SLUP를 사용하여 & Catalyst 9800 Smart Licensing 문제 해결 구성

목차

소개

이 문서에서는 Catalyst 9800 WLC(Wireless LAN Controller)에서 SLUP(Smart Licensing Using Policy)를 구성하고 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

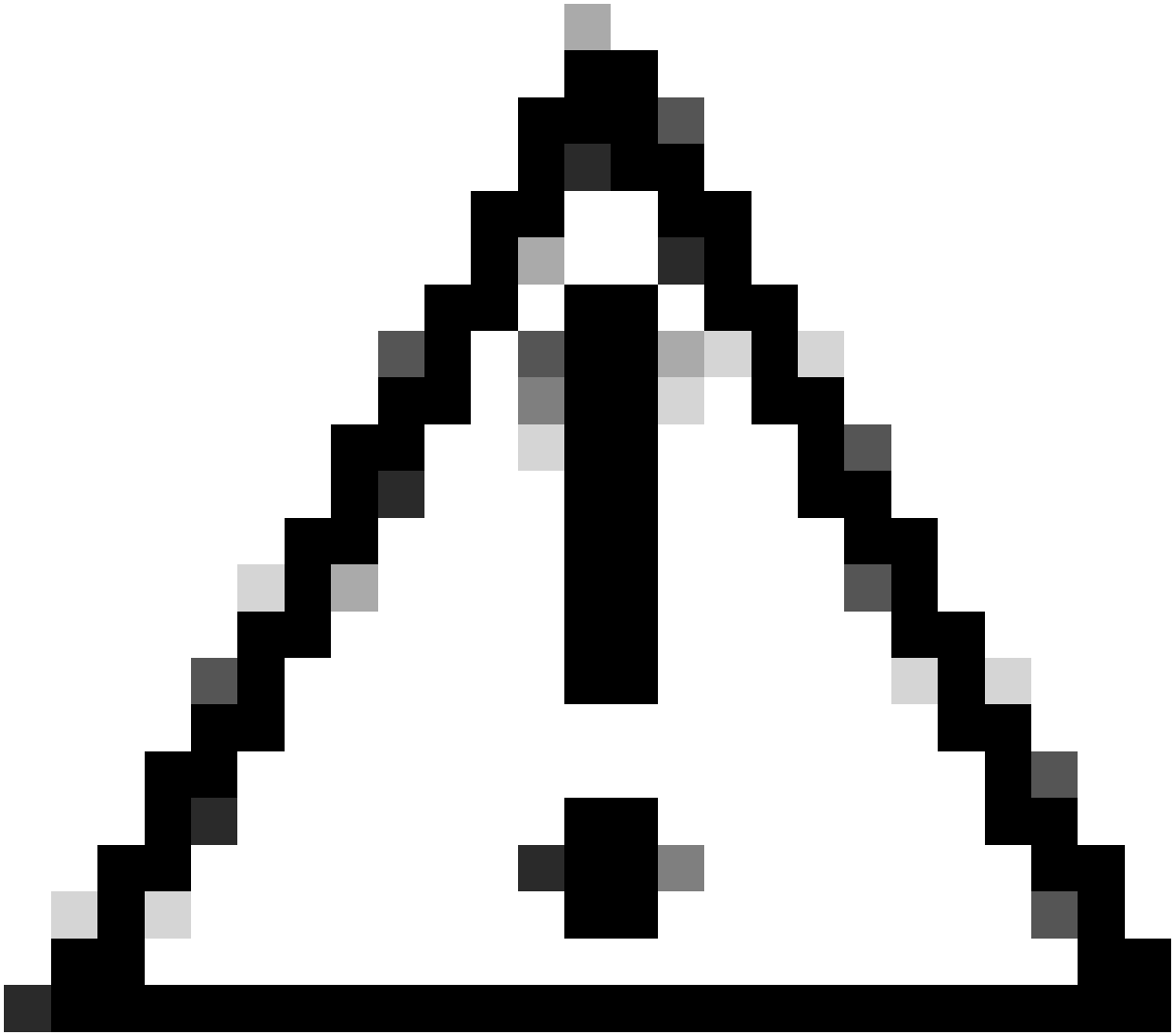
- SLUP(Smart Licensing Using Policy)
- Catalyst 9800 WLC(Wireless LAN Controller)

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

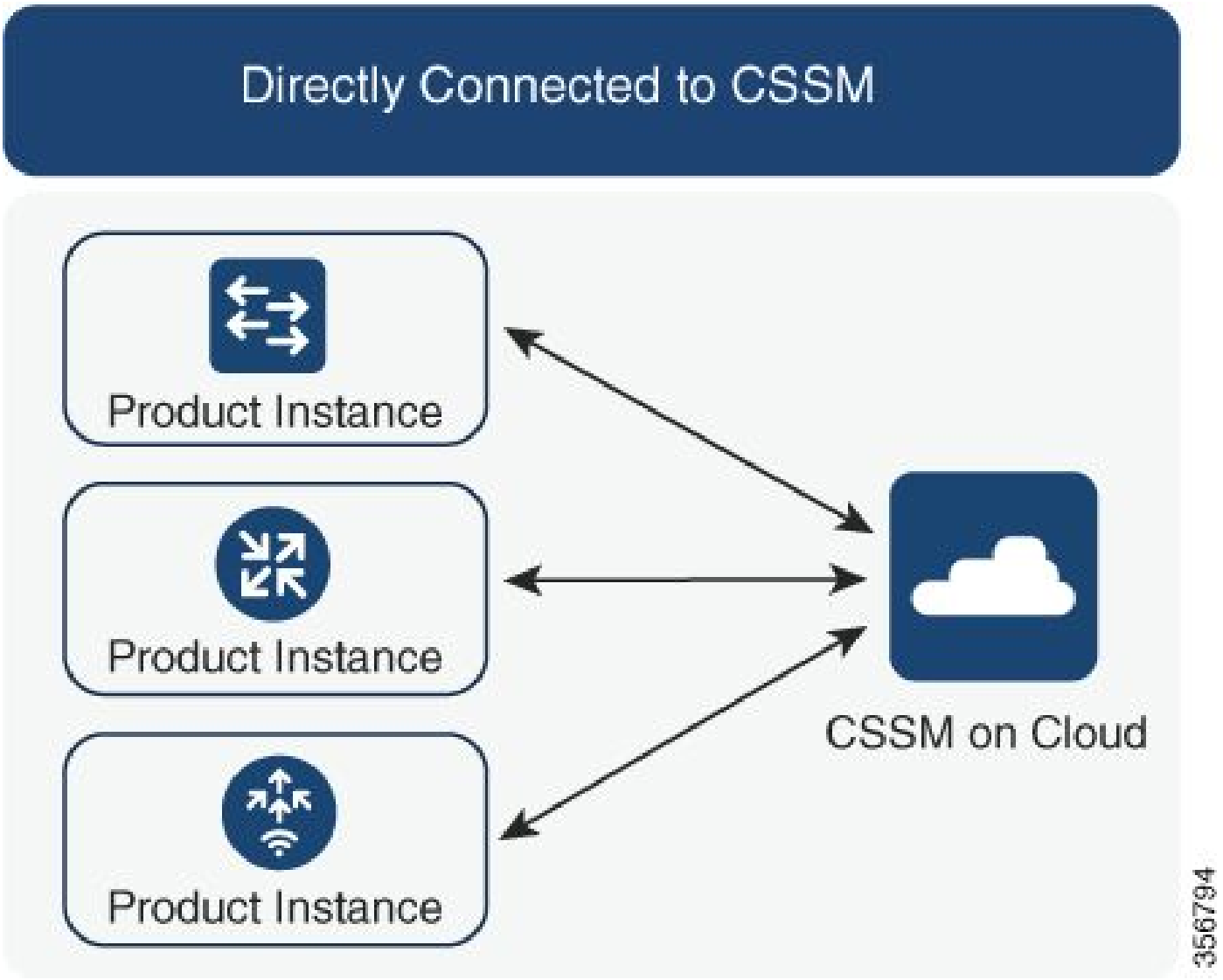
배경 정보



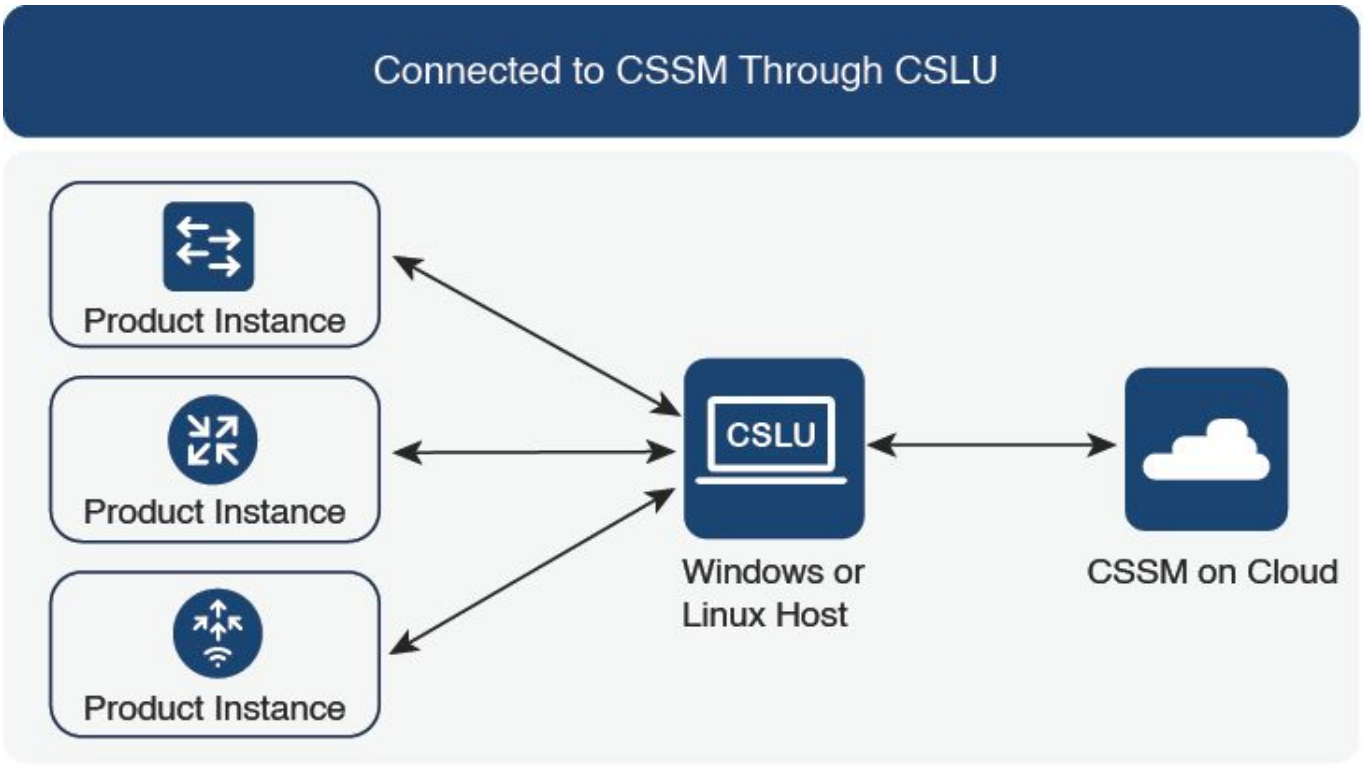
주의: 이 문서의 참고 사항에는 유용한 제안이나 문서에서 다루지 않는 자료에 대한 참조 정보가 포함되어 있습니다. 각 메모를 읽는 것이 좋습니다.

1. Cisco Smart Software Manager Cloud(CSSM 클라우드)에 직접 연결
2. CSLU(Cisco Smart License Utility Manager)를 통해 CSSM에 연결됨
3. 온프레미스 Smart Software Manager(온프레미스 SSM)를 통해 CSSM에 연결됨

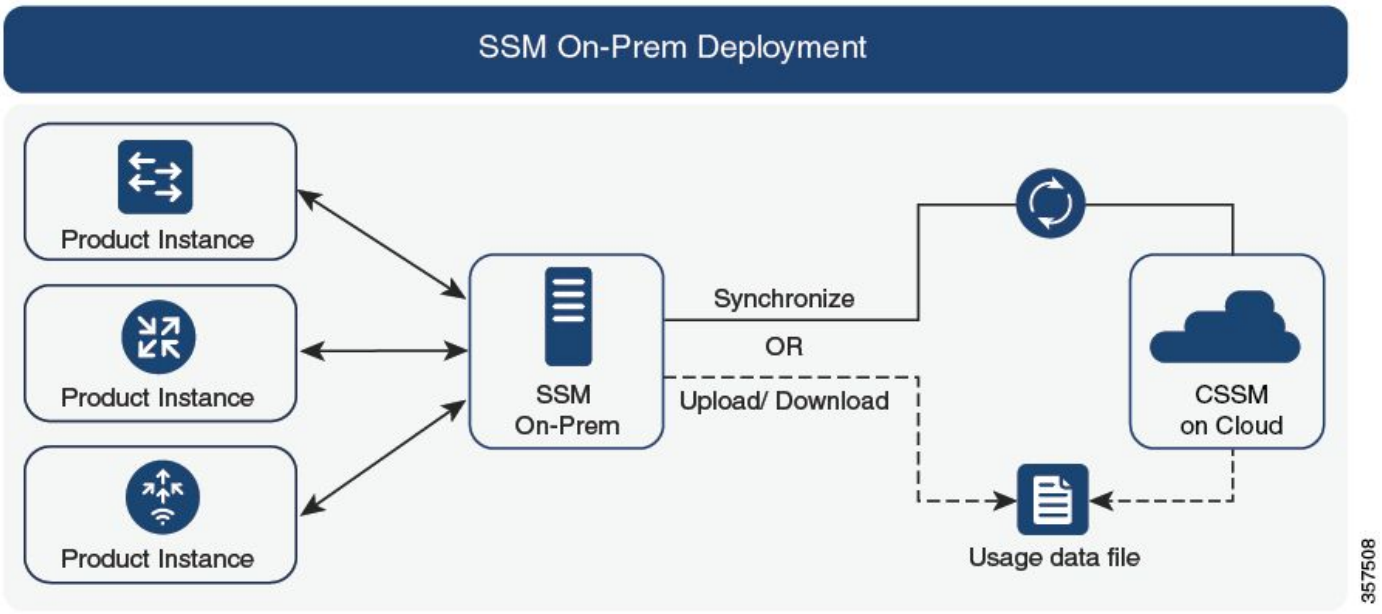
이 문서에서는 Catalyst 9800의 모든 Smart Licensing 시나리오를 다루지 않습니다. 자세한 내용은 Smart Licensing Using Policy Configuration Guide를 참조하십시오. 그러나 이 문서에서는 Catalyst 9800에서 정책 문제를 사용하여 직접 연결, CSLU 및 온프레미스 SSM 스마트 라이센싱을 트러블슈팅하는 데 유용한 일련의 명령을 제공합니다.



옵션 1. CSSM(Cisco Smart Licensing Cloud Servers)에 직접 연결



옵션 2. CSLU를 통한 연결



옵션 3. 온프레미스 Smart Software Manager(온프레미스 SSM)를 통한 연결

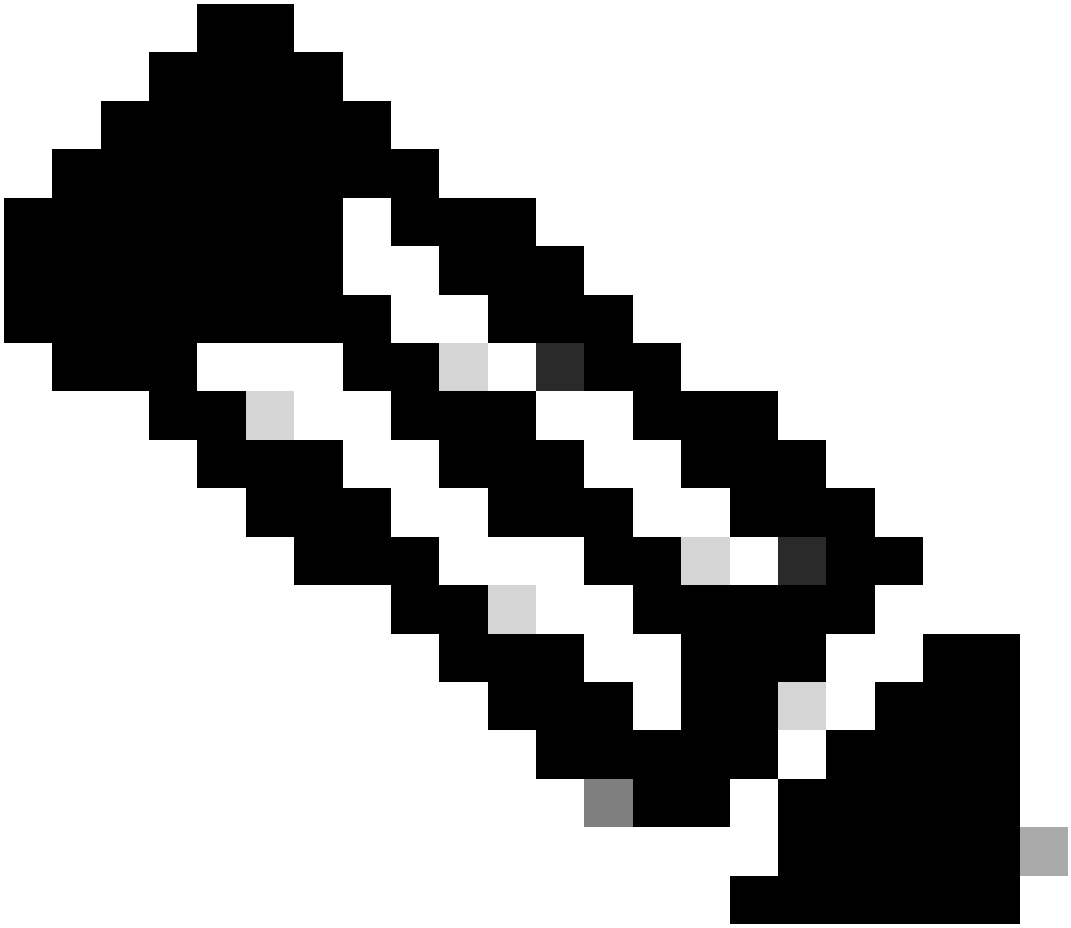
참고: 이 문서에 언급된 모든 명령은 버전 17.3.2 이상을 실행하는 WLC에만 적용됩니다.

기존 라이센싱 vs. SLUP

Catalyst 9800에는 코드 버전 17.3.2와 함께 Smart Licensing Using Policy(정책을 사용하는 스마트 라이센싱) 기능이 도입되었습니다. 초기 17.3.2 릴리스에서는 17.3.3 릴리스와 함께 도입된 WLC webUI의 SLUP 컨피그레이션 메뉴가 누락되었습니다. SLUP는 몇 가지 측면에서 기존의 스마트 라

이센싱과 다릅니다.

- 이제 WLC는 tools.cisco.com 도메인이 아닌 smartreceiver.cisco.com 도메인을 통해 CSSM과 통신합니다.
- 등록 대신 WLC는 이제 CSSM 또는 온프레미스 SSM과의 신뢰를 설정합니다.
- CLI 명령이 약간 변경되었습니다.
- 더 이상 SLR(Smart Licensing Reservation)이 없습니다. 대신 정기적으로 사용량을 수동으로 보고할 수 있습니다.
- 평가 모드가 더 이상 없습니다. WLC는 라이센스가 없더라도 전체 용량에서 계속 작동합니다. 시스템은 명예 기반이며 정기적으로(에어갭이 설치된 네트워크의 경우 자동 또는 수동으로) 라이센스 사용을 보고해야 합니다.



경고: Cisco Catalyst 9800-CL Wireless Controller를 사용하는 경우 Cisco IOS® XE Cupertino 17.7.1부터 시작하는 필수 ACK 요구 사항을 숙지해야 합니다. Cisco Catalyst 9800-CL Wireless Controller에 대한 RUM 보고 및 승인 요구 사항을 참조하십시오.

설정

직접 연결 CSSM

CSSM에서 토큰이 생성된 후 신뢰를 설정하려면 다음 명령을 실행해야 합니다.

참고: 토큰 최대값 HA SSO에서 WLC의 경우 사용 수는 2개 이상이어야 합니다.

```
configure terminal
ip http client source-interface <interface>
ip http client secure-trustpoint <TP>
license smart transport smart
license smart url default
exit
write memory
terminal monitor
license smart trust idtoken <token> all force
```

- ip http client source-interface 명령은 라이센스 관련 패킷을 소싱할 L3 인터페이스를 지정합니다
- ip http client secure-trustpoint 명령은 CSSM 통신에 사용할 신뢰 지점/인증서를 지정합니다. 신뢰 지점 이름은 show crypto pki trustpoints 명령을 사용하여 찾을 수 있습니다. 자체 서명 인증서 TP-self-signed-xxxxxxxxxx 인증서 또는 제조업체 설치 인증서(MIC라고도 함, 9800-40, 9800-80 및 9800-L에서만 사용 가능)를 사용하는 것이 좋으며, 일반적으로 CISCO_IDEVID_SUDI입니다.
- Terminal monitor 명령을 사용하면 WLC에서 로그를 콘솔에 인쇄하고 트러스트가 성공적으로 설정되었는지 확인할 수 있습니다. 모니터가 없는 터미널을 사용하여 비활성화할 수 있습니다.
- 마지막 명령의 all 키워드는 HA SSO 클러스터의 모든 WLC에 CSSM과의 트러스트를 설정하도록 지시합니다.
- 키워드 force는 WLC에 이전에 설정된 트러스트를 재정의하고 새 트러스트를 시도하도록 지시합니다.

참고: 트러스트가 설정되지 않은 경우 9800은 명령이 실행된 후 1분 후에 다시 시도하고 일정 시간 동안 다시 시도하지 않습니다. 토큰 명령을 다시 입력하여 새 트러스트 설정을 적용합니다.

CSLU에 연결됨

CSLU(Cisco Smart License Utility Manager)는 Windows 기반 애플리케이션(Linux에서도 사용 가능)으로, 고객이 Smart Licensed가 활성화된 제품 인스턴스를 Cisco CSSM(Smart Software Manager)에 직접 연결하는 대신 프레미스에서 라이센스 및 관련 제품 인스턴스를 관리할 수 있도록 합니다.

이 섹션에서는 9800 무선 컨피그레이션만 다룹니다. CSLU를 사용하여 라이센싱을 구성하는 다른 단계(예: CSLU 설치, CSLU 소프트웨어 구성 등)도 있습니다. 구성 가이드에서 다룹니다. 제품 인스턴스 시작 또는 CSLU 시작 통신 방법을 구현할지 또는 해당 작업 순서를 완료할지 여부를 지정합니다.

제품 인스턴스 시작됨

1. 컨트롤러에서 CSLU로의 네트워크 연결 보장
2. 전송 유형이 cslu로 설정되어 있는지 확인합니다.

```
(config)#license smart transport cslu
(config)#exit
#copy running-config startup-config
```

3. 컨트롤러에서 CSLU를 검색하려는 경우 작업을 수행해야 합니다. DNS를 사용하여 CSLU를 검색하려는 경우 아무 작업도 필요하지 않습니다. URL을 사용하여 검색하려는 경우 다음 명령을 입력하십시오.

```
(config)#license smart url cslu http://<cslu_ip>:8182/cslu/v1/pi
(config)#exit
#copy running-config startup-config
```

CSLU 개시

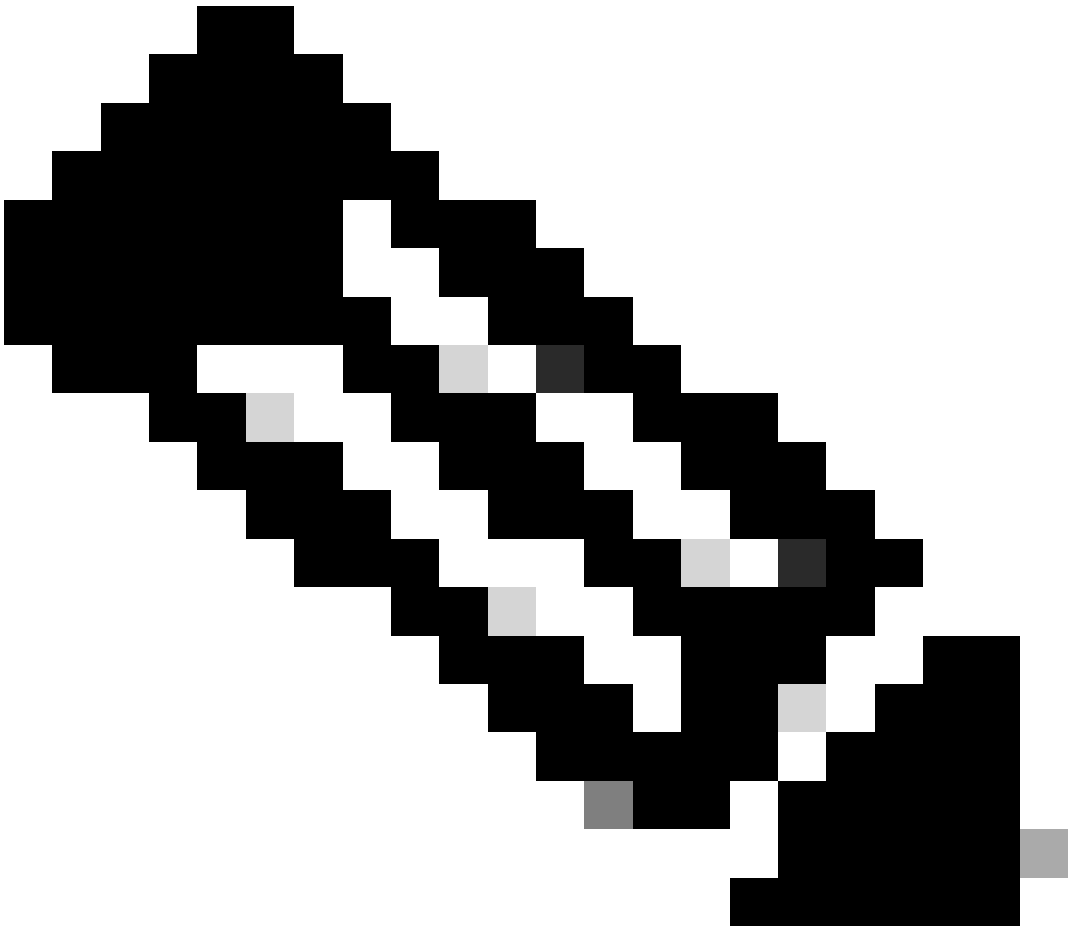
CSLU에서 시작한 통신을 구성할 때 필요한 유일한 작업은 컨트롤러에서 CSLU에 대한 네트워크 연결을 확인하고 확인하는 것입니다.

SSM 온프레미스 연결

온프레미스 SSM을 사용하는 컨피그레이션은 직접 연결과 매우 유사합니다. 온프레미스 버전에서는 8202102 이상 버전을 실행해야 합니다. SLUP 릴리스(17.3.2 이상)의 경우 CSLU URL 및 전송 유형을 사용하는 것이 좋습니다. URL은 **Smart** Licensing(**스마트 라이센싱) > Inventory(인벤토리) > <Virtual Account> > General(일반) 섹션**의 On-prem webUI 인터페이스에서 가져올 수 있습니다.

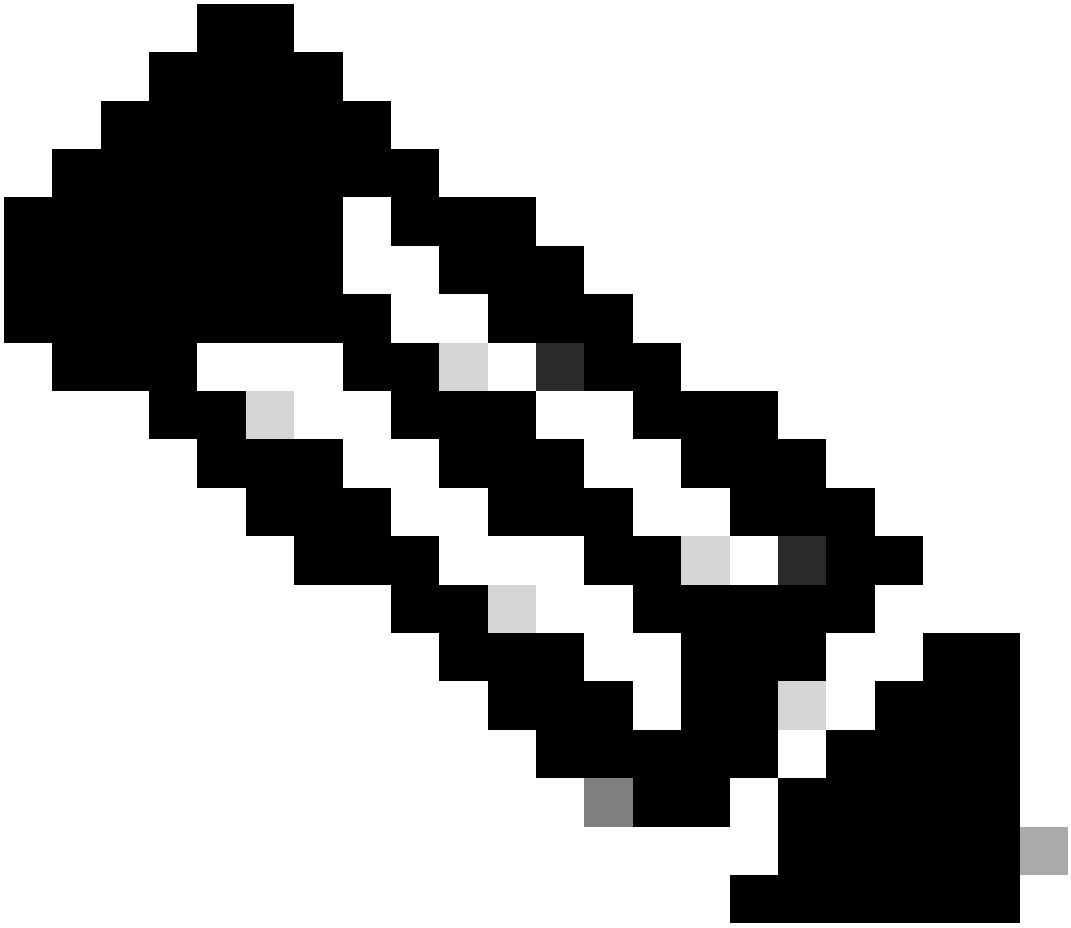
```
configure terminal
 ip http client source-interface <interface>
 ip http client secure-trustpoint <TP>
 license smart transport cslu
 license smart url https://<on-prem-ssm-domain>/SmartTransport
 crypto pki trustpoint SLA-TrustPoint
  revocation-check none
 exit
write memory
terminal monitor
```

온프레미스 SSM에서는 트러스트 토큰을 사용할 필요가 없습니다.



참고: %PKI-3-CRL_FETCH_FAIL: 신뢰 지점 SLA-TrustPoint에 대한 CRL 가져오기에 실패한 경우 SLA-TrustPoint에서 revocation-check none을 구성하지 않았기 때문입니다. 스마트 라이센싱에 사용되는 신뢰 지점입니다. 온프렘의 경우, 라이센싱 서버의 인증서는 CRL 확인이 불가능한 자체 서명 인증서인 경우가 가장 많으므로 폐기 검사를 구성하지 않아야 합니다.

HTTPS 프록시를 통한 스마트 전송 구성



참고: 인증된 프록시는 코드 릴리스 17.9.2부터 아직 지원되지 않습니다. 인프라에서 인증된 프록시를 사용 중인 경우 CSLU(Cisco Smart License Utility Manager)를 사용해 보십시오. 이 서버는 이러한 유형의 서버를 지원합니다.

스마트 전송 모드를 사용할 때 프록시 서버를 사용하여 CSSM과 통신하는 절차는 다음과 같습니다.

```
configure terminal
  ip http client source-interface <interface>
  ip http client secure-trustpoint <TP>
  license smart transport smart
  license smart url default
  license smart proxy address <proxy ip/fqdn>
  license smart proxy port <proxy port>
exit
write memory
terminal monitor
license smart trust idtoken <token> all force
```

통신 주파수

CLI 또는 GUI에서 구성할 수 있는 보고 간격은 적용되지 않습니다.

9800 WLC는 웹 인터페이스 또는 CLI를 통해 어떤 보고 간격을 구성하든 8시간마다 CSSM 또는 온프레미스 Smart Software Manager와 통신합니다. 즉, 새로 가입한 액세스 포인트는 처음 가입한 후 최대 8시간까지 CSSM에 나타날 수 있습니다.

show license air entities summary 명령을 사용하여 다음에 라이센스가 계산되고 보고될 때 이를 파악할 수 있습니다. 이 명령은 일반적인 show tech 또는 show license all 출력에 포함되지 않습니다.

<#root>

WLC#

show license air entities summary

```
Last license report time.....................: 07:38:15.237 UTC Fri Aug 27 2021
Upcoming license report time.................: 15:38:15.972 UTC Fri Aug 27 2021
No. of APs active at last report.............: 3
No. of APs newly added with last report.......: 0
No. of APs deleted with last report...........: 0
```

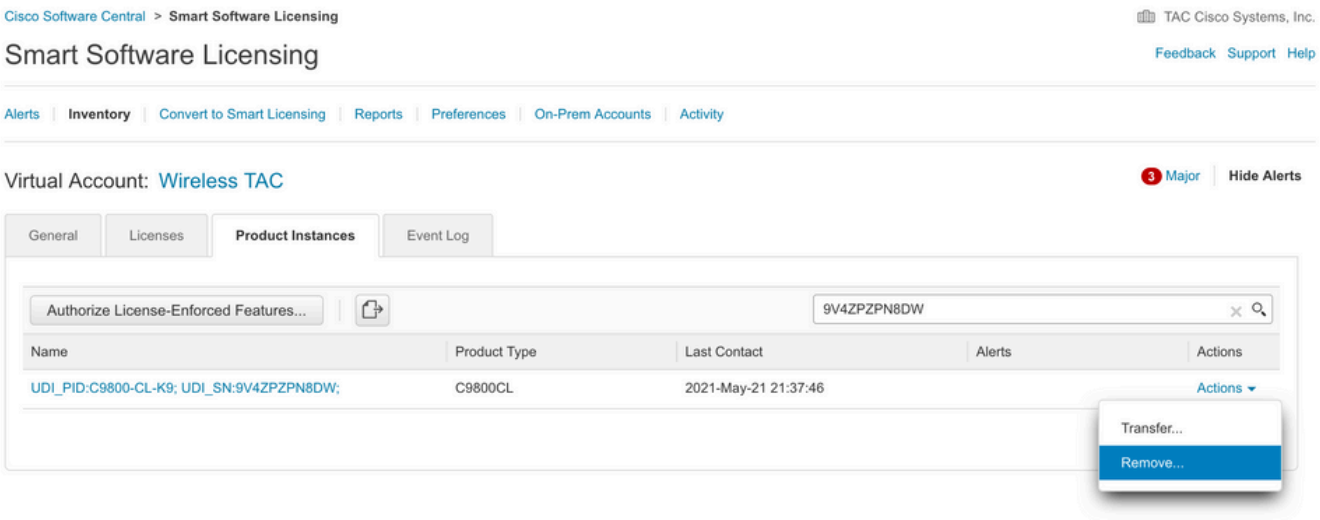
라이센스 공장 재설정

Catalyst 9800 WLC는 모든 라이센싱 컨피그레이션 및 트러스트 공장 재설정을 가질 수 있으며 다른 모든 컨피그레이션을 계속 유지할 수 있습니다. 이 경우 WLC를 다시 로드해야 합니다.

```
WLC-1#license smart factory reset
%Warning: reload required after "license smart factory reset" command
```

RMA 또는 하드웨어 교체 시

9800 WLC를 교체해야 하는 경우, 새 디바이스는 CSSM/On-prem Smart Software Manager에 등록해야 하며 새 디바이스로 인식됩니다. 이전 디바이스의 라이센스 수를 릴리스하려면 Product Instances(제품 인스턴스)에서 수동으로 삭제해야 합니다.



특정 라이센스 등록(SLR)에서 업그레이드

17.3.2 이전의 이전 WLC 릴리스는 SLR(Specific License Registration)이라는 특수한 오프라인 라이센싱 방법을 사용했습니다. 이 라이센싱 방법은 SLUP(17.3.2 이상)를 사용하는 릴리스에서 더 이상 사용되지 않습니다.

SLR을 사용 중이던 9800 컨트롤러를 릴리스 포스트 17.3.2 또는 17.4.1로 업그레이드할 경우 SLR 명령에 의존하지 않고 오프라인 SLUP 보고로 이동하는 것이 좋습니다. 라이센스 사용 RUM 파일을 저장하고 Smart Licensing Portal에 등록합니다. SLR이 더 이상 최신 릴리스에 없으므로 올바른 라이센스 수를 보고하고 사용하지 않는 라이센스를 릴리스합니다. 라이센스는 더 이상 차단되지 않지만 정확한 사용 횟수가 보고됩니다.

문제 해결

인터넷 액세스, 포트 확인 및 Ping

기존 스마트 라이센싱에서 사용했던 tools.cisco.com 대신 새 SLUP는 smartreceiver.cisco.com 도메인을 사용하여 신뢰를 설정합니다. 이 문서를 작성할 때 이 도메인은 여러 개의 서로 다른 IP 주소로 확인됩니다. 이 주소 중 일부만 ping할 수 있습니다. WLC에서 인터넷 연결 가능성 테스트로 PING을 사용하면 안 됩니다. 이러한 서버에 ping을 수행할 수 없다고 해서 제대로 작동하지 않는 것은 아닙니다.

ping 대신 포트 443을 통한 텔넷을 연결성 테스트로 사용해야 합니다. 텔넷은 smartreceiver.cisco.com 도메인에 대해 또는 서버 IP 주소에 대해 직접 확인할 수 있습니다. 트래픽이 차단되고 있지 않으면 포트가 출력에 open으로 표시되어야 합니다.

```
WLC-1#telnet smartreceiver.cisco.com 443
Trying smartreceiver.cisco.com (192.330.220.90, 443)... Open <-------
[Connection to 192.330.220.90 closed by foreign host]
```

Syslog

토큰이 구성되는 동안 terminal monitor 명령이 활성화되면 WLC는 CLI에서 관련 로그를 출력합니다. 이러한 메시지는 show logging 명령을 실행하는 경우에도 확인할 수 있습니다. 성공적으로 설정된 트러스트의 로그는 다음과 같습니다.

```
WLC-1#license smart trust idtoken <token> all force
Aug 22 12:13:08.425: %CRYPTO_ENGINE-5-KEY_DELETED: A key named SLA-KeyPair has been removed from key st
Aug 22 12:13:08.952: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named SLA-KeyPair has been generated or impor
Aug 22 12:13:08.975: %PKI-6-CONFIGAUTOSAVE: Running configuration saved to NVRAM
Aug 22 12:13:11.879: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was successfully in
```

정의된 DNS 서버가 없거나 작동하지 않는 DNS 서버가 있는 WLC 로그:

```
Aug 23 09:19:43.486: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart Software Man
```

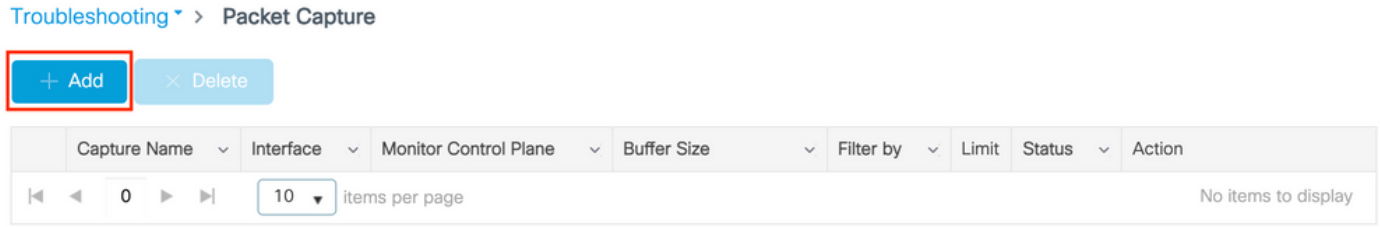
작동 중인 DNS 서버가 있지만 인터넷 액세스가 없는 WLC 로그:

```
Aug 23 09:23:30.701: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart Software Man
```

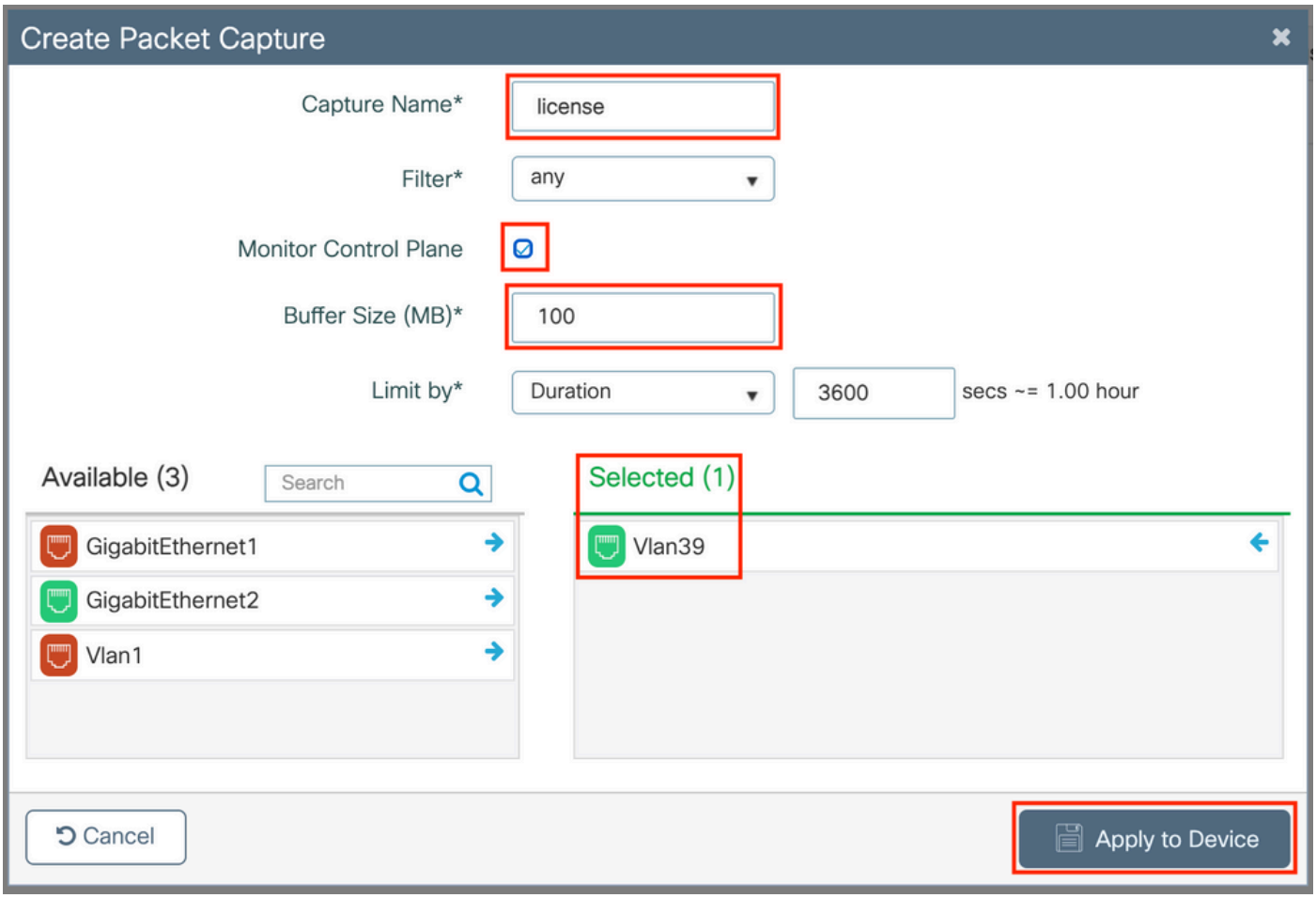
패킷 캡처

WLC와 CSSM/On-prem SSM 간의 통신이 암호화되어 HTTPS를 통해 전송되더라도 패킷 캡처를 수행하면 어떤 이유로 신뢰가 설정되지 않았는지 알 수 있습니다. 패킷 캡처를 수집하는 가장 쉬운 방법은 WLC 웹 인터페이스를 사용하는 것입니다.

Troubleshooting(문제 해결) > Packet Capture(패킷 캡처)로 이동합니다. 새 캡처 지점을 만듭니다.



컨트롤 플레인 모니터링 확인란이 활성화되어 있는지 확인합니다. 버퍼 크기를 최대 100MB로 늘립니다. 캡처해야 하는 인터페이스를 추가합니다. Smart Licensing 트래픽은 기본적으로 무선 관리 인터페이스 또는 ip http client source-interface 명령으로 정의된 인터페이스에서 소싱됩니다.



캡처를 시작하고 license smart trust idtoken <token> all force 명령을 실행합니다.

신뢰 설정의 패킷 캡처에는 다음 단계가 포함되어야 합니다.

1. SYN, SYN-ACK 및 ACK 시퀀스를 사용한 TCP 세션 설정
2. 서버 및 클라이언트 인증서 교환 모두와 TLS 세션 설정. 설정이 새 세션 티켓 패킷으로 끝납니다
3. WLC에서 라이센스 사용량을 보고하는 암호화된 패킷 교환(애플리케이션 데이터 프레임)
4. FIN-PSH-ACK, FIN-ACK & ACK 시퀀스를 통한 TCP 세션 종료

참고: 패킷 캡처에는 TCP 창 업데이트 및 애플리케이션 데이터 프레임의 배수를 포함하여 훨씬 많은 프레임이 포함됩니다

CSSM 클라우드는 3개의 서로 다른 공용 IP 주소를 사용하므로 WLC와 CSSM 간의 모든 패킷 캡처

를 필터링하려면 다음 wireshark 필터를 사용합니다.

```
ip.addr==172.163.15.144 or ip.addr==192.168.220.90 or ip.addr==172.163.15.144
```

온프레미스 SSM을 사용하는 경우 SSM IP 주소를 필터링합니다.

```
ip.addr==<on-prem-ssm-ip>
```

예: 모든 중요 패킷 캡처가 필터링된 직접 연결된 CSSM을 통한 성공적인 신뢰 설정의 패킷 캡처:

No.	Arrival Time	Source	Destination	Protocol	Info
559	Aug 23, 2021 11:31:13.35…	192.168.10.150	192.133.220.90	TCP	22425 → 443 [SYN] Seq=0 Win=4128 Len=0 MSS=536
576	Aug 23, 2021 11:31:13.46…	192.133.220.90	192.168.10.150	TCP	443 → 22425 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1390
578	Aug 23, 2021 11:31:13.46…	192.168.10.150	192.133.220.90	TCP	22425 → 443 [ACK] Seq=1 Ack=1 Win=4128 Len=0
580	Aug 23, 2021 11:31:13.46…	192.168.10.150	192.133.220.90	TLSv1.2	Client Hello
608	Aug 23, 2021 11:31:13.58…	192.133.220.90	192.168.10.150	TLSv1.2	Server Hello
612	Aug 23, 2021 11:31:13.58…	192.168.10.150	192.133.220.90	TCP	[TCP Window Update] 22425 → 443 [ACK] Seq=168 Ack=537 Win=4128 Len=0
614	Aug 23, 2021 11:31:13.58…	192.133.220.90	192.168.10.150	TCP	443 → 22425 [ACK] Seq=537 Ack=168 Win=31953 Len=536 [TCP segment of a reassembled PDU]
673	Aug 23, 2021 11:31:13.70…	192.133.220.90	192.168.10.150	TLSv1.2	Certificate [TCP segment of a reassembled PDU]
675	Aug 23, 2021 11:31:13.70…	192.133.220.90	192.168.10.150	TLSv1.2	Server Key Exchange [TCP segment of a reassembled PDU]
695	Aug 23, 2021 11:31:13.71…	192.133.220.90	192.168.10.150	TLSv1.2	Certificate Request, Server Hello Done
711	Aug 23, 2021 11:31:13.85…	192.168.10.150	192.133.220.90	TLSv1.2	Certificate, Client Key Exchange
718	Aug 23, 2021 11:31:14.01…	192.168.10.150	192.133.220.90	TLSv1.2	Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
737	Aug 23, 2021 11:31:14.13…	192.133.220.90	192.168.10.150	TLSv1.2	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
745	Aug 23, 2021 11:31:14.13…	192.168.10.150	192.133.220.90	TLSv1.2	Application Data
747	Aug 23, 2021 11:31:14.13…	192.168.10.150	192.133.220.90	TLSv1.2	Application Data
749	Aug 23, 2021 11:31:14.13…	192.168.10.150	192.133.220.90	TLSv1.2	Application Data, Application Data
22…	Aug 23, 2021 11:31:45.00…	192.168.10.150	192.133.220.90	TCP	22425 → 443 [FIN, PSH, ACK] Seq=4306 Ack=9738 Win=3625 Len=0
22…	Aug 23, 2021 11:31:45.11…	192.133.220.90	192.168.10.150	TCP	443 → 22425 [FIN, ACK] Seq=9738 Ack=4307 Win=31250 Len=0
22…	Aug 23, 2021 11:31:45.11…	192.168.10.150	192.133.220.90	TCP	22425 → 443 [ACK] Seq=4307 Ack=9739 Win=3625 Len=0

명령 표시

이러한 show 명령에는 신뢰 설정에 대한 유용한 정보가 포함되어 있습니다.

```
show license status
show license summary
show tech-support license
show license tech-support
show license air entities summary

show license history message (useful to see the history and content of messages sent to SL)

show tech wireless (actually gets show log and show run on top of the rest which can be useful)
```

show license history message 명령은 WLC에서 보내고 CSSM에서 다시 받은 실제 메시지를 표시할 수 있으므로 보다 유용한 명령 중 하나입니다.

성공적인 신탁 설정에는 "REQUEST: Aug 23 10:18:08 2021 Central" 및 "RESPONSE: Aug 23 10:18:10 2021 Central" 메시지가 인쇄되어 있습니다. RESPONSE LINE(응답 회선) 뒤에 아무것도 없는 경우 WLC가 CSSM으로부터 응답을 받지 못한 것입니다.

성공적인 트러스트 설정을 위한 show license history 메시지 출력의 예입니다.

```
REQUEST: Aug 23 10:18:08 2021 Central
{"request":"{\"header\":{\"request_type\":\"POLL_REQ\",\"sudi\":{\"udi_pid\":\"C9800-CL-K9\",\"udi_seri
NB\"},\"version\":\"1.3\",\"locale\":\"en_US.UTF-8\",\"signing_cert_serial_number\":\"3\",\"id_cert_ser
\",\"product_instance_identifier\":\"\",\"connect_info\":{\"name\":\"C_agent\",\"version\":\"5.0.9_rel/
e,\"additional_info\":\"\",\"capabilities\":[\"UTILITY\",\"DLC\",\"AppHA\",\"MULTITIER\",\"EXPORT_2\",\
Y_USAGE\"]}},\"request_data\":\"{\\\"sudi\\\":{\\\"udi_pid\\\":\\\"C9800-CL-K9\\\",\\\"udi_serial_numbe
\"},\\\"timestamp\\\":1629713888600,\\\"nonce\\\":\\\"11702702165338740293\\\",\\\"product_instance_ide
\"original_request_type\\\":\\\"LICENSE_USAGE\\\",\\\"original_piid\\\":\\\"2e84a42f-c903-44c5-83b2-e62
":7898262236}\"}","signature":{"type":"SHA256","key":"59152896","value":"eiJ7IuQaTCFxgUkwls76WZxa5DRI5A
OgMqQd5POU6VNsH2j9dHco4T1NJ/aCMbR1MRmkfxyVSWsx4lmjJL1lmpOSi3ZS4FBMvlF/EBOUfowREe2oz2lrQp1cAFpPn5SlaFezW
/Nu6SQZfIW+IdF+2qnJeNFAIZbNpgOB5d5HIJvDmDImvDu3bMRHhQAWr2KKzGFr6jPzOhs7bGY/+FlfTLQk5LFEUaKTNH/tuxJPFHlF
h9//uhsd+NaQyfdRFludkbfUBTFkvPxHW9/5w=="}}

  RESPONSE: Aug 23 10:18:10 2021 Central
{"signature":{"type":"SHA256","value":"TXZE034fqAul2jy9V4+HoB2hDShl9au/5sgodiCVatmu671/6MyN7kZfEzREufY8
SLrjTfO4grGeQTcH7yEjOD+gztWXCOu8RBT7/Bo9aBs\n4x1iOE6flPB3BP6yu7KIEUQZ8yHzlwDT+mVtJGi6TRrtYnV3KQMpCUmF5F
wOksf3SfXreNZJuzWXzjHvtmlusCQXw7ZTBzffYsNKOOlkJlr\nvgB2PkV7JUlsA481kpIvlPul6IiJXqk+2PC2IzCrCLG57lVN3XgX
1pEl2SHyQ/DAw==","piid":null,"cert_sn":null},"response":"{\"header\":{\"version\":\"1.3\",\"locale\":\"
mp\":1629713890172,\"nonce\":null,\"request_type\":\"POLL_REQ\",\"sudi\":{\"udi_pid\":\"C9800-CL-K9\",\
9PJK8D7OCNB\"},\"agent_actions\":null,\"connect_info\":{\"name\":\"SSM\",\"version\":\"1.3\",\"producti
s\":[\"DLC\",\"AppHA\",\"EXPORT_2\",\"POLICY_USAGE\",\"UTILITY\"],\"additional_info\":\"\"},\"signing_c
\",\"id_cert_serial_number\":\"59152896\",\"product_instance_identifier\":\"\"},\"status_code\":\"FAILE
\"Invalid ProductInstanceIdentifier: 2e84a42f-c903-44c5-83b2-e62e258c780f provided in the polling reque
262236\",\"retry_time_seconds\":0,\"response_data\":\"\"}","sch_response":null}
```

디버그/btrace

license smart trust idtoken all force 명령을 사용하여 트러스트 설정을 시도한 후 몇 분 후에 이 명령을 실행합니다. IOSRP 로그는 매우 자세한 정보를 제공합니다. 추가 | smart-licensing 로그만 가져오려면 명령에 smart-agent"를 포함합니다.

```
show logging process iosrp start last 5 minutes
show logging process iosrp start last 5 minutes | include smart-agent
```

또한 이러한 디버그를 실행한 다음 라이센스 명령을 재구성하여 새 연결을 강제할 수 있습니다.

```
debug license events
debug license errors
debug license agent all
```

일반적인 문제

WLC에 인터넷 액세스가 없거나 방화벽이 트래픽을 차단/변경

WLC에 내장된 패킷 캡처를 사용하면 WLC가 CSSM 또는 온프레미스 SSM에서 어떤 것을 다시 수

신하는지 쉽게 확인할 수 있습니다. 응답이 없는 경우 방화벽이 뭔가를 차단하고 있을 가능성이 있습니다.

show license history message 명령은 CSSM 클라우드 또는 온프레미스 SSM에서 응답이 수신되지 않은 경우 요청이 전송된 후 1초 후에 빈 응답을 인쇄합니다.

예를 들어, 이렇게 하면 빈 응답이 수신되었지만 실제로는 응답이 전혀 없다고 생각할 수 있습니다.

```
REQUEST: Jun 29 11:12:39 2021 CET
{"request":"{\"header\":{\"request_type\":\"ID_TOKEN_TRUST\",\"sudi\":{\"udi_pid\":\"C9800-CL-K9\",\"ud
RESPONSE: Jun 29 11:12:40 2021 CET
```

참고: 현재 개선 요청 Cisco 버그 ID CSCvy84684가 있습니다. 이 메시지는 응답이 없을 때 빈 응답을 출력합니다. 이는 show license history message 명령의 출력을 향상시키기 위한 것입니다

패킷 캡처의 알 수 없는 CA 경고

CSSM 또는 온프레미스 SSM과 통신하려면 9800 쪽에 적합한 인증서가 필요합니다. 자체 서명될 수 있지만 유효하지 않거나 만료될 수 없습니다. 이 경우 패킷 캡처는 9800 HTTP 클라이언트 인증서가 만료되었을 때 CSSM이 전송한 알 수 없는 CA에 대한 TLS 알림을 표시합니다.

스마트 라이센싱은 WLC 웹 인터페이스가 사용하는 ip http 서버와 다른 ip http 클라이언트 컨피그레이션을 사용합니다. 즉, 다음 명령을 올바르게 구성해야 합니다.

```
ip http client source-interface <interface>
ip http client secure-trustpoint <TP>
```

신뢰 지점 이름은 show crypto pki trustpoints 명령을 사용하여 찾을 수 있습니다. 일반적으로 CISCO_IDEVID_SUDI라고 하며 9800-80, 9800-40 및 9800-L에서만 사용할 수 있는 자체 서명 인증서 TP-self-signed-xxxxxxxxxxxx 인증서 또는 MIC(Manufacturer Installed Certificate)를 사용하는 것이 좋습니다.

SSL 암호 해독 기능이 있는 방화벽과 같이 TLS 가로채기를 수행하는 디바이스는 C9800이 Cisco Licensing Server와 핸드셰이크를 성공적으로 설정하지 못하도록 할 수 있습니다. 표시되는 HTTPS 인증서가 Cisco Licensing Server 인증서 대신 방화벽 인증서이기 때문입니다.

참고: source-interface 및 secure-trustpoint 명령을 모두 구성해야 합니다. WLC에 L3 인터페이스가 하나뿐인 경우에도 source-interface 명령이 필요합니다.

관련 정보

- 9800에서 Air Gap 모드를 사용하는 Smart Licensing
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.