# API 방법을 통해 CSM에서 CSV 형식으로 ACL 추 출

### 목차

소개 <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>배경 정보</u> <u>네트워크 다이어그램</u> <u>CSM API 라이센스 설치/확인</u> <u>구성 단계</u> <u>CSM API 작업</u> <u>로그인 방법</u> <u>ACL 규칙 가져오기</u> <u>다음을 확인합니다.</u> 문제 해결

### 소개

이 문서에서는 CSM(Cisco Security Manager)에서 CSM API 방법을 통해 관리하는 디바이스의 ACL(Access Control List)을 CSV(Comma-Separated Values) 형식으로 추출하는 방법에 대해 설명 합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CSM(Cisco Security Manager)
- CSM API
- API 기본 지식

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- CSM 서버
- CSM API 라이센스 Product Name: L-CSMPR-API Product Description: L-CSMPR-API : Cisco Security Manager Pro - License to enable API Access
- CSM에서 관리하는 ASA(Adaptive Security Appliance)
- API 클라이언트.cURL, Python 또는 Postman을 사용할 수 있습니다.이 기사는 Postman의 전

체 프로세스를 보여줍니다. CSM 클라이언트 애플리케이션을 닫아야 합니다.CSM 클라이언트 애플리케이션이 열려 있는 경우 는 API 메서드를 사용하는 사용자와는 다른 사용자여야 합니다 .그렇지 않으면 API에서 오류를 반환합니다.API 기능을 사용하기 위한 추가 사전 요구 사항을 보려면 다음 가이드를 사용할 수 있습니다.API 사전 요구 사항

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

### 배경 정보

CSM(Cisco Security Manager)에는 API를 통해 구현해야 하는 관리되는 디바이스 컨피그레이션에 대한 몇 가지 기능이 있습니다.

이러한 구성 옵션 중 하나는 CSM에서 관리하는 각 디바이스에 구성된 ACL(Access Control List) 목 록을 추출하는 방법입니다.지금까지 CSM API를 사용하는 것이 이 요구 사항을 충족하는 유일한 방 법입니다.

이러한 목적으로 Postman은 API Client 및 CSM 버전 4.19 SP1, ASA 5515 버전 9.8(4)으로 사용됩니다.

### 네트워크 다이어그램

CSM GUI Client



## CSM API 라이센스 설치/확인

CSM API는 라이센스 기능입니다. CSM에 API 라이센스가 있는지 확인할 수 있습니다. CSM 클라 이언트에서는 Tools > Security Manager Administration > Licensing 페이지로 이동하여 라이센스가 이미 설치되어 있는지 확인합니다.



#### ۵,

#### 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

SM PS		
	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	
	Install License	Expire's On
	License File Installed on SecurityManager419_Api_0_1.1c 29 Jan 2020, 02:11:25 PST	Expire's On 28 Apr 2020, 12:00:00 PDT
	Install License License Pile Installed on SecurityManager419_Api_0_1.1c 29 Jan 2020, 02:11:25 PST SecurityManager411_StdTaProUpgr 31 May 2016, 01:29:21 PDT	Expire's On 28 Apr 2020, 12:00:00 PDT Never
	Install License License File Sistalled on SecurityManager419_Api_0_1.1c 29 Jan 2020, 02:11:25 PST SecurityManager411_StdToProUpgr 31 May 2016, 01:29:21 PDT	Expire's On 28 Apr 2020, 12:00:00 PDT Never

적용된 API 라이센스가 없지만 이미 .lic 파일을 가지고 있는 경우 라이센스를 설치할 수 있는 경우 Install a License(라이센스 설치) 버튼을 클릭하고 CSM 서버가 있는 동일한 디스크 아래에 라이센 스 파일을 저장해야 합니다.

최신 Cisco Security Manager 라이센스를 설치하려면 다음 단계를 수행하십시오.

1단계. 받은 이메일에서 첨부 라이센스 파일(.lic)을 파일 시스템에 저장합니다.

2단계. 저장된 라이센스 파일을 Cisco Security Manager 서버 파일 시스템의 알려진 위치에 복사합니다.

3단계. Cisco Security Manager Client를 시작합니다.

4단계. Tools(툴)->Security Manager Administration(보안 관리자 관리)으로 이동합니다.

5단계. **Cisco Security Manager - Administration**(**Cisco 보안 관리자 - 관리**) 창에서 Licensing(라이 센싱)을 선택합니다.

6단계. Install a License(라이센스 설치) 버튼을 클릭합니다.

7단계. Install License(라이센스 설치) 대화 상자에서 Browse(찾아보기) 버튼을 선택합니다.

8단계. Cisco Security Manager 서버 파일 시스템에서 저장된 라이센스 파일을 찾아 선택하고 **확인** 버튼을 선택합니다.

9단계. **라이센스 설치** 대화 상자에서 **확인** 버튼을 클릭합니다.

10단계. 표시된 라이센스 요약 정보를 확인하고 닫기 버튼을 클릭합니다.

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
Ucense File  License File  CK	Browse Cancel Help
SecurityManager413_Pro_50_1.lc 26 Jun 2017, 03:24:26 PDT	Never

19 <b>9</b> - 19		Choose The License File			
)III • 🎽 CSM			♥ ] Q,+ Search CSH		
Pro	gram Files	Name	Date modified	Size	
4 🎍 Pro	gram Piles (x86)	🔮 CSM20200 1290 70926764.lc	29/01/2020 7:09 AM	10	
	Common Files	SecurityManager413_Addon_100_1.lc	12/06/2020 4:30 AM	18	
1 1	CSCOpx	SecurityManager413_Addon_50_1.1c	12/06/2020 4:30 AM	19	
	cam-repository cpi-bin collect conf databases dbupdete etc copyright icenses	×			
File selected:*	C5M20200129070	926764.Ac			
	\(WIN-A73U18QCA72\C: \Program Files (x86)\CSCOpx\etc\(censes\CSM				
Path:					

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 Licen License File: enses\CSM\CSM2020012907092676	A.lc Browse
License File	
SecurityMan OK	Cancel Help
SecurityMan	
pecuntymanager+13_PT0_50_1.1c 26 Jun 2017, 03(24)26 PDT	rvever

API 라이센스는 CSM Professional Edition용으로 라이센스가 부여된 서버에만 적용할 수 있습니다 .라이센스의 Standard 버전을 실행하는 CSM에는 라이센스를 적용할 수 없습니다.<u>API 라이센스 요</u> <u>구 사항</u>

# 구성 단계

#### API 클라이언트 설정

Postman을 사용하는 경우 구성해야 하는 설정이 있으면 각 API 클라이언트에 따라 다르지만 비슷 해야 합니다.

• 프록시 사용 안 함

• SSL 확인 - 꺼짐

CSM 설정

• 활성화된 API입니다.Tools > Security Manager Administration > API에서 API 설정

<b>A</b>	Cisco Security Manager - Administration	_ <b>_</b> ×
Allocat     A	Art Art Result Set Payload Max Size (Mg).* 2 Result Set Payload Max Size (Mg).* 2	Save Reset Restore Defaults
Report Nanoper     Report Nanoper     Sounds Settings     Sounds Settings     Portalipance Settings		
Aut Expansion     Server Searly     Tata Over User Search     Tata Over User Search     Total Management     Total Management     Who Not Default     Workflow     Wood Search     Wood Searchy		
		Go to System in Control Panel to activate Wind over

### CSM API 작업

아래의 두 가지 호출을 API 클라이언트에서 구성해야 합니다.

- 1. 로그인 방법
- 2. ACL 값 가져오기
- 프로세스를 통한 참조:

이 실습에서 사용되는 CSM 액세스 세부 정보:

CSM 호스트 이름(IP 주소):192.168.66.116. API에서 URL의 호스트 이름을 사용합니다.

사용자:**관리자** 

암호:**관리자123** 

#### 로그인 방법

이 메서드는 다른 서비스에서 호출되는 다른 메서드 앞에 와야 합니다.

CSM API 가이드:메서드 로그인

#### 요청

- 1. HTTP 방법:POST
- 2. url:https://<hostname>/nbi/login
- 3. 본문

위치:

사용자 이름:세션과 연결된 CSM 클라이언트 사용자 이름

암호:세션과 연결된 CSM 클라이언트 비밀번호.

**reqld**:이 특성은 클라이언트에서 수행한 요청을 고유하게 식별하며, 이 값은 CSM 서버가 연결된 응 답에서 에코됩니다.사용자가 식별자로 사용하려는 모든 항목으로 설정할 수 있습니다.

**하트비트요청됨**:이 속성은 선택적으로 정의할 수 있습니다.특성이 true로 설정된 경우 CSM 클라이 언트는 CSM 서버로부터 하트비트 콜백을 수신합니다.서버가 2분에 가까운 빈도(비활성 시간 제한 )로 클라이언트에 ping을 시도합니다.클라이언트가 하트비트에 응답하지 않으면 API는 다음 간격 동안 하트비트를 재시도합니다.하트비트가 성공하면 세션 비활성 시간 제한이 재설정됩니다.

**콜백URL**:CSM 서버가 콜백을 만드는 URL입니다.heartbeatRequested가 true인 경우 이 값을 지정 해야 합니다.HTTPS 기반 콜백 URL만 허용됩니다.

▶ login Comments 0 https://192.168.66.116/nbi/login POST Send Body 🔵 Settings Params Authorization none 🔵 form-data 🛛 🔍 x-www-form-urlencoded 🛛 🕘 raw 💭 binary 💭 GraphQL k?xml version="1.0" encoding="UTF-8"?>
<csm:loginRequest xmlns:csm="csm"> 1>1.0</ qId>123</ me>admin</u d>Admin123</p <callbackUrl>https://192.168.66.116/nbi/login</callbackUrl></csm:loginReguest>

4. 보내기

이 예와 같이 표시하려면 raw 옵션을 선택합니다.

#### 응답

Login API는 사용자 자격 증명을 확인하고 세션 토큰을 보안 쿠키로 반환합니다.세션 값은 asCookie 키 아래에 저장되며 이 값을 **Cookie 값으로 저장해야 합니다**.

POST + https://192.168.30.17/nbi/login	Send - Save -
Params Authorization Headers (10) Body  Pre-request Script Tests Settings	
● none ● form-data ● x-www-form-urlencoded ● raw ● binary ● GraphQL XML ▼	
1 ().ml version="1.0" encoding="UIF-0">> 2 ~ (csm:loginRequest mains:csm="csm"> 3 cprotVersion:).4(/protVersion> 4 creqL>122(/regL> 5 customest-admin(/uername>	
6 <password>cisco123</password>	
<pre>c cliss(kr) https://i52.166.30.17/mbi/login//callosektrl&gt; 9 c//smilogin@equal()</pre>	
Body Cookies (1) Headers (11) Test Results Status: 200 2	
Pretty Raw Preview Visualize XML 🔻 📅	<b>a</b> Q
1 []/xml version="1.0" encoding="UF-6";] 2 cnsl:loginResponse xmlms:nsl="csm"> 3 cprutVersion:lof/protVersion> 4 creqId:123 5 cservd:ceVersion>2.6 6 csessionTimeoutInMins> 7 c/nsl:loginResponse>	
Activate W Go to System	
🖼 Bootcamp	Build Browse 🖬 🖄 (

Body	Cookies (1) Headers (11)	Test Results	asCookie Valu			
	Name	Value	Domain	Path	HttpOnly	

### ACL 규칙 가져오기

**execDeviceReadOnlyCLICmds 메서드를 사용합니다.**이 방법으로 실행할 수 있는 명령 집합은 통계 , 특정 디바이스의 작업에 대한 추가 정보를 제공하는 모니터링 명령과 같은 읽기 전용 명령입니다.

### <u>CSM API 사용 설명서의 방법 세부사항</u>

#### 요청

- 1. HTTP 방법:**POST**
- 2. url:https://hostname/nbi/utilservice/execDeviceReadOnlyCLICmds
- 3. HTTP 헤더:인증 세션을 식별하는 로그인 방법에서 반환되는 쿠키.

메서드 **로그인**에서 이전에 가져온 asCookie 값을 입력합니다.

키:"asCookie"를 입력합니다.

가치:입력 값을 가져왔습니다.

확인란을 클릭하여 활성화합니다.

#### 4. 본문

**참고:**위의 XML 본문을 사용하여 다음과 같이 "show" 명령을 실행할 수 있습니다."show run all", "show run object", "show run nat" 등

XML "<deviceReadOnlyCLICmd>" 요소는 "<cmd>" 및 "<argument>" 내에 지정된 명령 이 읽기 전용임을 나타냅니다.

#### 위치:

**디바이스IP**:명령을 실행해야 하는 디바이스 IP 주소입니다.

cmd:고정 명령 "show"입니다.regex는 대/소문자 [sS][hH][oO][wW]를 혼합하여 사용할 수 있습니다.

**인수**:show 명령 인수입니다.디바이스의 실행 중인 컨피그레이션을 표시하려면 "run"을 선택하고 액 세스 목록 세부사항을 표시하려면 **"access-list**"를 선택합니다.

5. 보내기

Launchpa		POST login	POST Get ACL	× + •••	No Environment	• • •
▶ Get ACL					📮 Comments 🛛	Examples 1 🔻
POST	→ https://192.	168.66.116/nbi/utilservice/execD	eviceReadOnlyCLICmds	2	Send	▼ Save <del>▼</del>
Params	Authorization H	eaders (10) Body • Pi	e-request Script Tests	Settings	5	Cookies Code
none	🔵 form-data 🛛 🔍 🗴	-www-form-urlencoded 🛛 💿 ra	w 🔵 binary 🗨 Graph0	QL XML ▼		
1 K7X 2 ~ <cs 3 ~ op 4 ~ or 5 ~ <d 6 ~ <d 7 ~ co 8 &lt; aa 9 ~ <!--</td--><td>mt version= 1.0 e m:execDeviceReadOn rotVersions1.0 eqId&gt;123 eviceReadOnlyCLICm eviceIP&gt;192.168.66 md&gt;show rgument&gt;access-lis deviceReadOnlyCLIC sm:execDeviceReadO</td><td><pre>https://www.ncounge-one-ary- lyCLICmdsRequest xmlns:cs otVersion&gt; d&gt; .1 t md&gt; nlyCLICmdsRequest&gt;</pre></td><td>m="CSM"&gt;</td><td>4</td><td></td><td></td></d </d </cs 	mt version= 1.0 e m:execDeviceReadOn rotVersions1.0 eqId>123 eviceReadOnlyCLICm eviceIP>192.168.66 md>show rgument>access-lis deviceReadOnlyCLIC sm:execDeviceReadO	<pre>https://www.ncounge-one-ary- lyCLICmdsRequest xmlns:cs otVersion&gt; d&gt; .1 t md&gt; nlyCLICmdsRequest&gt;</pre>	m="CSM">	4		
Response						

응답

# 다음을 확인합니다.

응답을 파일로 저장할 수 있습니다.Save **Response > Save to a file로 이동합니다.**그런 다음 파일 위치를 선택하고 .csv 형식으로 저장합니다.

Select path to save file	Postman –	Ø X
③ ③ ⋷ ↑ ■ Desktop • ✓ 爻 Search Desktop:	P 11 My Workspace + 2 Invite 0 Use	crade 💌
Organize • Newfolder		
* Favorites 2.11 KB 2.14 KB	Post la chida ad     Post https://192.168.30.17/nb/con_      Post getGroupLise + •••     No Environment *	
Controp     Contrologic     Recent places     To:     To:	Comments (a) Example	
CSM4.19.05ev/ce_PackLeee Institutionymbere Self-Estractor Researce Software CSM420200129070926764.sip	nto Send • Se	
Downloads fs-csm-419-win-k9.zip	ess Script Tests Settings Cook	
Music     Potman     Petrues     Potwen     V     204 KB     136 KB	D binary @ GraphQL XML *	
File name response.csv		
Save as type: All Files (".")	✓	
Hide Folders     Save     Cancel		
Body Cookies (1) Headers (7) Test Results	Status: 405 Method Not Allowed Time: Time: 1101 State 405.0	
ETY	VALUE Save as example	
Date (0	Thu, 02 Apr 2020 01x8347 GMT Save to a file	
Server (I)	Apache	
Allow @		
Content-Length ()	253	
Keep Aive 🕕	timeout=20, max=10000	
Connection (0)	Keep Alive	
Content-Type ()	text/html; charset=iso-8859-1	
	Activate Windows Go to System in Control Panel to activate Windows	

그런 다음 Excel 응용 프로그램과 함께 이 .csv 파일을 열 수 있어야 합니다..csv 파일 형식에서 출력 을 PDF, TXT 등의 다른 파일 형식으로 저장할 수 있습니다.

### 문제 해결

API를 사용한 가능한 실패 응답

1. 설치된 API 라이센스가 없습니다.

원인:API 라이센스가 만료되었거나, 설치되지 않았거나, 활성화되지 않았습니다.

가능한 솔루션:Tools(툴) > Security Manager Administration(보안 관리자 관리) > Licensing(라이센 싱) 페이지에서 라이센스 만료일 확인

Tools(툴) > Security Manager Administration(보안 관리자 관리) > API 아래에서 API 기능이 활성화 되었는지 확인합니다.

이 가이드의 위에서 CSM API License Installation/Verification 섹션의 설정을 확인합니다.

2. API 로그인에 사용할 CSM IP 주소가 잘못되었습니다.

원인:API 호출의 URL에서 CSM 서버의 IP 주소가 잘못되었습니다.

가능한 솔루션:API 클라이언트의 URL에서 호스트 이름이 CSM 서버의 올바른 IP 주소인지 확인합 니다. URL:https://<hostname>/nbi/login

3. 잘못된 ASA IP 주소.

원인:<deviceIP></deviceIP> 태그 사이의 본문에 정의된 IP 주소는 올바른 주소가 아니어야 합니다.

가능한 솔루션:올바른 디바이스 IP 주소가 Body Syntax에 정의되어 있는지 확인합니다.

4. 방화벽에 연결되지 않습니다.

원인:디바이스가 CSM과 연결되지 않았습니다.

가능한 솔루션:CSM 서버에서 Test Connectivity(연결 테스트)를 실행하고 디바이스에 대한 추가 연 결 문제를 해결합니다.

자세한 오류 코드 및 설명은 다음 <u>링크</u>의 Cisco Security Manager API 사양 가이드에서 자세한 내용 을<u>확인하십시오.</u>