

Catalyst 9000 스위치의 SLP Smart Transport 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 Catalyst 9000 스위치에서 Smart Transport를 사용하여 SLP(Smart Licensing Using Policy)의 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

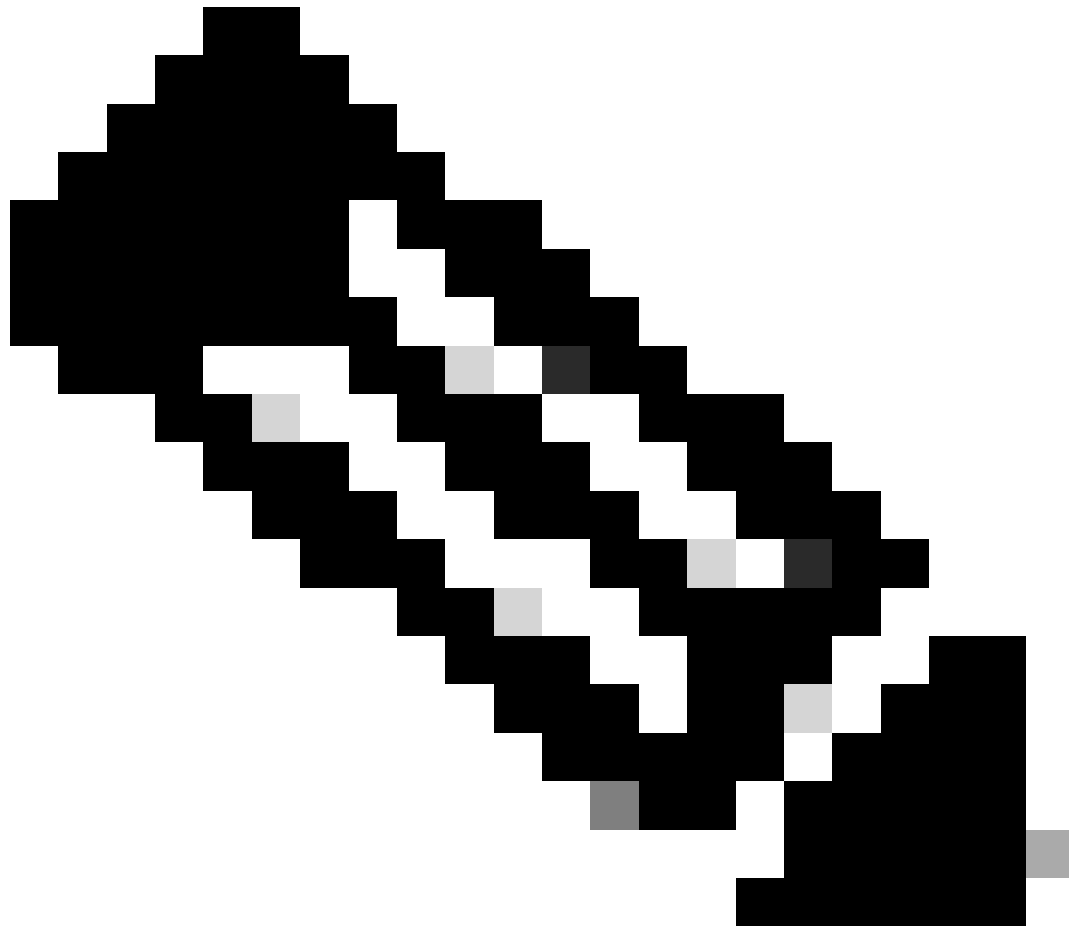
Cisco에서는 이 주제에 대해 잘 알고 숙지할 것을 권장합니다.

- Cisco IOS® XE 디바이스에서 정책을 사용하는 스마트 라이선싱

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Catalyst 9200
- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS XE 17.9.1 이상 버전



참고: 다른 Cisco 플랫폼에서 이러한 기능을 활성화하는 데 사용되는 명령에 대해서는 해당 구성 가이드를 참조하십시오.

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

Smart Licensing Using Policy는 고급 버전의 Smart Licensing으로, 네트워크 운영이 중단되지 않도록 보장하는 라이선싱 솔루션을 제공하는 것을 기본 목표로 설계되었습니다. EMC Centera는 업무 중단을 초래하지 않고 고객이 구매하여 사용하는 하드웨어 및 소프트웨어 라이선스를 관리하기 위한 규정 준수 관계를 구축합니다.

Smart Licensing 보고가 제대로 작동하려면 Catalyst 9000 스위치를 CSSM(Cisco Smart Software Manager)과 연결하여 라이선스 사용량을 보고합니다. CSSM은 모든 Cisco 소프트웨어 라이선스를 관리하고 사용을 검토할 수 있는 중앙 집중식 플랫폼 역할을 하며, 이는 향후 라이선스 요구 사항에

대한 계획을 수립하는 데 도움이 됩니다.

Catalyst 9000 스위치를 CSSM에 연결할 수 있는 토폴로지는 여러 가지가 있지만, 이 문서에서는 스위치가 CSSM에 직접 연결되는 특정 토폴로지에 초점을 맞춥니다. 즉, 스위치가 인터넷에서 호스팅되는 CSSM에 도달하여 연결을 설정할 수 있어야 합니다.

이 직접 연결 토폴로지에는 두 가지 전송 옵션이 있습니다. Smart Transport 및 Call Home이 권장되는 방법입니다. 또한 Smart Transport는 HTTPS 프록시 사용을 지원하며 CSSM과의 Smart Licensing 통신을 처리할 특정 VRF를 선택할 수 있도록 합니다.

Smart Transport를 사용하는 경우 Catalyst 9000 스위치는 HTTPS 메시지 내에서 CSSM과 JSON(JavaScript Object Notation) 형식으로 라이선스 사용 정보를 교환합니다. RUM Report라고 하는 이 정보는 스위치에 의해 전송되며 CSSM의 응답은 ACK라고 합니다.

이 토폴로지의 최소 보고 빈도는 1일로 제한됩니다. 즉, 제품 인스턴스에서 하루에 RUM 보고서를 1개까지만 전송하여 특정 라이선스에 대해 과도한 수의 보고서가 생성 및 전송되지 않도록 합니다. 이렇게 하면 RUM 보고서의 초과 생산으로 인한 메모리 관련 문제 및 시스템 속도 저하를 해결할 수 있습니다.

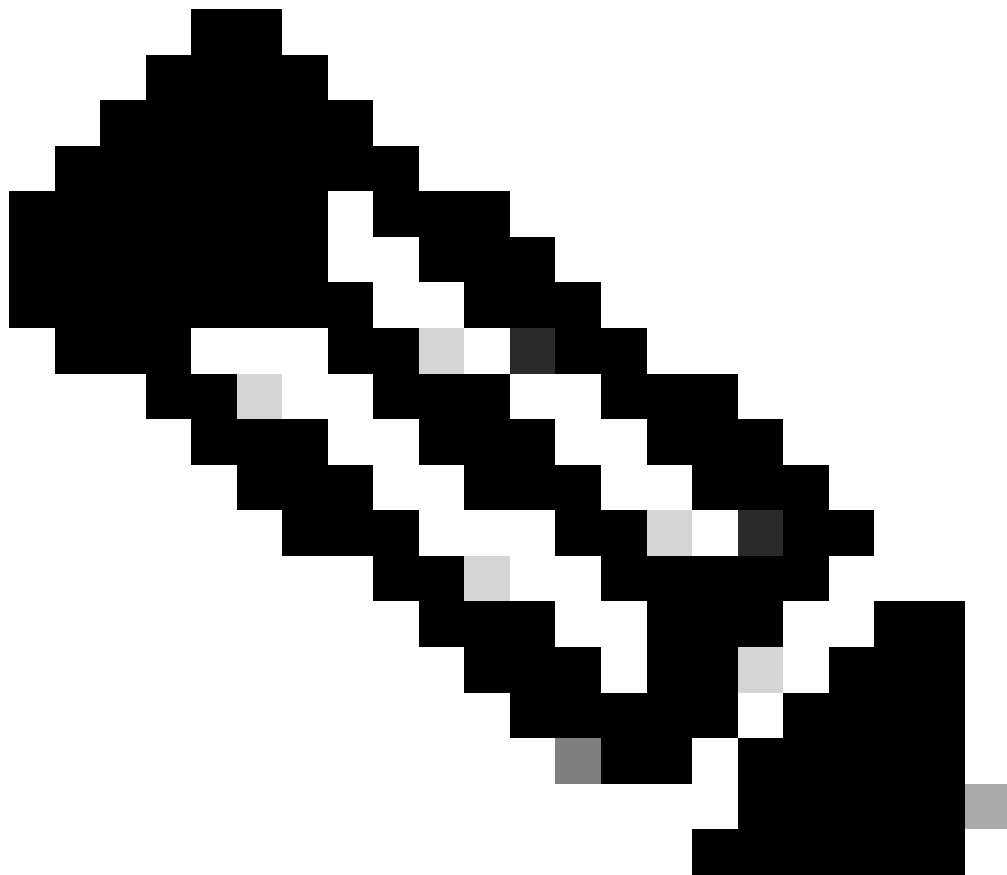
필요한 경우 특권 EXEC 모드에서 명령을 사용하여 이 제한^{license smart sync}제한을 재정의할 수 있습니다

구성

Smart Transport로 SLP를 구성하려면 다음 단계를 수행합니다.

1. 전송 유형으로 Smart를 구성하고 기본 URL을 사용합니다.

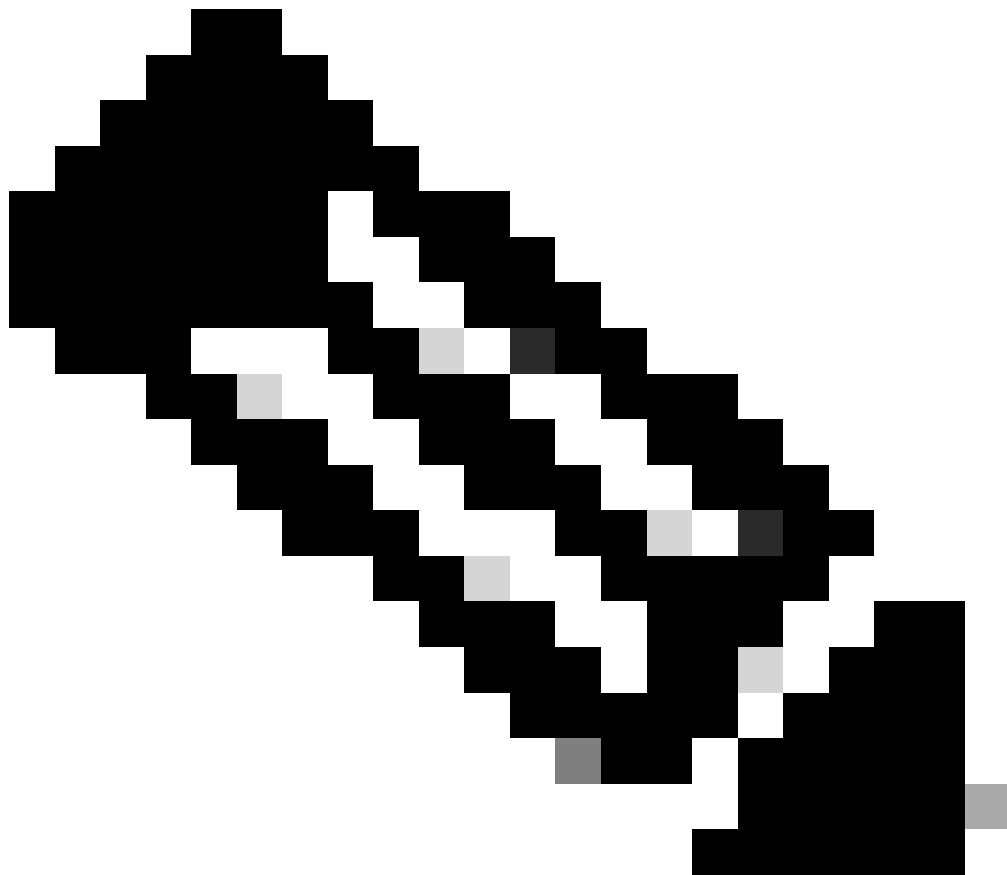
```
Switch#configure terminal
Switch(config)#license smart transport smart
Switch(config)#license smart url default
```



참고: Smart Transport에 VRF가 사용되는 경우 `license smart vrf`
구성해야 합니다.

2. DNS 확인 및 HTTP 클라이언트 연결을 위한 DNS 서버 및 소스 인터페이스를 구성합니다.

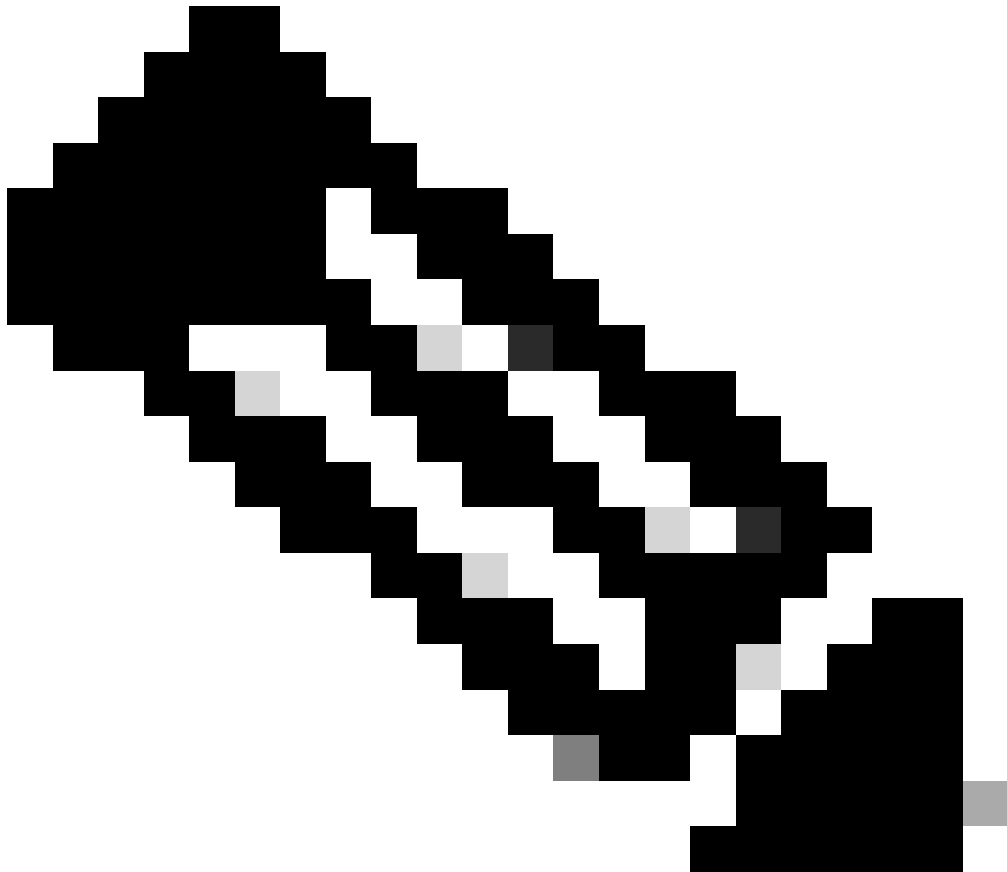
```
Switch(config)#ip domain lookup
Switch(config)#ip name-server 10.31.104.74
Switch(config)#ip domain name cisco.com
Switch(config)#ip domain lookup source-interface Vlan10
```



참고: Smart Transport에 VRF를 사용하는 경우 이러한 명령의 VRF 변형을 사용해야 합니다.

3. 필요한 경우 HTTPS 프록시를 구성합니다.

```
Switch(config)#license smart proxy address 192.168.217.105  
Switch(config)#license smart proxy port 80
```



참고: 프록시 서버는 IP 주소 또는 호스트 이름을 사용하여 구성할 수 있습니다.

4. Virtual Account에서 토큰을 생성합니다. 이 단계를 완료하려면 이 문서에 설명된 프로세스를 [따르십시오](#).

5. 스위치에 신뢰 코드를 설치합니다.

```
Switch#license smart trust idtoken NGFkODgzMGUtZmNkMS00NTRjLWI5MjUtYjI0YWYzZjU1ZGQzLTE3NDAYNjU5%OA  
[OK]
```

CSSM을 사용한 트러스트 설정에 성공하면 이와 유사한 syslog가 표시됩니다.

```
*Jan 24 23:19:05.144: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was successfu
```

또한 `show license status` 신뢰 코드 설치 시간을 표시합니다.

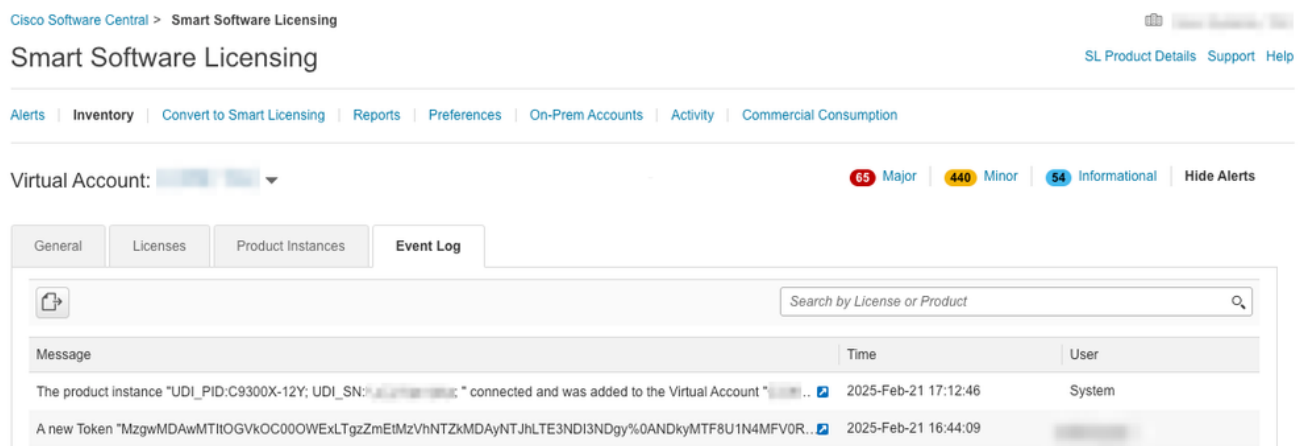
<#root>

Switch#show license status | i Trust

Trust Code Installed: Jan 24 23:19:05 2025 UTC

<--- Trust code was installed

마지막으로, Virtual Account Event Log(가상 어카운트 이벤트 로그)에 스위치가 추가된 것으로 표시됩니다.



The screenshot shows the Cisco Software Central interface for Smart Software Licensing. The top navigation bar includes links for Alerts, Inventory, Convert to Smart Licensing, Reports, Preferences, On-Prem Accounts, Activity, and Commercial Consumption. The main content area displays the 'Event Log' for a specific Virtual Account. The log table contains two entries:

Message	Time	User
The product instance "UDI_PID:C9300X-12Y; UDI_SN:..." connected and was added to the Virtual Account "..."	2025-Feb-21 17:12:46	System
A new Token "MzgwMDAwMTI0GVkOC00OWExLTgzZmEIMzVhNTZkMDAyNTJhLTE3NDI3NDgy%0ANDkyMTF8U1N4MFV0R..."	2025-Feb-21 16:44:09	

디바이스를 표시하는 가상 어카운트 이벤트 로그

문제 해결

CSSM을 사용한 트러스트 설정에 실패할 경우 실패 사유를 나타내는 syslog가 표시됩니다.

*Jan 24 15:17:46.341: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart Software Ma

통신 실패의 가능한 원인은 다음과 같습니다.

- 서버 호스트 이름/도메인 이름을 확인할 수 없습니다. Smart Transport URL 또는 프록시 서버 호스트 이름이 DNS에 의해 확인되지 않았습니다. DNS 서버의 이름 확인 구성 및 연결 가능성을 확인합니다.
- 연결 시간 초과: 연결을 시도했지만 응답이 없습니다. 패킷 캡처를 사용하여 CSSM과의

HTTPS 연결이 설정되었는지 확인하고 프록시 서버 또는 방화벽과 같은 디바이스가 연결을 차단하고 있는지 확인합니다. 프록시 서버를 사용하는 경우 올바른 포트가 사용 중인지 확인하십시오.

Smart Transport로 SLP를 트러블슈팅하려면 다음 단계 및 검증 명령을 수행합니다.

1. Smart Licensing 이벤트를 로그를 확인합니다.

```
<#root>
```

```
Switch#
```

```
show license eventlog 1
```

```
**** Event Log ****
```

```
2025-01-24 13:58:23.900 UTC SAEVT_INIT_START version="5.5.29_rel/114"
2025-01-24 13:58:23.922 UTC SAEVT_INIT_CRYPT0 success="False" error="Crypto Initialization has not
2025-01-24 13:58:23.922 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmRegister"
2025-01-24 13:58:27.620 UTC SAEVT_READY
2025-01-24 13:58:27.621 UTC SAEVT_ENABLED
2025-01-24 13:58:27.665 UTC SAEVT_EXPORT_FLAG exportAllowed="False"
2025-01-24 13:58:27.732 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_SYSDAT
2025-01-24 13:58:27.742 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_SYSDAT
2025-01-24 13:58:27.742 UTC SAEVT_TAG_AUTHORIZED count="1" entitlementTag="regid.2017-05.com.cisco
2025-01-24 13:58:27.744 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_SYSDAT
2025-01-24 13:58:27.744 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_LICENS
2025-01-24 13:58:27.763 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_SYSDAT
2025-01-24 13:58:27.767 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_SYSDAT
2025-01-24 13:58:27.767 UTC SAEVT_TAG_AUTHORIZED count="1" entitlementTag="regid.2017-05.com.cisco
2025-01-24 13:58:27.767 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_SYSDAT
2025-01-24 13:58:27.768 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_LICENS
2025-01-24 13:58:30.425 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmInitialize"
2025-01-24 13:58:30.431 UTC SAEVT_HA_CHASSIS_ROLE udi="PID:C9300-48UN,SN:<SN>"
2025-01-24 13:58:30.431 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmRegister"
2025-01-24 13:58:37.975 UTC SAEVT_HA_ROLE udi="PID:C9300-48UN,SN:<SN>" haRole="Active"
2025-01-24 13:58:38.048 UTC SAEVT_HA_CHASSIS_ROLE udi="PID:C9300-48UN,SN:<SN>" haRole="Active"
2025-01-24 13:58:38.048 UTC SAEVT_HA_ROLE udi="PID:C9300-48UN,SN:<SN>" haRole="Active"
2025-01-24 13:58:38.062 UTC SAEVT_INIT_CONFIG_READ_BEGIN
2025-01-24 13:58:40.884 UTC SAEVT_HOSTNAME_CHANGE
2025-01-24 13:58:41.734 UTC SAEVT_HA_EVENT eventType="SmartAgentSetNVPairs"
2025-01-24 13:58:42.408 UTC SAEVT_INIT_CONFIG_READ_DONE
2025-01-24 13:58:42.531 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_OIR_AD
2025-01-24 13:58:42.531 UTC SAEVT_HA_CONFIG
2025-01-24 13:58:42.531 UTC SAEVT_HA_UDI udi="PID:C9300-48UN,SN:<SN>" haRole="Active"
2025-01-24 13:58:42.732 UTC SAEVT_LICENSE_USAGE count="0" type="destroy" entitlementTag="regid.201
2025-01-24 13:58:42.744 UTC SAEVT_LICENSE_USAGE count="0" type="destroy" entitlementTag="regid.201
2025-01-24 13:58:43.140 UTC SAEVT_INIT_SYSTEM_INIT
2025-01-24 13:58:44.143 UTC SAEVT_INIT_CRYPT0 success="False" error="Crypto Initialization has not
2025-01-24 13:59:14.143 UTC SAEVT_INIT_CRYPT0 success="True"
2025-01-24 13:59:14.144 UTC SAEVT_COMM_RESTORED
2025-01-24 13:59:14.176 UTC SAEVT_INIT_COMPLETE
2025-01-24 14:00:14.145 UTC SAEVT_PRIVACY_CHANGED enabled="True"
2025-01-24 14:00:27.432 UTC
```

```
SAEVT_UTILITY_REPORT_START
```

```
2025-01-24 15:17:46.341 UTC
```

```
SAEVT_COMM_FAIL error="Connection timed out". <--- Connection timed out
2025-01-24 15:35:22.627 UTC SAEVT_COMM_RESTORED <--- Communication with CSSM restored
```

2. Ping을 전송하고 텔넷 연결을 시도하여 CSSM과의 연결을 검증합니다. 이렇게 하면 이름 확인이 수행되며 스위치와 CSSM 간에 관리 블록이 없음을 확인합니다.

```
<#root>
```

```
Switch#
```

```
show ip interface brief | exclude unassigned
```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan10	10.31.121.118				
YES	DHCP	up		up	

```
Switch#
```

```
ping smartreceiver.cisco.com source Vlan10
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to X.X.X.X, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5)
```

```
, round-trip min/avg/max = 364/365/368 ms
```

```
Switch#
```

```
telnet smartreceiver.cisco.com 443 /ipv4 /source-interface vlan10
```

```
Trying X.X.X.X, 80 ...
```

```
Open
```

```
[Connection to X.X.X.X closed by foreign host]
```

또는 프록시 서버를 사용 중인 경우 프록시 서버의 IP 주소 및 포트를 사용하여 동일한 명령을 시도할 수 있습니다.

```
<#root>
```

```
Switch#
```

```
ping 192.168.217.105
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.217.105, timeout is 2 seconds:
```

!!!!

Success rate is 100 percent (5/5)

, round-trip min/avg/max = 364/365/368 ms

Switch#

telnet 192.168.217.105 80 /ipv4 /source-interface vlan10

Trying 192.168.217.105, 80 ...

Open

[Connection to 192.168.217.105 closed by foreign host]

3. RUM 보고서가 전송되고 있으며 응답이 있는지 확인합니다.

<#root>

Switch#

show license history message

Message History (oldest to newest):

=====

Trust Establishment:

REQUEST: Jan 24 23:18:59 2025 UTC <--- RUM report was sent

{"request":{"header":{"request_type":"ID_TOKEN_TRUST","sudi":{"udi_pid":"C9300-48UN",

RESPONSE: Jan 24 23:19:05 2025 UTC <--- Response from CSSM was received

{"signature":{"type":null,"value":null,"piid":null,"cert_sn":null},"response":{"header":{"vers

Usage Reporting:

No past history

Result Polling:

No past history

Authorization Request:

No past history

Authorization Return:

No past history

Trust Sync:

No past history

Import Message History (oldest to newest):

=====

Import POLICY:

No past Import history

Import AUTH:

No past Import history

Import TRUST CODE:
Received on Jan 24 23:19:05 2025 UTC
<TRUST_CODE>

Import RUM ACK:
No past Import history

Import CONVERSION ACK:
No past Import history

Import ACCOUNT INFO:
Last policy received on Jan 24 23:19:05 2025 UTC
<ACCOUNT_INFO>

Switch#

show license tech support | sec Trust

Trust Establishment:
Attempts: Total=1,

Success=1

, Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response: OK on Jan 24 23:19:05 2025 UTC <--- Trust establishment succeeded

Failure Reason:

Last Success Time: Jan 24 23:19:05 2025 UTC

Last Failure Time:

Trust Acknowledgement:

Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response:

Failure Reason:

Last Success Time:

Last Failure Time:

Trust Sync:

Attempts: Total=1,

Success=1,

Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response: OK on Jan 24 23:19:50 2025 UTC

Failure Reason:

Last Success Time: Jan 24 23:19:50 2025 UTC

Last Failure Time:

Trusted Store Interface: True

Local Device: P:C9300-48UN,S:

, state[2], Trust Data INSTALLED TrustId:612
Overall Trust: INSTALLED (2) <--- Trust code installed

요청이 전송되었지만 CSSM에서 응답이 없는 경우 명령에서 `show license history message` 지정된 응답에 대한 JSON 데이터를 표시하지 않으며 오류에 대한 자세한 내용을 확인할 수 있습니다.

```
<#root>
```

```
Switch#
```

```
show license history message
```

```
! <--- Output omitted for brevity --->  
Trust Establishment:
```

```
REQUEST: Feb 21 16:54:49 2025 UTC
```

```
{"request":{"header":{"request_type":"ID_TOKEN_TRUST","sudi":{"udi_pid":"C9300X-12Y",
```

```
RESPONSE: Feb 21 16:54:49 2025 UTC
```

```
<--- The line is empty, which means there was no response from CSSM
```

```
REQUEST: Feb 21 16:55:19 2025 UTC
```

```
{"request":{"header":{"request_type":"ID_TOKEN_TRUST","sudi":{"udi_pid":"C9300X-12Y",  
! <--- Output omitted for brevity --->
```

```
Switch#
```

```
show license tech support | sec Trust
```

```
Trust Establishment:  
Attempts: Total=2, Success=0,
```

```
Fail=2
```

```
Ongoing Failure: Overall=2 Communication=2
```

```
Last Response: NO REPLY on Feb 21 16:55:39 2025 UTC
```

```
<--- Failure reason was NO REPLY
```

```
Failure Reason: <none>  
Last Success Time: <none>  
Last Failure Time: Feb 21 16:55:39 2025 UTC  
Trust Acknowledgement:  
Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0  
Last Response: <none>
```

```
Failure Reason: <none>
Last Success Time: <none>
Last Failure Time: <none>
Trust Sync:
Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
Last Response: <none>
Failure Reason: <none>
Last Success Time: <none>
Last Failure Time: <none>
Trusted Store Interface: True
Local Device: P:C9300-48UN,S:<SN>, state[1],
```

NOT INSTALLED

TrustId:605

<--- Trust point exists but it is not installed yet

Overall Trust: No ID

4. CSSM과 동기화하도록 RUM 보고서를 전송하도록 스위치를 트리거합니다.

```
<#root>
```

```
Switch#
```

```
show clock
```

```
*23:38:54.683 UTC Fri Jan 24 2025
```

```
Switch#
```

```
show license tech support | i Utility
```

```
Utility:
```

```
Start Utility Measurements: Jan 24 23:35:55 2025 UTC (4 minutes, 38 seconds remaining)
```

```
Send Utility RUM reports: Feb 23 23:20:56 2025 UTC (29 days, 23 hours, 49 minutes, 39 seconds remaining)
```

```
Process Utility RUM reports: Jan 25 23:30:58 2025 UTC (23 hours, 59 minutes, 41 seconds remaining)
```

```
Switch#
```

```
show license history message | i REQUEST
```

```
REQUEST: Jan 24 23:18:59 2025 UTC
```

```
REQUEST: Jan 24 23:20:50 2025 UTC
```

```
REQUEST: Jan 24 23:25:55 2025 UTC
```

```
REQUEST: Jan 24 23:19:41 2025 UTC
```

```
Switch#
```

```
license smart sync all <--- Trigger synchronization
```

```
Switch#
```

```
show license history message | i REQUEST
```

REQUEST: Jan 24 23:18:59 2025 UTC
REQUEST: Jan 24 23:20:50 2025 UTC
REQUEST: Jan 24 23:25:55 2025 UTC
REQUEST: Jan 24 23:19:41 2025 UTC

REQUEST: Jan 24 23:39:05 2025 UTC

<--- New RUM report was sent

Switch#

show license tech support | sec Trust

Trust Establishment:

Attempts: Total=1, Success=1, Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response: OK on Jan 24 23:19:05 2025 UTC

Failure Reason:

Last Success Time: Jan 24 23:19:05 2025 UTC

Last Failure Time:

Trust Acknowledgement:

Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response:

Failure Reason:

Last Success Time:

Last Failure Time:

Trust Sync:

Attempts:

Total=2, Success=2

, Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response: OK on Jan 24 23:39:14 2025 UTC <--- Successful response from CSSM

Failure Reason:

Last Success Time: Jan 24 23:39:14 2025 UTC

Last Failure Time:

Trusted Store Interface: True

Local Device: P:C9300-48UN,S:<SN>, state[2], Trust Data INSTALLED TrustId:612

Overall Trust: INSTALLED (2)

5. 스위치가 CSSM과의 HTTPS 연결을 설정하는지 검증하려면 패킷 캡처를 수행할 수 있습니다
. 프록시 서버를 사용한 성공적인 연결의 패킷 캡처 예입니다.

<#root>

Switch#

sh ip cef 10.31.104.78

0.0.0.0/0

nexthop 10.31.121.65 Vlan10

Switch#

sh ip arp 10.31.121.65

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	10.31.121.65	0			

2c31.24b1.6bc6

ARPA Vlan10

Switch#

show mac address-table address 2c31.24b1.6bc6

Mac Address Table			
Vlan	Mac Address	Type	Ports
10	2c31.24b1.6bc6	DYNAMIC	

Fi1/0/48

Total Mac Addresses for this criterion: 1

Switch#

monitor capture CSSM interface Fi1/0/48 both match any

Switch#

monitor capture CSSM start

Started capture point : CSSM

Switch#

show clock

*

15:41:10.058 UTC

Fri Jan 24 2025

Switch#

license smart sync all

Switch#sh license hist mess | i REQUEST
REQUEST: Jan 24 15:35:17 2025 UTC

REQUEST: Jan 24 15:41:58 2025 UTC

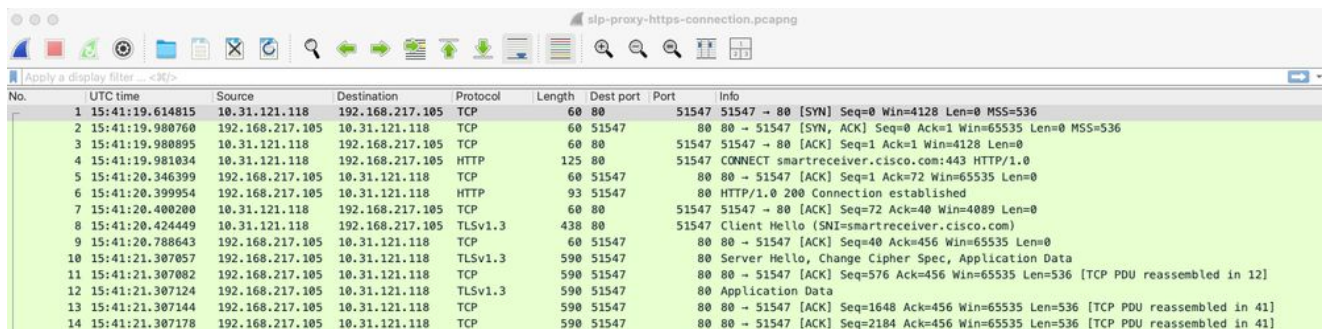
Switch#

monitor capture CSSM stop

Switch#

monitor capture CSSM export location flash:slp-proxy-https-connection.pcap

Export Started Successfully



No.	UTC time	Source	Destination	Protocol	Length	Dest port	Port	Info
1	15:41:19.614815	10.31.121.118	192.168.217.105	TCP	60	80	51547	51547 → 80 [SYN] Seq=0 Win=4128 Len=0 MSS=536
2	15:41:19.980760	192.168.217.105	10.31.121.118	TCP	60	51547	80	80 → 51547 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=536
3	15:41:19.980895	10.31.121.118	192.168.217.105	TCP	60	80	51547	51547 → 80 [ACK] Seq=1 Ack=1 Win=4128 Len=0
4	15:41:19.981034	10.31.121.118	192.168.217.105	HTTP	125	80	51547	CONNECT smartreceiver.cisco.com:443 HTTP/1.0
5	15:41:20.346399	192.168.217.105	10.31.121.118	TCP	60	51547	80	80 → 51547 [ACK] Seq=1 Ack=72 Win=65535 Len=0
6	15:41:20.399954	192.168.217.105	10.31.121.118	HTTP	93	51547	80	HTTP/1.0 200 Connection established
7	15:41:20.400200	10.31.121.118	192.168.217.105	TCP	60	80	51547	51547 → 80 [ACK] Seq=72 Ack=40 Win=4089 Len=0
8	15:41:20.424449	10.31.121.118	192.168.217.105	TLSv1.3	438	80	51547	Client Hello (SNI=smartreceiver.cisco.com)
9	15:41:20.788643	192.168.217.105	10.31.121.118	TCP	60	51547	80	80 → 51547 [ACK] Seq=40 Ack=456 Win=65535 Len=0
10	15:41:21.307857	192.168.217.105	10.31.121.118	TLSv1.3	590	51547	80	Server Hello, Change Cipher Spec, Application Data
11	15:41:21.307882	192.168.217.105	10.31.121.118	TCP	590	51547	80	80 → 51547 [ACK] Seq=576 Ack=456 Win=65535 Len=536 [TCP PDU reassembled in 12]
12	15:41:21.307124	192.168.217.105	10.31.121.118	TLSv1.3	590	51547	80	Application Data
13	15:41:21.307144	192.168.217.105	10.31.121.118	TCP	590	51547	80	80 → 51547 [ACK] Seq=1648 Ack=456 Win=65535 Len=536 [TCP PDU reassembled in 41]
14	15:41:21.307178	192.168.217.105	10.31.121.118	TCP	590	51547	80	80 → 51547 [ACK] Seq=2184 Ack=456 Win=65535 Len=536 [TCP PDU reassembled in 41]

프록시 서버를 사용하여 CSSM과의 성공적인 HTTPS 연결의 패킷 캡처입니다.

- 패킷 캡처에서 HTTPS 연결을 설정하려고 시도했지만 실패하는 것으로 표시되는 경우, TLS 또는 SSL 핸드셰이크 실패 때문일 수 있습니다. 이러한 디버그는 추가 조사에 사용할 수 있습니다.

```
debug ip http client all
debug ssl openssl states
debug ssl openssl errors
debug crypto pki messages
debug crypto pki transactions
```

- 설치된 신뢰 코드를 스위치에서 제거해야 하는 경우, Smart Licensing 공장 재설정을 수행할 수 있습니다. 이 프로세스에는 다시 로드가 필요합니다. 공장 초기화 후 새 신뢰 코드를 설치할 수 있습니다. 이 명령을 사용하면 정책을 비롯한 모든 라이선스 정보가 제거됩니다.

```
<#root>
```

```
Switch#
```

```
license smart factory reset
```

```
%Warning: reload required after "license smart factory reset" command
```

```
Switch#
```

```
show license status | include Trust
```

```
Trust Code Installed:
```

```
<--- Installed trust code now shows none
```

Switch#

reload

관련 정보

- [Cisco Catalyst 9000 Series 스위치용 정책을 사용하는 스마트 라이선싱](#)
- [Catalyst 스위칭을 위한 스마트 라이선싱 이해](#)
- [Cisco Live: 정책을 사용한 Smart Licensing 소개](#)
- [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.