </deviceReadOnlyCLICmd>
10 </csm:execDeviceReadOnlyCLICmdsRequest>
```

応答

```
<?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>
```

確認

[Save Response as a File]オプションがあります。「レスポンスの保存」>「ファイルに保存」に移動します。次に、ファイルの場所を選択し、.csvタイプで保存します。



次に、この.csvファイルをExcelアプリケーションで開くことができるようにする必要があります。 .csvファイルタイプから、出力をPDF、TXTなどの他のファイルタイプとして保存できます。

トラブルシューティング

APIを使用して発生する可能性のあるエラー応答。

1. APIライセンスがインストールされていません。

原因：APIライセンスの有効期限が切れているか、インストールされていないか、有効になっていません。

考えられる解決策：[Tools] > [Security Manager Administration] > [Licensing]ページで、ライセンスの有効期限を確認します

[Tools] > [Security Manager Administration] > [API]でAPI機能が有効になっていることを確認します

このガイドの上の「CSM APIライセンスのインストールと検証」セクションの設定を確認します。

2. APIログインに使用されているCSM IPアドレスが正しくありません。

原因：CSMサーバのIPアドレスがAPI呼び出しのURLに間違っています。

考えられる解決策：APIクライアントのURLで、ホスト名がCSMサーバの正しいIPアドレスであることを確認します。

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

3.誤ったASA IPアドレス。

原因：<deviceIP></deviceIP>タグの間のBodyに定義されているIPアドレスは、正しいものであってはなりません。

考えられる解決策：正しいデバイスのIPアドレスが[Body Syntax]で定義されていることを確認します。

4.ファイアウォールへの接続なし。

原因：デバイスはCSMと接続していません

考えられる解決策：CSMサーバからテスト接続を実行し、デバイスへのさらなる接続のトラブルシューティングを行います。

エラーコードと説明の詳細については、次のリンクにある『Cisco Security Manager API Specification Guide』を参照してください。