

Catalyst 스위칭을 위한 스마트 라이선싱 이해

목차

[소개](#)

[목적](#)

[정책을 사용하는 스마트 라이선싱](#)

[용어](#)

[변화가 필요한 이유](#)

[사용 가능한 라이선스](#)

[Base 라이선스](#)

[애드온 라이선스](#)

[새로운 구성 요소](#)

[정책](#)

[RUM 보고서](#)

[그린필드\(Greenfield\) 구축 사례의 제조 흐름](#)

[CSLU](#)

[SLP - 직접 연결](#)

[라이선스 보고](#)

[Direct Connect - Smart Transport](#)

[직접 연결 - Call-Home 전송](#)

[SLP - CSLU](#)

[CSLU 설치 및 컨피그레이션](#)

[푸시 모드를 사용하는 CSLU](#)

[CSLU 자동 검색](#)

[끌어오기 모드를 사용하는 CSLU](#)

[RESTAPI를 사용하는 풀 모드](#)

[CSLU - 설정 절차](#)

[RESTCONF를 사용하는 풀 모드](#)

[CSLU - 설정 절차](#)

[NETCONF를 사용하는 풀 모드](#)

[CSLU - 설정 절차](#)

[연결 끊김 모드를 사용하는 CSLU](#)

[SLP - 오프라인 모드](#)

[동작 변경](#)

[문제 해결](#)

[일반적인 문제 해결 질문](#)

[디버그 PI](#)

[CSLU 디버그](#)

[관련 참조](#)

소개

이 문서에서는 Catalyst 스위칭 플랫폼에서 정책을 사용하는 스마트 라이선싱 기능과 지원되는 구축에 대해 설명합니다.

목적

버전 17.3.2 및 17.4.1부터 Cisco IOS® XE까지 Cat9k 제품군의 모든 Catalyst 스위칭 플랫폼은 SLP(Smart Licensing using Policy)의 새로운 라이선싱 모델을 지원합니다. 이 문서의 목적은 주로 Greenfield 구축을 위한 SLP의 구현 및 구축에 대해 지원되는 여러 모델을 이해하는 것입니다.

정책을 사용하는 스마트 라이선싱

SLP를 사용하면 디바이스에서 즉시 사용 가능한 모든 라이선스가 있습니다. 이전 개념인 평가 모드, 등록 및 예약은 SLP와 함께 사라집니다. SLP에서는 라이선스 및 라이선스 사용량을 보고하는 것이 관건입니다. 라이선스는 여전히 시행되지 않으며 라이선스 수준은 그대로 유지됩니다. Catalyst 스위치 플랫폼의 경우 HSECK9 라이선스 외에 수출 통제 라이선스 레벨은 없습니다. 유일한 변경 사항은 라이선스 사용 보고 및 추적입니다. 이 섹션에서는 용어, 변경 이유, SLP와 함께 제공되는 새로운 구성 요소, CSLU(Cisco Smart Licensing Utility) 및 제품 주문 흐름에 대해 자세히 설명합니다.

용어

- CSSM 또는 SSM - Cisco 스마트 소프트웨어 관리자
- SA - Smart Account
- VA - 가상 어카운트
- SL - Smart Licensing
- PLR - 영구 라이선스 예약
- SLR - Smart License 예약
- PID - 제품 ID
- SCH - Smart Call Home
- PI - 제품 인스턴스
- CSLU - Cisco Smart Licensing 유틸리티
- RUM - 리소스 사용률 측정
- ACK - 승인
- UDI - 고유 장치 식별 - PID + SN
- SLP - 정책을 사용하는 스마트 라이선싱

변화가 필요한 이유

의 Smart Licensing 모델이 도입됨에 따라 Cisco는 trust and verify 다양한 구축 메커니즘을 지원하여 라이선스 사용량을 추적하고 CSSM에 보고합니다. 하지만 모든 종류의 구축에 쉽게 적용할 수 있는 것은 아니었습니다. 현장의 피드백과 요구 사항이 있어 Smart Licensing을 도입하기에 유리했습니다. 몇 가지 과제는 다음과 같습니다.

- SL 등록을 사용하는 경우 - 구축의 문제가 되는 CSSM에 연결하기 위해 장치가 항상 인터넷에 연결되어 있어야 합니다.
- 온프레미스 Satellite 서버는 구축 및 유지 관리 비용이 더 많이 듭니다.

- SLR은 에어 갭(air-gapped) 네트워크만 지원합니다.
- 이러한 모델 중 하나를 지원하지 않는 구축에서는 라이선스를 구매한 후에도 Unregistered/Eval expired 해당 상태에서 디바이스를 실행해야 합니다.

SLP는 현장의 다양한 요청을 용이하게 처리하기 위해 도입되었습니다. SLP에서는 CSSM에 제품을 등록할 필요가 없습니다. 구매한 모든 라이선스 레벨은 즉시 '사용 중'입니다. 이렇게 하면 디바이스에 있던 day-0 마찰이 제거됩니다. 또한 SLP는 라이선스 프로비저닝의 워크플로를 최소화하고 초과 접점을 줄입니다. 장치가 24시간 내내 CSSM에 연결될 필요는 없습니다. 또한 SLP는 연결이 끊긴 네트워크에서 라이선스를 사용하고, 라이선스 사용량을 오프라인으로 보고하고, 고객 정책에 따라 결정된 간격으로 라이선스를 보고할 수 있는 기능도 제공합니다.

사용 가능한 라이선스

사용 가능한 소프트웨어 기능은 기본 또는 애드온 라이선스 레벨에 해당합니다. 기본 라이선스는 영구 라이선스이며 추가 라이선스는 3년, 5년, 7년 단위로 사용할 수 있습니다.

Base 라이선스

- 네트워크 필수 요소
- 네트워크 이점
- HSECK9

애드온 라이선스

- DNA 필수 요소
- DNA의 장점

참고: HSECK9는 수출 통제 라이선스입니다. 라이선스 및 해당 기능을 활성화하려면 SLAC가 필요합니다.

새로운 구성 요소

정책

정책은 PI의 기본 동작을 결정합니다. 다양한 라이선스 레벨 및 조건에 대한 라이선싱 보고 요구 사항 특성을 알려줍니다. 또한 정책은 CSSM으로 전송되는 모든 보고서에 대해 ACK 메시지를 PI로 다시 전송해야 하는지 여부를 결정합니다. 정책에는 정책의 이름 및 정책 설치 시기도 포함됩니다. Cisco의 기본 정책은 모든 Catalyst 제품에 공통적으로 적용됩니다. 그러나 보고 간격과 ACK 응답 생략을 다르게 하고자 하는 경우에도 고객 정의 정책이 허용됩니다.

정책은 다양한 경우에 PI에 설치할 수 있습니다.

- 소프트웨어에 있는 기본 정책
- Cisco Manufacturing에서 설치한 정책
- ACK 응답을 통해 설치되는 정책
- CLI를 통해 수동으로 설치되는 정책
- Yang 요청을 사용하여 푸시된 정책

이 출력은 기본 정책의 모양을 보여줍니다.

Policy:

Policy in use: Merged from multiple sources.
Reporting ACK required: yes (CISCO default)
Unenforced/Non-Export Perpetual Attributes:
First report requirement (days): 365 (CISCO default)
Reporting frequency (days): 0 (CISCO default)
Report on change (days): 90 (CISCO default)
Unenforced/Non-Export Subscription Attributes:
First report requirement (days): 90 (CISCO default)
Reporting frequency (days): 90 (CISCO default)
Report on change (days): 90 (CISCO default)
Enforced (Perpetual/Subscription) License Attributes:
First report requirement (days): 0 (CISCO default)
Reporting frequency (days): 0 (CISCO default)
Report on change (days): 0 (CISCO default)
Export (Perpetual/Subscription) License Attributes:
First report requirement (days): 0 (CISCO default)
Reporting frequency (days): 0 (CISCO default)
Report on change (days): 0 (CISCO default)

 **참고:** 시스템 컨피그레이션을 삭제/수정하거나 nvram을 지우거나 플래시를 포맷하면 정책을 지울 수 없습니다filesystem. 정책은 라이선스 **smart factory** 재설정에서 Cisco default로 **설정됩니다**.

RUM 보고서

RUM은 PI에 의해 생성되고 저장되는 사용 보고서입니다. SLP에 대한 ISO19770-4 표준 RUM 보고서가 완료됩니다. RUM 보고서는 PI에서 수행된 라이선스 사용에 대한 모든 변경 사항을 보고서 파일로 저장합니다. 각 라이선스 레벨의 사용 데이터는 별도의 RUM 보고서에 저장됩니다. RUM 보고서 측정치는 일정한 간격으로 PI에 수집되어 저장됩니다. PI의 라이선스 사용이 변경되거나 사용 보고가 트리거될 때마다 또는 보고서가 최대 크기/샘플에 도달하면 모든 라이선스 레벨에 대한 새 RUM 보고서가 생성됩니다. 다른 경우에, 존재하는 RUM 리포트는 새로운 샘플 및 업데이트된 타임스탬프로 덮어쓰여질 수 있다. 기본 RUM 보고서 유틸리티 측정은

15분마다 수행됩니다. 보고 간격마다 RUM 보고서가 Cisco CSSM으로 전송됩니다.

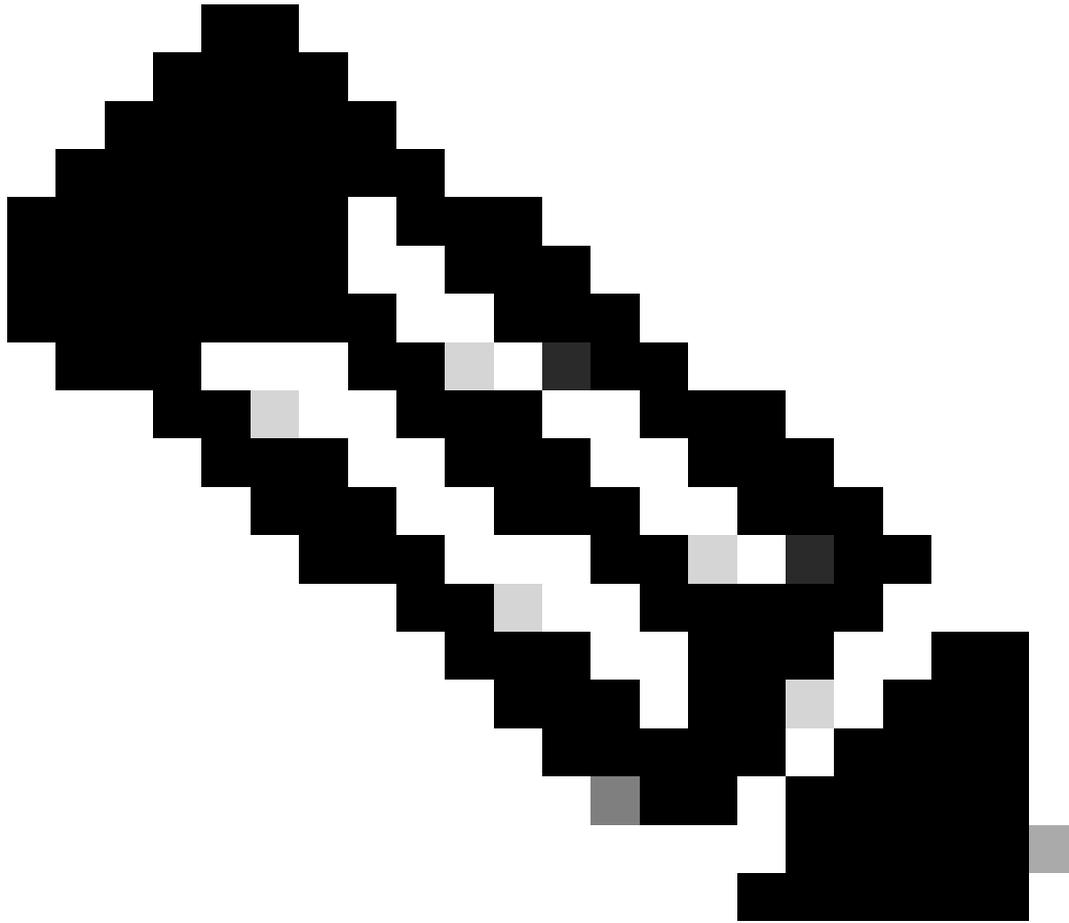
모든 RUM 보고서는 PI에서 서명하고 CSSM에서 검증합니다. CSSM은 PI에서 RUM 보고서 데이터를 받으면 보고서를 검증하고 라이선스 사용 변경 일정을 확인한 후 그에 따라 CSSM 데이터를 업데이트합니다. 그런 다음 CSSM은 ACK 응답 메시지를 통해 PI에 다시 응답합니다.

RUM 보고서는 여러 가지 방법으로 CSSM에 전송할 수 있습니다.

- PI는 보고 간격에 따라 RUM 보고서를 CSSM에 직접 전송합니다.
- PI가 RUM 보고서를 CSLU에 푸시합니다.
- CSLU는 및 모델을 통해 정기적으로 PI에서 RUMRESTAPI 보고서를 YANG 가져옵니다.
- RUM 보고서는 CLI를 통해 PI에 수동으로 저장되고 CSSM에 수동으로 업로드됩니다.



참고: 시스템 컨피그레이션을 삭제/수정하거나 nvram을 지우거나 플래시를 포맷하면 RUM 보고서를 지울 수 없습니다 filesystem. 모든 RUM 보고서는 '라이선스 smart factory reset'에서 PI에서 제거할 수 있습니다.



주: 기본 보고 간격은 30일입니다.

그린필드(Greenfield) 구축 사례의 제조 흐름

Cisco CCW(Cisco Commerce Workspace)에서 새 제품을 주문하면 PI는 제조 팀에서 수행하는 작업 플로우를 거칩니다. 이는 RUM 보고서에 서명하는 보안 프로세스를 촉진하고 PI 등록 시 day-0 마찰을 제거하기 위한 것입니다. 일단 주문이 이루어지면 존재하는 SA/VA 또는 새로 생성된 SA/VA가 제품과 연결됩니다. Cisco 제조 팀은 제품을 배송하기 전에 다음 작업을 처리합니다.

- 디바이스에 Trust Code를 설치합니다. 트러스트 코드 서명이 장치 UDI를 기반으로 설치됩니다. 모든 제품에 설치되어 있습니다

- Install Purchase Code(구매 코드 설치) - 제품과 함께 구매하는 라이선스 레벨에 대한 정보입니다. 모든 제품에 설치되어 있습니다
- SLAC - Smart License 인증 코드 - Catalyst 플랫폼에는 해당되지 않습니다.
- Install Policy(설치 정책) - 사용자의 입력에 따라 Default(기본) 또는 Custom Policy(사용자 지정 정책)를 설정합니다.
- 라이선스 사용량을 CSSM - SA/VA에 보고합니다.

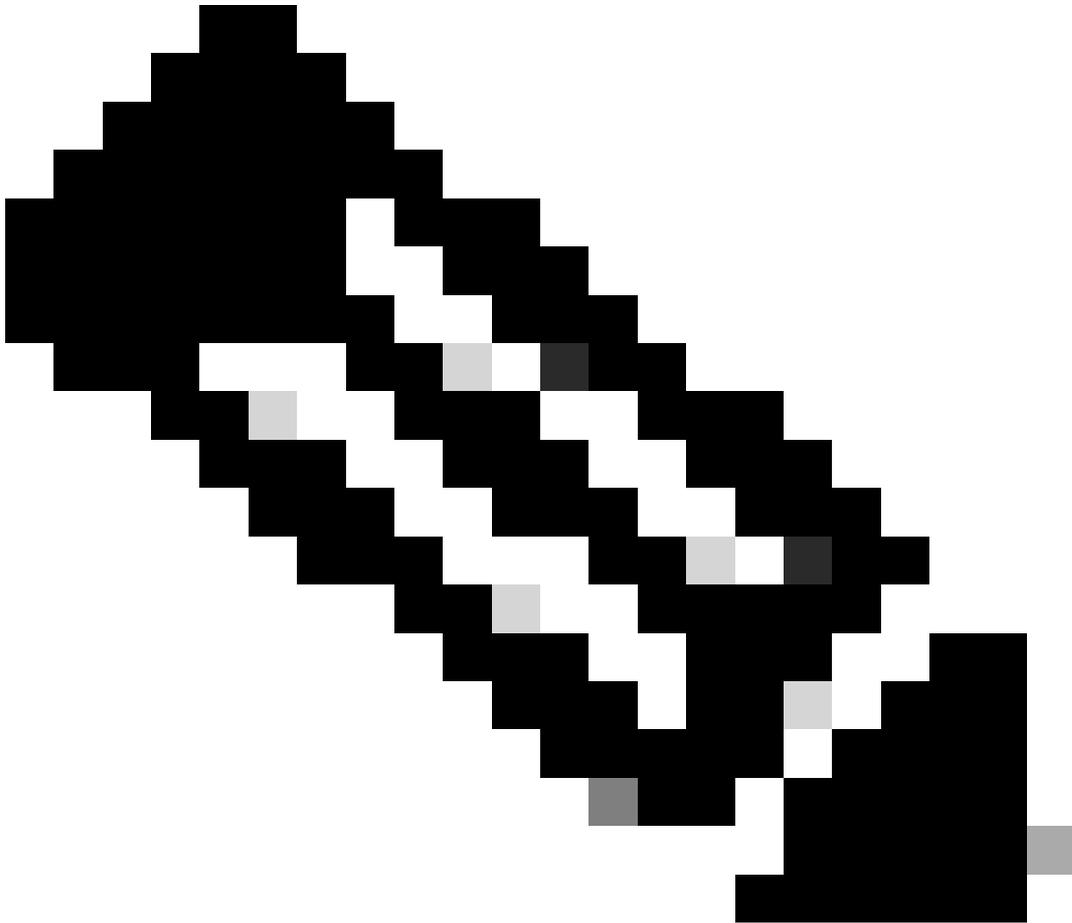


참고: 17.3.3 릴리스에서는 C9200/C9200L을 제외한 모든 Catalyst 스위칭 플랫폼에서 이 흐름이 이어집니다.

참고: 트러스트 코드는 C9200/C9200L을 제외한 모든 Catalyst 스위칭 플랫폼에 대해 17.7.1의 제조에서만 설치됩니다.

CSLU

SLP는 간단하면서도 강력한 새로운 톨 CSLU를 제공합니다. CSLU는 RHEL/Debian 기반의 Windows 10 운영 체제 또는 Linux 버전에서 실행되는 GUI 기반 톨입니다. 로컬 사설 네트워크에서 실행할 수 있는 CSLU는 CSSM과 연결된 PI에서 RUM 포트를 수집합니다. CSLU는 로컬 네트워크의 PI에 대한 RUM 보고서를 수집하고 인터넷을 통해 RUM 보고서를 CSSM에 주기적으로 푸시하는 방식으로 프로비저닝되어야 합니다. CSLU는 프로비저닝된 디바이스의 UDI에 대한 세부 정보만 표시하는 간단한 톨입니다. 풀의 PI, 구매한 라이선스 및 사용되지 않은 라이선스에 대한 모든 라이선스 사용 데이터는 CSSM의 SA/VA에서만 볼 수 있으므로 확인할 수 있습니다. 최대 10K PI의 사용 보고서를 수집할 수 있어 강력하다. CSLU는 CSSM의 ACK 메시지를 다시 PI로 푸시할 책임이 있습니다.

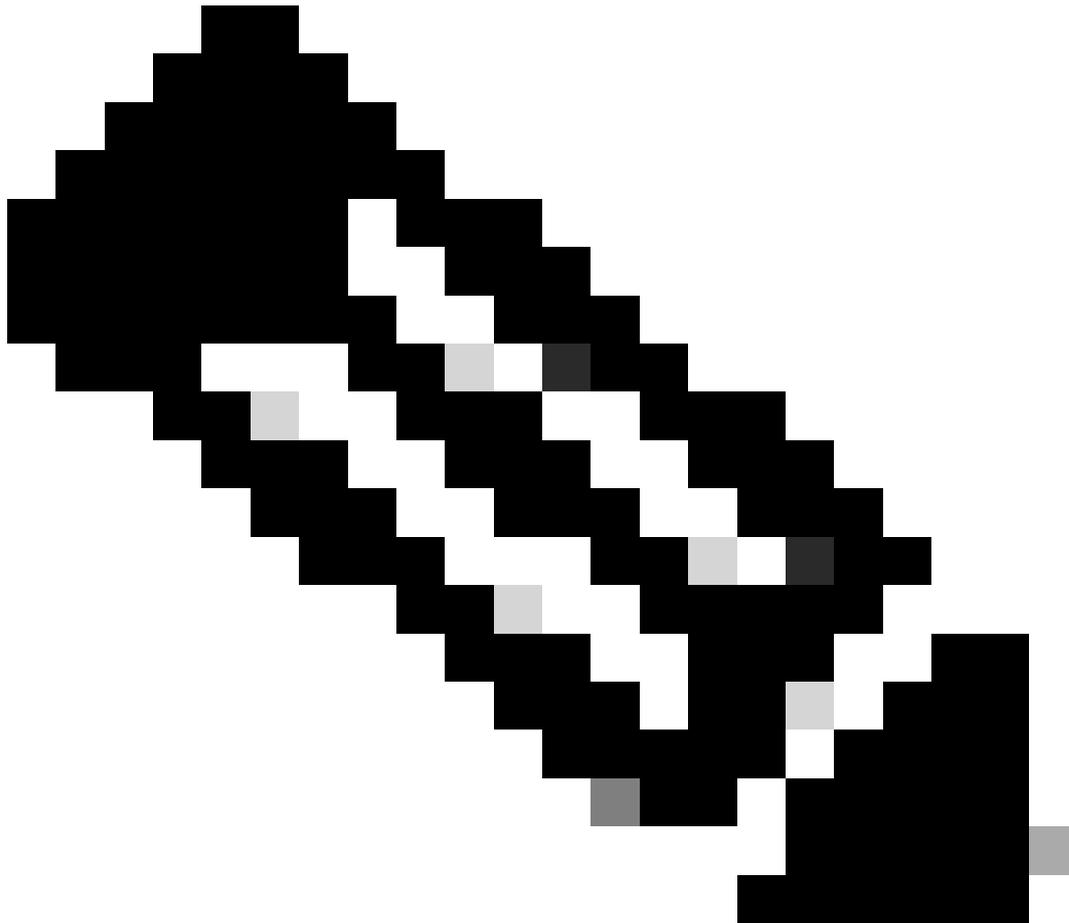
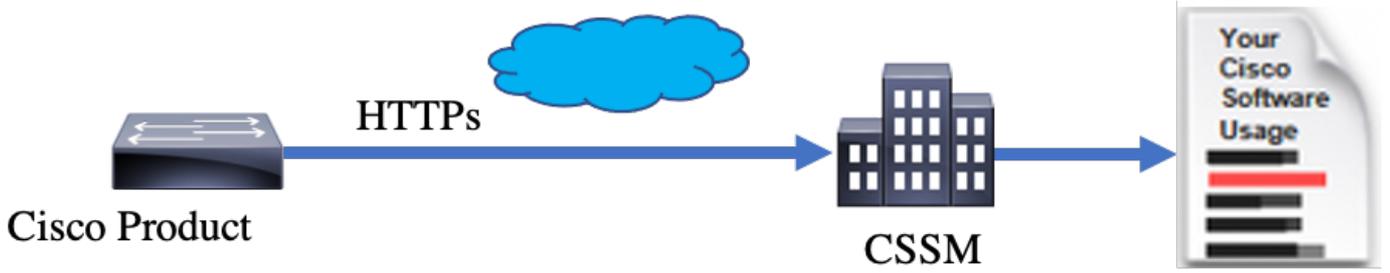


참고: 자세한 컨피그레이션 및 지원되는 CSLU 작동 모드에 대해서는 CSLU 기반 톨폴로지 섹션을 참조하십시오.

참고: CSLU의 Linux 버전은 릴리스 17.7.1부터 지원됩니다.

SLP - 직접 연결

출고 시 출하된 제품에서 기본 전송 모드는 CSLU로 구성됩니다. 직접 연결 방법을 사용하려면 요구 사항에 따라 전송 모드를 Call-home 또는 SMART로 변경해야 합니다. 토폴로지의 Direct Connect 방법에 대한 기본 요구 사항은 CSSM에 연결할 수 있도록 인터넷에 연결하는 것입니다. 또한 CSSM에 연결하려면 필요한 L3 컨피그레이션, DNS 및 도메인 컨피그레이션이 디바이스에 있는지 확인해야 합니다.



참고: CSSM에 직접 연결할 경우 Smart Transport가 권장되는 전송 방법입니다.

Direct Connect 토폴로지에서 RUM 보고서는 CSSM으로 직접 전송됩니다. 라이선스 보고서를 사용하려면 디바이스에 Trust Code(신뢰 코드)를 설치해야 합니다. 신뢰 코드는 배송되기 전에 Cisco Manufacturing에서 디바이스에 설치합니다. 디바이스에 Trust Code를 설치할 수도 있습니다.

Trust Code(신뢰 코드)는 Virtual Account - General(가상 어카운트 - 일반) 페이지에서 CSSM에서 가져온 토큰 문자열입니다. 신뢰 코드는 CLI를 통해 설치할 수 있습니다.

```
Switch#license smart trust idtoken <> all/local
```

 **참고:** 모든 옵션은 HA 또는 스택킹 백 시스템에 사용해야 합니다. 독립형 디바이스의 경우 local 옵션을 사용할 수 있습니다.

```
Switch#license smart trust idtoken <> all/local.
```

On Successful installation of policy, the same can be verified through 'show license status' CLI.

```
Switch#show license status
```

Utility:

Status: DISABLED

Smart Licensing Using Policy:

Status: ENABLED

Data Privacy:

Sending Hostname: yes

Callhome hostname privacy: DISABLED

Smart Licensing hostname privacy: DISABLED

Version privacy: DISABLED

Transport:

Type: Callhome

Policy:

Policy in use: Installed On Nov 07 22:50:04 2020 UTC

Policy name: SLP Policy

Reporting ACK required: yes (Customer Policy)

Unenforced/Non-Export Perpetual Attributes:

First report requirement (days): 60 (Customer Policy)

Reporting frequency (days): 60 (Customer Policy)

Report on change (days): 60 (Customer Policy)

Unenforced/Non-Export Subscription Attributes:

First report requirement (days): 30 (Customer Policy)

Reporting frequency (days): 30 (Customer Policy)

Report on change (days): 30 (Customer Policy)

Enforced (Perpetual/Subscription) License Attributes:

First report requirement (days): 0 (CISCO default)

Reporting frequency (days): 90 (Customer Policy)

Report on change (days): 90 (Customer Policy)
Export (Perpetual/Subscription) License Attributes:
First report requirement (days): 0 (CISCO default)
Reporting frequency (days): 90 (Customer Policy)
Report on change (days): 90 (Customer Policy)

Miscellaneous:

Custom Id: <empty>

Usage Reporting:

Last ACK received: Nov 03 12:57:01 2020 UTC

Next ACK deadline: Dec 03 12:57:01 2020 UTC

Reporting push interval: 30 days

Next ACK push check: <none>

Next report push: Nov 07 22:50:35 2020 UTC

Last report push: Nov 03 12:55:57 2020 UTC

Last report file write: <none>

Trust Code Installed:

Active: PID:C9500-24Y4C,SN:CAT2344L4GH

INSTALLED on Nov 07 22:50:04 2020 UTC

Standby: PID:C9500-24Y4C,SN:CAT2344L4GJ

INSTALLED on Nov 07 22:50:04 2020 UTC

신뢰 코드가 성공적으로 설치되면 PI는 CSSM에 직접 사용량을 보고할 수 있습니다. 다음 조건을 충족하면 라이선스가 보고됩니다.

- 성공적인 신뢰 코드 설치
- 모든 기본 보고 간격
- 온디바이스 다시 로드/부팅
- 전환
- 스택 멤버 추가 또는 제거
- 라이선스 동기화의 수동 트리거

CSSM에 대한 라이선스 보고는 다음 CLI로 트리거할 수 있습니다.

```
Switch#license smart sync all
```

의 Usage Reporting(사용 보고) show license status 섹션에서는 마지막으로 수신한 ACK, 다음 ACK 기한, 다음 보고서 푸시 및 마지막 보고서 푸시의 일정을 알려줍니다.

Usage Reporting:

Last ACK received: Nov 03 12:57:01 2020 UTC
Next ACK deadline: Dec 03 12:57:01 2020 UTC
Reporting push interval: 30 days
Next ACK push check: <none>
Next report push: Nov 07 22:50:35 2020 UTC
Last report push: Nov 03 12:55:57 2020 UTC
Last report file write: <none>

Direct Connect - Smart Transport

Direct Connect 또는 Direct Cloud Access 모드 토폴로지에서 SMART Transport를 사용하는 경우, 이는 디바이스에서 필요한 컨피그레이션입니다.

Configure the desired Transport mode using below CLI.

```
Switch(config)#license smart transport smart
```

Running config on Smart Transport Mode:

```
!  
license smart url smart https://smartreceiver.cisco.com/licservice/license  
license smart transport smart  
!
```

직접 연결 - Call-Home 전송

Direct Connect 또는 Direct Cloud Access 모드 토폴로지에서 Call-home Transport를 사용하는 경우 이는 디바이스에서 필요한 컨피그레이션입니다.

Configure the desired Transport mode using below CLI.

```
Switch(config)#license smart transport callhome
```

Running config on Smart Transport Mode:

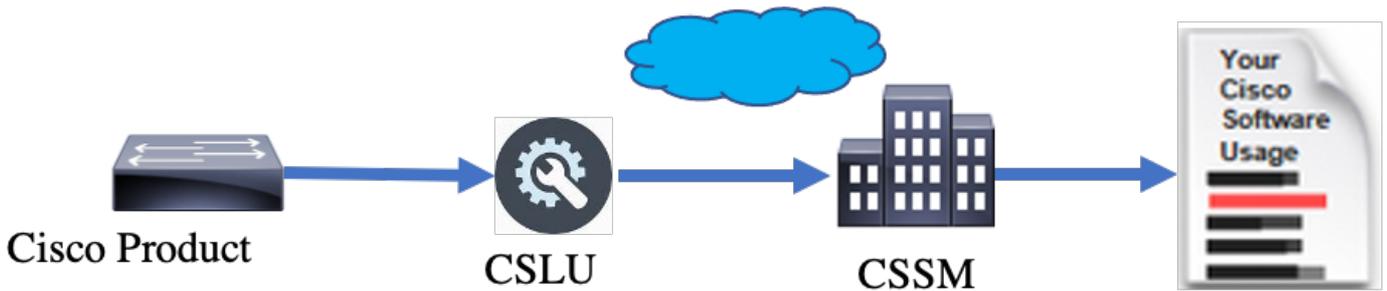
```
!  
service call-home  
!  
call-home  
contact-email-addr shmandal@cisco.com  
no http secure server-identity-check  
profile "CiscoTAC-1"  
active
```

reporting smart-licensing-data
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination transport-method http
!

 **참고:** 기본적으로 Call-home의 대상 주소는 CSSM URL로 구성됩니다. 이는 컨피그레이션에서 확인할 수 show run all 있습니다.

SLP - CSLU

CSLU 모드는 17.3.2 이상을 실행하는 공장 출하 장치에서 기본 전송 모드입니다. 또한 Eval/Eval 만료된 라이선스에서 마이그레이션 하는 경우 SLP로 이동한 후의 전송 모드는 CSLU입니다. CSLU 기반 토폴로지에서는 CSLU는 PI와 CSSM 사이에 위치합니다. CSLU는 사용자가 Cisco Cloud - CSSM에 직접 네트워크를 연결하지 않도록 합니다. CSLU는 사실 네트워크에서 로컬로 실행할 수 있으며, 연결된 모든 PI에서 사용 보고서를 다운로드할 수 있습니다. 사용 보고서는 인터넷을 통해 CSSM으로 전송되기 전에 Windows PC에 로컬로 저장됩니다. CSLU는 경량형 도구입니다. 연결된 PI 목록만 볼 수 있으며 UDI를 사용하여 식별할 수 있습니다. CSLU는 PI 또는 라이선스 레벨 또는 라이선스 사용량의 이중화 정보를 표시하거나 포함할 수 없습니다.

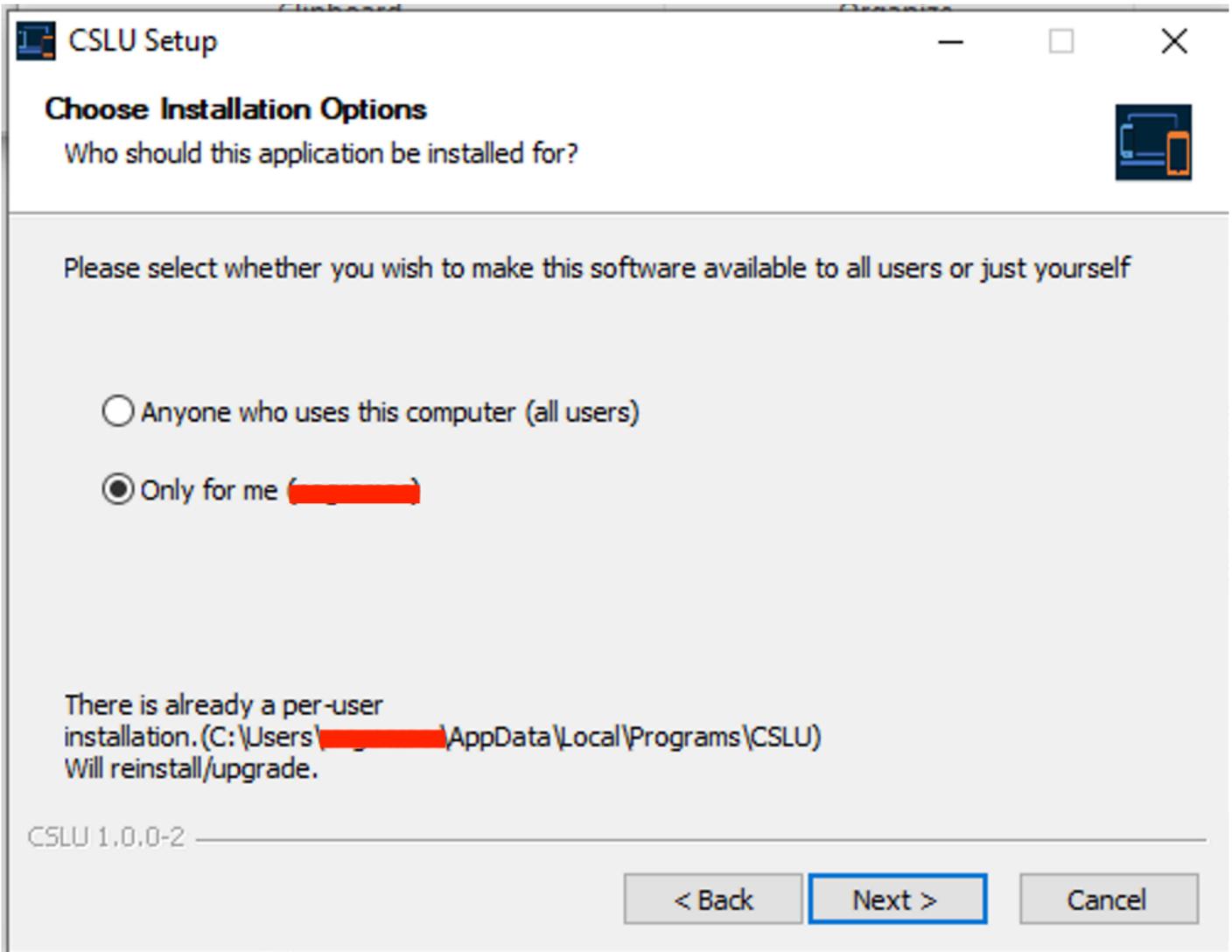


CSLU 설치 및 컨피그레이션

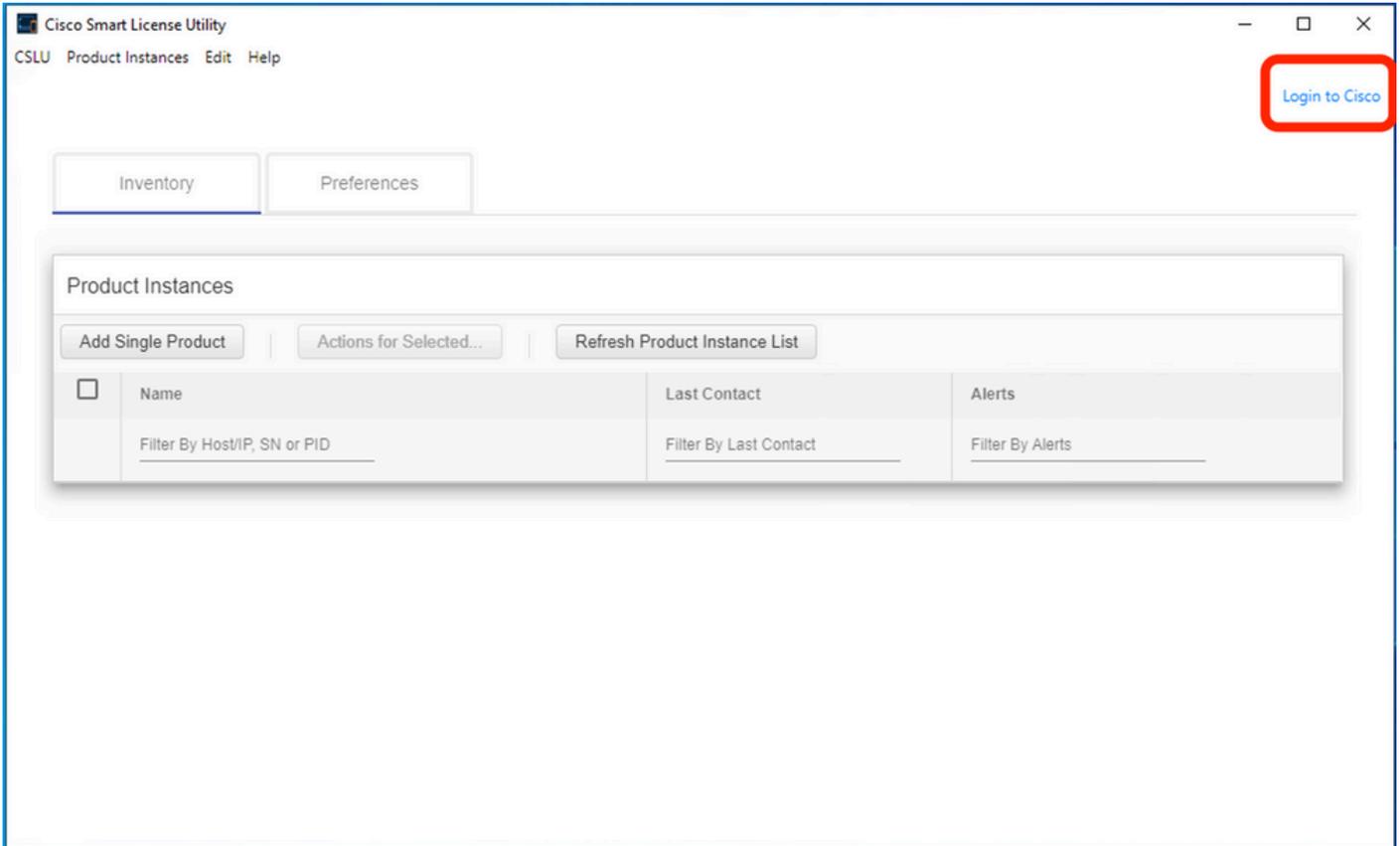
CSLU 도구는 Windows 10 시스템에 설치 및 작동합니다. 이 소프트웨어는 CCO에서 무료로 다운로드하여 사용할 수 있습니다. 도구가 설치되면 Help(도움말) 메뉴에서 Quick Start Guide/User Manual(빠른 시작 설명서/사용자 설명서)을 다운로드하여 로 이동할 수 Help > Download Help Manual 있습니다.

CSLU를 설치하려면 사용권 계약에 동의해야 합니다.

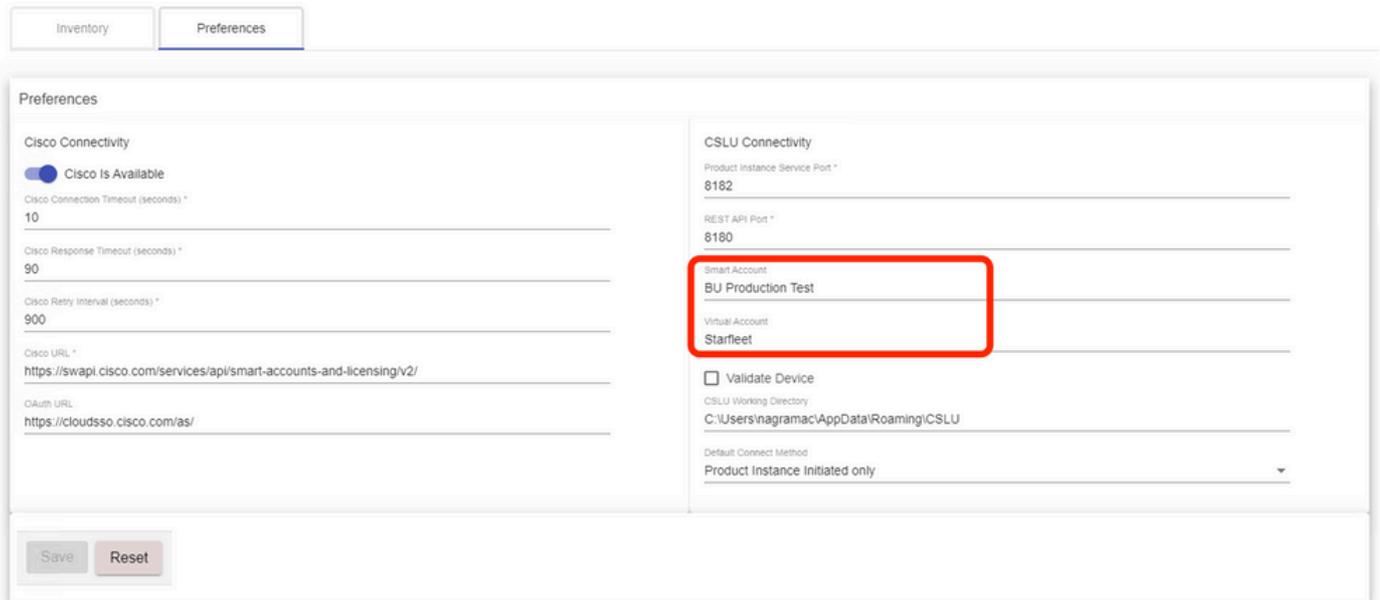
응용 프로그램은 현재 사용자에게 대해서만 설치하고 컴퓨터에서 작업하는 모든 사용자에게 대해서는 설치하지 않는 것이 좋습니다. CSLU의 이전 버전이 이미 PC에 있는 경우, 이를 미리 제거하는 것이 좋습니다. 그럼에도 불구하고, 새로운 설치 소프트웨어를 업그레이드하기 위해 신경을 쓴다.



설치 후 애플리케이션의 오른쪽 상단 모서리에 있는 로그인 옵션을 사용하여 Cisco에 로그인합니다. CEC 자격 증명을 사용합니다. 그리고 로그인을 통해 CSLU와 CSSM 간에 신뢰가 설정됩니다.



Cisco에 로그인한 후 툴의 Preference(환경 설정) 창에서 드롭다운 메뉴를 통해 SA 및 VA 세부사항이 올바르게 선택되었는지 확인합니다. 컨피그레이션을 저장해야 합니다.



CSLU의 일정 탭 - CSLU의 일정 탭을 통해 다음을 구성할 수 있습니다.

- CSSM에서 사용 가능한 데이터를 폴링합니다. - CSSM에서 데이터의 작업 타이밍, 마지막 끝어오기 시간 및 다음 끝어오기 시간을 표시합니다.
- 제거된 데이터 정리 - CSLU 데이터 저장소에서 제거된 모든 데이터를 제거합니다. 수동으로 트리거할 수도 있습니다.

- Pull device data - CSLU pull 모드를 트리거합니다.

Scheduler			
Refresh Job Information			
System Jobs			
Name	Status	Next Execution Time	Start
Poll CSSM for Available Data	scheduled	09-Feb-2023 18:35	
Clean Up Purged Data	scheduled	24-Feb-2023 01:40	Start
Operational Jobs			
Name	Status	Next Execution Time	Start
Pull Device Data	scheduled	24-Feb-2023 01:14	Start

푸시 모드를 사용하는 CSLU

CSLU는 기본적으로 PUSH 모드에서 작동합니다. PUSH 모드에서는 PI가 정기적으로 CSLU에 사용량 보고서를 전송합니다. 디바이스에서 CSLU에 대한 L3 네트워크 연결을 사용할 수 있는지 확인해야 합니다. PI가 CSLU와 통신하려면 CSLU를 실행하는 Windows 시스템의 IP 주소를 구성해야 합니다.

Switch(config)#license smart url cslu <http://<IP of CSLU>:8182/cslu/v1/pi>

The same can be verified through 'show license status' CLI

Switch#show license status

Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%

No time source, 20:59:25.156 EDT Sat Nov 7 2020

Utility:

Status: DISABLED

Smart Licensing Using Policy:

Status: ENABLED

Data Privacy:

Sending Hostname: yes

Callhome hostname privacy: DISABLED

Smart Licensing hostname privacy: DISABLED

Version privacy: DISABLED

Transport:

Type: cslu

Cslu address: [http://<IP of CS LU>:8182/cslu/v1/pi](http://<IP_of_CS LU>:8182/cslu/v1/pi)

Proxy:

Not Configured

Policy:

Policy in use: Merged from multiple sources.

Reporting ACK required: yes (CISCO default)

Unenforced/Non-Export Perpetual Attributes:

First report requirement (days): 365 (CISCO default)

Reporting frequency (days): 0 (CISCO default)

Report on change (days): 90 (CISCO default)

Unenforced/Non-Export Subscription Attributes:

First report requirement (days): 90 (CISCO default)

Reporting frequency (days): 90 (CISCO default)

Report on change (days): 90 (CISCO default)

Enforced (Perpetual/Subscription) License Attributes:

First report requirement (days): 0 (CISCO default)

Reporting frequency (days): 0 (CISCO default)

Report on change (days): 0 (CISCO default)

Export (Perpetual/Subscription) License Attributes:

First report requirement (days): 0 (CISCO default)

Reporting frequency (days): 0 (CISCO default)

Report on change (days): 0 (CISCO default)

Miscellaneous:

Custom Id: <empty>

Usage Reporting:

Last ACK received: <none>

Next ACK deadline: Feb 05 15:32:51 2021 EDT

Reporting push interval: 30 days

Next ACK push check: <none>

Next report push: Nov 07 15:34:51 2020 EDT

Last report push: <none>

Last report file write: <none>

Trust Code Installed: <none>

보고서는 다음 조건에 따라 PI에서 CSLU로 전송됩니다.

- 모든 기본 보고 간격
- 온디바이스 다시 로드/부팅
- 전환 시
- 스택 멤버 추가 또는 제거 시
- 라이선스 동기화의 수동 트리거

CSLU에서 인벤토리 페이지에는 현재 CSLU와 연결된 디바이스가 나열됩니다. 목록의 디바이스는 UDI를 통해 식별할 수 있습니다. 디바이스는 목록에서 PID 또는 SN을 기준으로 필터링하여 특정 디바이스를 식별할 수 있습니다.

CSLU 인벤토리 페이지에는 다음과 같은 두 개의 열이 있습니다.

- The **Last Contact**(**마지막 연락처**) 열 - 보고 상태가 변경된 경우 최신 타임스탬프를 표시합니다.

- Alert(경고) 열 - PI의 최신 보고 상태를 표시합니다.

PI가 CSLU에 보고서를 전송하면 CSLU는 CSSM에서 PI 항목을 생성합니다. Alerts(알림) 상태 및 Last Contact TS(최종 연락처 TS)가 업데이트됩니다.

Name	Last Contact	Alerts
UDI_PID.C9500-32QC; UDI_SN.CAT2148L15K	08-Nov-2020 06:37	COMPLETE: Usage report from product instance
UDI_PID.C9500-24Y4C; UDI_SN.CAT2344L4GH	03-Nov-2020 18:27	COMPLETE: Usage report acknowledgement to product instance

Name	Last Contact	Alerts
UDI_PID.C9500-32QC; UDI_SN.CAT2148L15K	08-Nov-2020 06:37	COMPLETE: Usage report uploaded to CSSM
UDI_PID.C9500-24Y4C; UDI_SN.CAT2344L4GH	03-Nov-2020 18:27	COMPLETE: Usage report acknowledgement to product instance

CSSM은 CSLU에서 보낸 보고서를 처리하고 라이선스 사용량을 기반으로 CSSM에서 제품 인스턴스를 추가/업데이트합니다. CSSM에서 날짜를 처리하고 업데이트하면 ACK 메시지가 CSLU에 다시 전송됩니다. CSLU는 메시지를 저장하고 다시 PI로 전달합니다.

ACK 메시지는 다음으로 구성됩니다.

- 전송된 모든 보고서에 대한 승인
- 정책
- 신뢰 코드

CSSM에서 새 정책을 사용할 수 있는 경우, 이제 PI에도 업데이트됩니다. 정책이 변경되지 않은 경우 PI에 푸시됩니다.



참고: 정책에 따라 ACK 메시지 보고가 필요하지 않으면 ACK 메시지가 전송되지 않습니다.

경고 메시지 열에는 다음 상태 중 하나가 포함될 수 있습니다.

- 제품 인스턴스의 사용 현황 보고서
- Cisco에 업로드된 사용 보고서
- 제품 인스턴스의 동기화 요청
- 동기화 요청이 CSSM에 업로드됨
- CSSM에서 받은 확인 응답
- 제품 인스턴스에 대한 사용 보고서 승인

 **참고:** HA 시스템의 CSLU에서는 항상 Active의 UDI에 대해서만 항목이 표시됩니다. CSSM에만 나열된 시스템의 개별 디바이스에 대한 모든 UDI가 있습니다.

CSLU 자동 검색

최소 컨피그레이션으로 확장 구축을 지원하기 위해 CSLU의 자동 검색이 지원됩니다. 즉, CSLU의 IP 주소/URL을 특별히 구성할 필요가 없습니다. 이를 위해서는 해당 DNS 서버에 엔트리를 추가하기만 하면 됩니다. 그러면 전송 모드가 CSLU(기본값)인 디바이스에서 자동으로 CSLU를 검색하고 보고서를 전송할 수 있습니다.

몇 가지 확실한 사항은 다음과 같습니다.

- DNS 서버에 항목을 만듭니다. CSLU의 IP 주소는 이름에 매핑되어야 합니다 `cslu-local`.
- 이름 서버 및 DNS 컨피그레이션이 디바이스에 있는지 확인합니다.

이를 통해 추가 컨피그레이션 없이 네트워크의 디바이스가 CSLU에 도달하고 정기적으로 RUM 보고서를 전송할 수 있습니다.

끌어오기 모드를 사용하는 CSLU

PULL 모드는 CSLU가 디바이스에서 RUM 보고서를 가져오는 프로세스를 시작하는 모드입니다. 여기서 디바이스 세부사항이 CSLU에 추가되고 CSLU는 정기적으로 추가된 모든 디바이스의 데이터를 가져옵니다. CSLU에서 PULL을 수동으로 트리거할 수도 있습니다. CSLU는 RUM 보고서를 CSSM으로 전송하고 CSSM에서 다시 수신한 ACK 메시지를 PI로 전송합니다. PULL 모드는 RESTAPI, NETCONF 및 의 세 가지 다른 수단으로 지원됩니다 RESTCONF.

RESTAPI를 사용하는 풀 모드

PULL 모드가 제대로 작동하려면 RESTAPI 디바이스와 CSLU에 필요한 컨피그레이션은 다음과 같습니다.

Configs on PI:

Ensure the network reachability from PI to CSLU is available and working.

```
!  
ip http server  
ip http authentication local  
ip http secure-server  
!  
aaa new-model  
aaa authentication login default local  
aaa authorization exec default local  
username admin privilege 15 password 0 lab  
!
```



참고: 사용자에게 Priv 레벨 15 액세스 권한이 있어야 합니다.

CSLU - 설정 절차

보고서를 자동으로 동기화하려면 CSLU가 CSSM에 로그인해야 합니다.

1단계. 인벤토리 페이지에서 선택합니다Add Single Product.

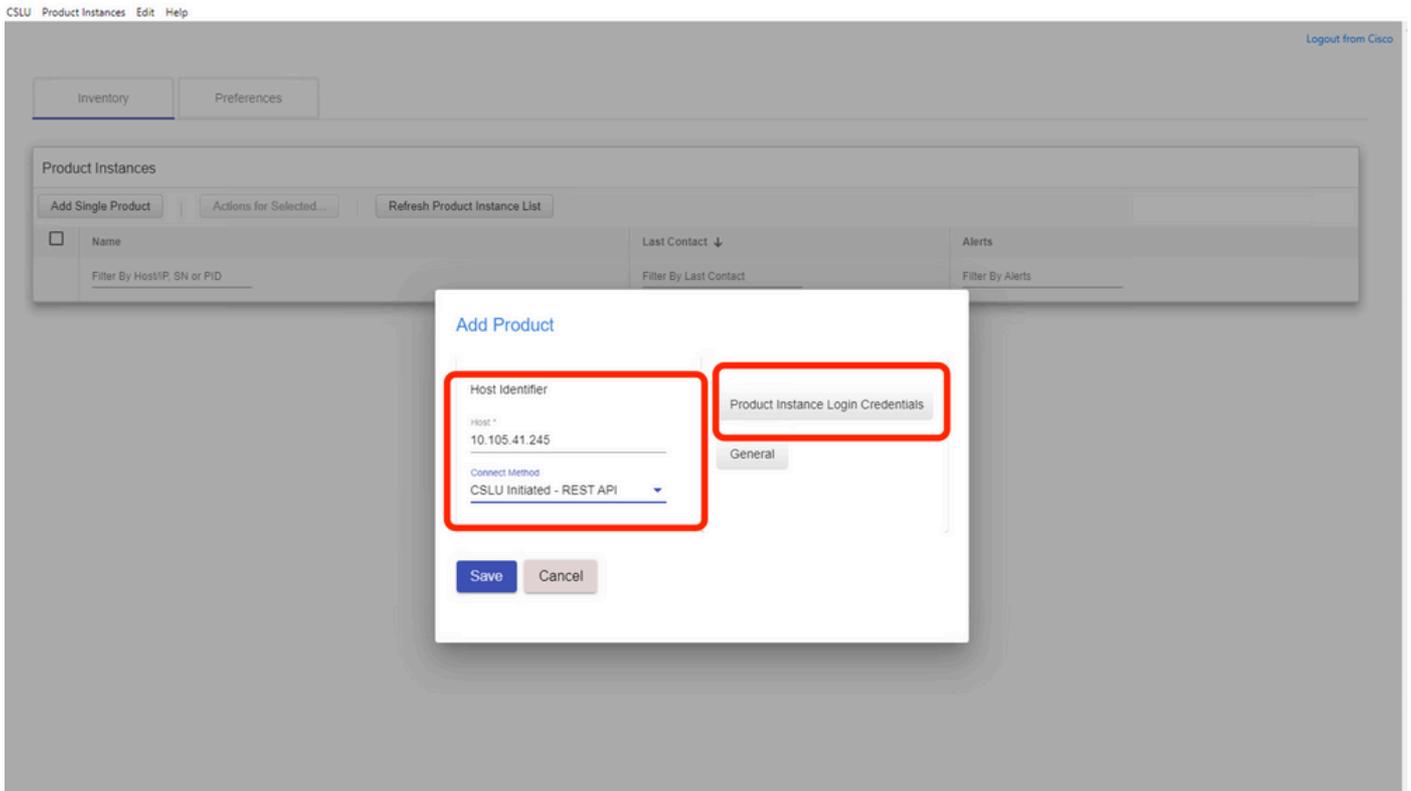
2단계. 디바이스 IP를 입력합니다.

3단계. 연결 방법을 다음으로 RestAPI 선택합니다.

4단계. 제품 인스턴스 로그인 자격 증명을 선택합니다.

5단계. Priv 15 액세스 권한이 있는 사용자의 사용자 자격 증명을 입력합니다.

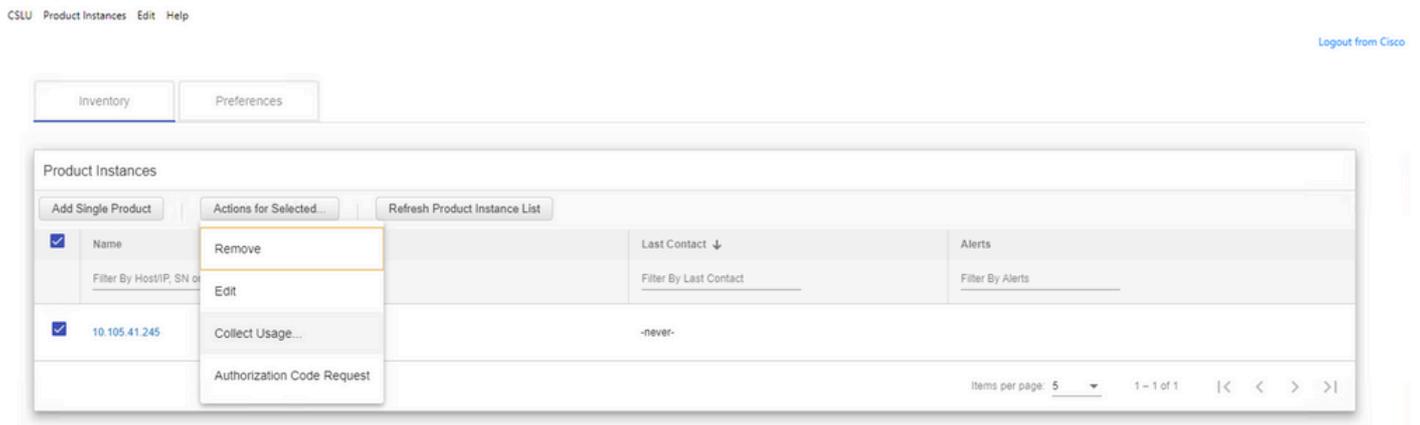
6단계. 구성을 저장합니다.

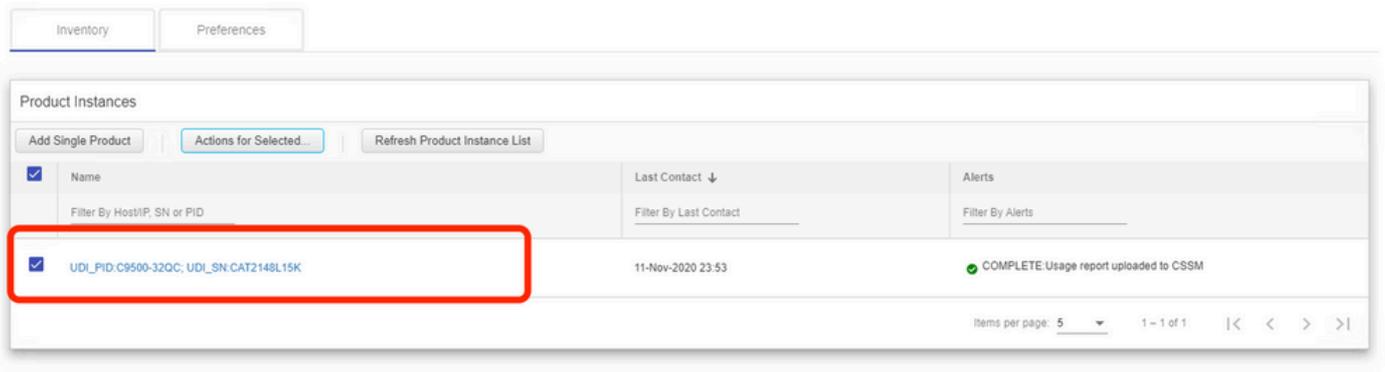


Name(이름) 필드에 IP 주소만 있는 디바이스가 추가됩니다.

디바이스를 선택하고 로 Actions for Selected > Collect Usage 이동합니다.

사용 데이터가 성공적으로 수집되면 Name 필드가 PI의 UDI로 업데이트되고 타임스탬프도 업데이트됩니다. 경고 필드는 최신 상태를 반영합니다.





CSSM에서 ACK 메시지를 수신할 때 디바이스가 여전히 사용 가능한 경우 ACK가 PI로 다시 전송됩니다. 그렇지 않으면 다음 Pull Interval(풀 간격)에 ACK가 전송됩니다.

RESTCONF를 사용하는 풀 모드

PULL 모드를 통해 RESTCONF 작업할 경우, 디바이스에서 필요한 컨피그레이션과 CSLU의 단계는 다음과 같습니다.

Configs on PI:

```
!
restconf
!
ip http secure-server
ip http authentication local
ip http client source-interface GigabitEthernet 0/0
!
username admin privilege 15 password 0 lab
!
```



참고: 이러한 컨피그레이션은 로컬 인증을 위한 것입니다. 원격 인증도 사용할 수 있습니다.

CSLU - 설정 절차

보고서를 자동으로 동기화하려면 CSLU가 CSSM에 로그인해야 합니다. CSLU 설정은 RUM 보고서 수집 및 보고와 RESTAPI 동일합니다.

1단계. 인벤토리 페이지에서 선택합니다 Add Single Product.

2단계. 디바이스 IP를 입력합니다.

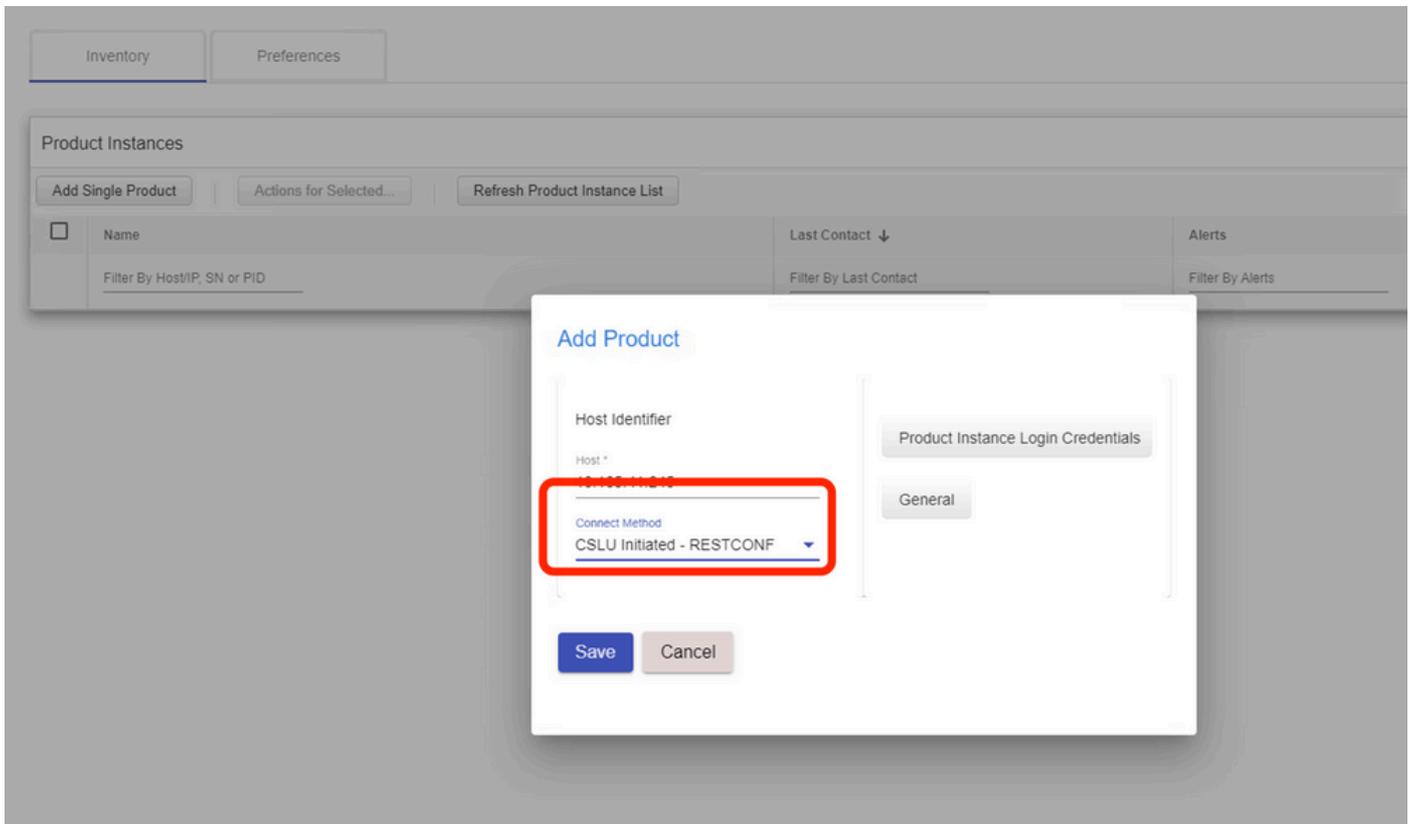
3단계. 연결 방법을 다음으로 RESTCONF 선택합니다.

4단계. 제품 인스턴스 로그인 자격 증명을 선택합니다.

5단계. Priv 15 액세스 권한이 있는 사용자의 사용자 자격 증명을 입력합니다.

6단계. 구성을 저장합니다.

7단계. 선택한 디바이스에 대한 사용량 데이터를 수집합니다.



NETCONF를 사용하는 풀 모드

PULL 모드가 제대로 작동하려면 NETCONF 디바이스에서 필요한 컨피그레이션과 CSLU의 단계가 다음과 같습니다.

Configs on PI:

```
!  
ip ssh version  
!  
netconf-yang  
netconf ssh  
netconf-yang feature candidate-datastore  
!  
username admin privilege 15 password 0 lab  
!
```

To ensure yang process is running, execute the command:

```
Switch#show platform software yang-management process  
confd : Running  
nesd : Running  
syncfd : Running  
ncsshd : Running
```

dmiauthd : Running
nginx : Running
ndbmand : Running
pubd : Running
gnmib : Not Running

 **참고:** 이러한 컨피그레이션은 로컬 인증을 위한 것입니다. 원격 인증도 사용할 수 있습니다.

CSLU - 설정 절차

보고서를 자동으로 동기화하려면 CSLU가 CSSM에 로그인해야 합니다. CSLU 설정은 RUM 보고서 수집 및 보고와 RESTAPI 동일합니다.

1단계. 인벤토리 페이지에서 선택합니다 Add Single Product.

2단계. 디바이스 IP를 입력합니다.

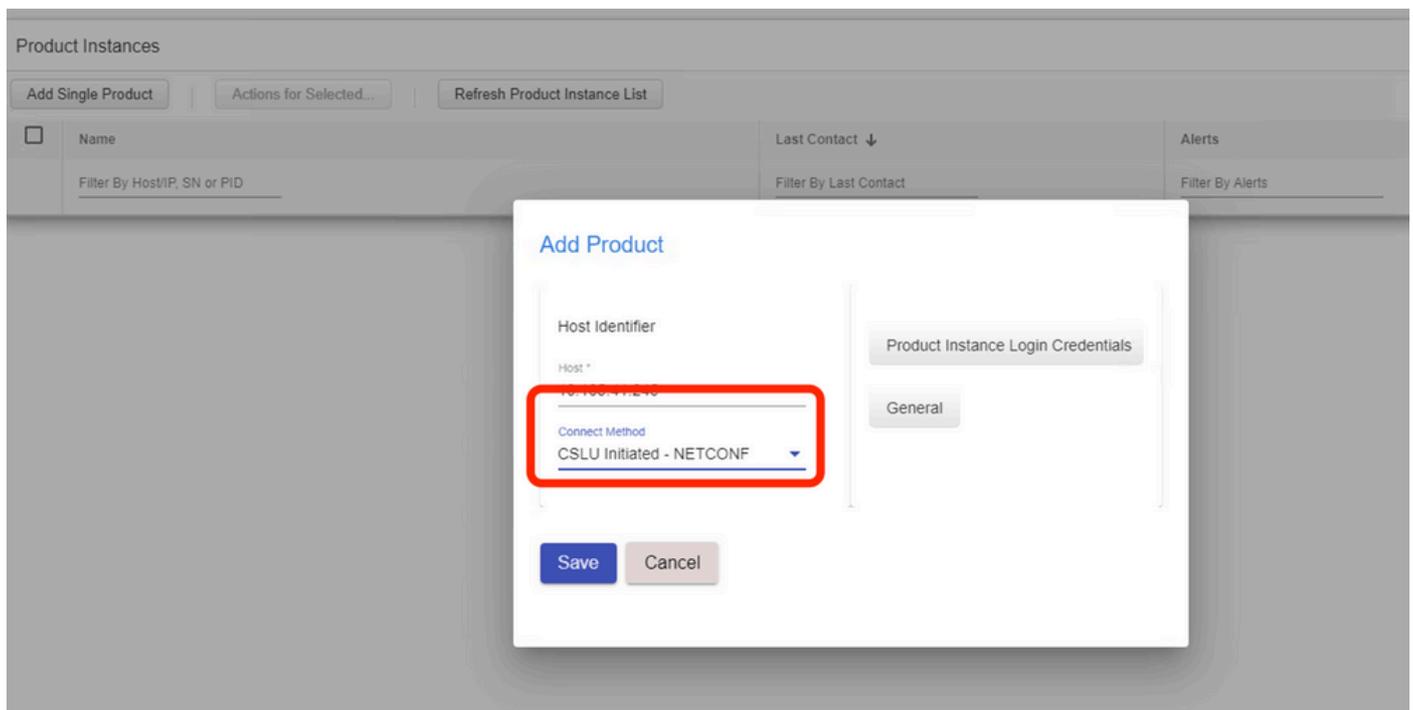
3단계. 연결 방법을 다음으로 NETCONF 선택합니다.

4단계. 제품 인스턴스 로그인 자격 증명을 선택합니다.

5단계. Priv 15 액세스 권한이 있는 사용자의 사용자 자격 증명을 입력합니다.

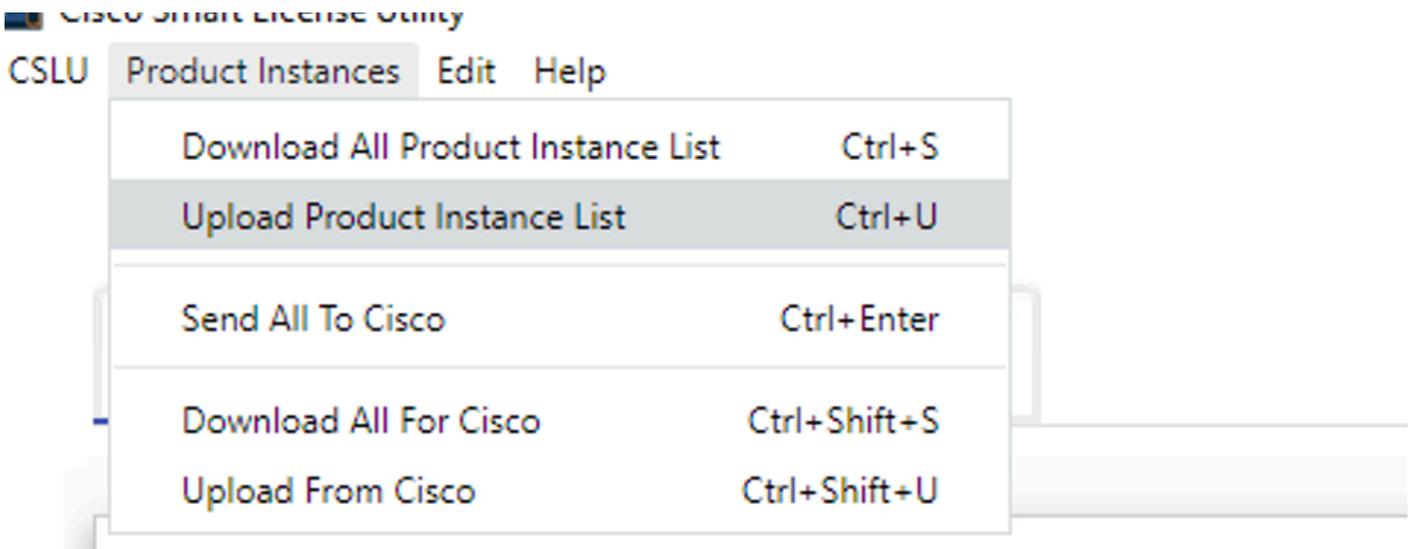
6단계. 구성을 저장합니다.

7단계. 선택한 디바이스에 대한 사용량 데이터를 수집합니다.

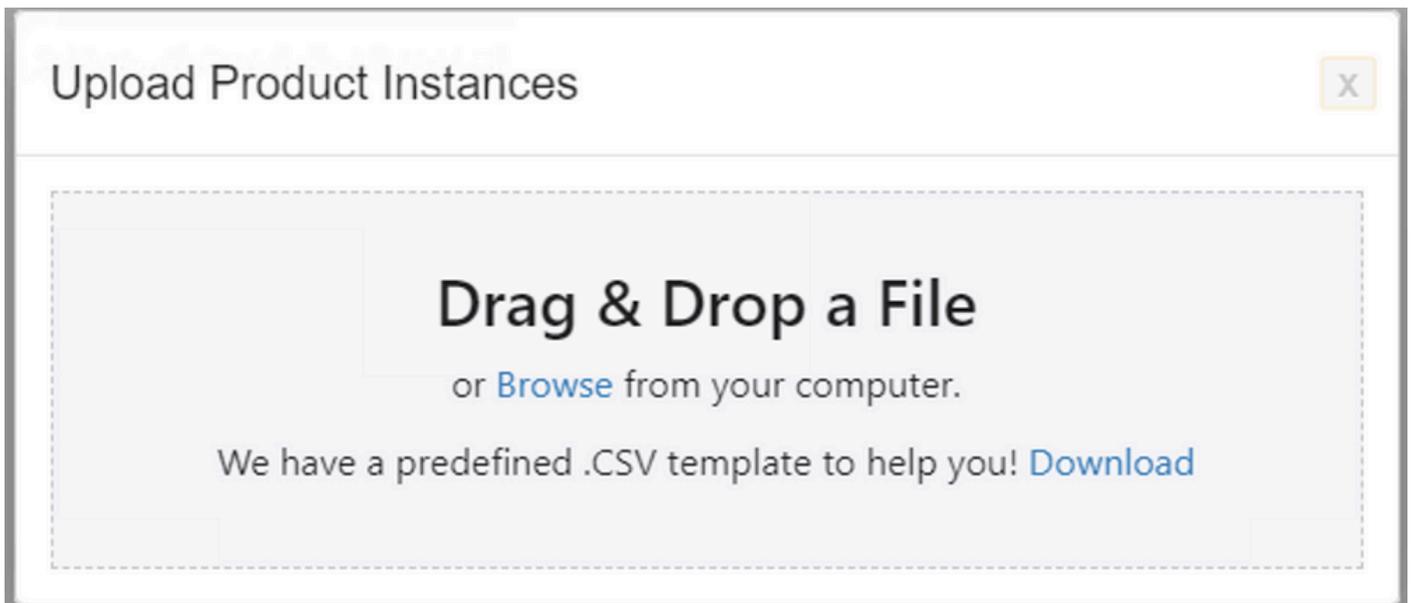


 **참고:** 모든 모델, NETCONF, RESTCONF 및 RESTAPI의 경우 디바이스 목록을 대량으로 추가할 수 있습니다.

대량 업로드를 수행하려면 이 이미지에 표시된 대로 Menu막대에서 Product Instance > Upload Product Instance List 로 이동합니다.



새 팝업 창이 열립니다. 템플릿 파일은 여기에서 다운로드할 수 있습니다. CSV 형식 파일에서 디바이스 목록의 디바이스 세부 정보를 입력하고 CSLU에 업로드하여 여러 디바이스를 추가합니다.



 **참고:** 모든 유형의 CSLU PULL 모드에서는 PI에서 전송 설정을 Off로 설정하는 것이 좋습니다. 이 작업은 CLI를 사용하여 수행할 수 있습니다.

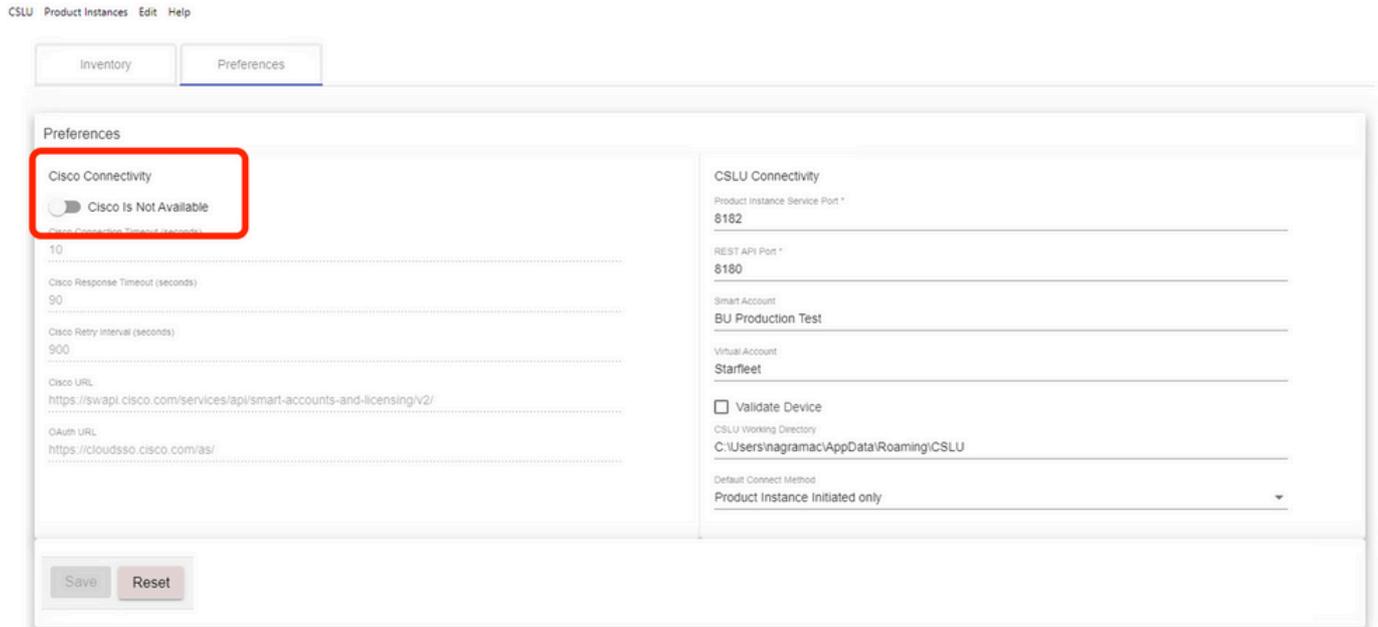
Switch(config)#license smart transport off

연결 끊김 모드를 사용하는 CSLU

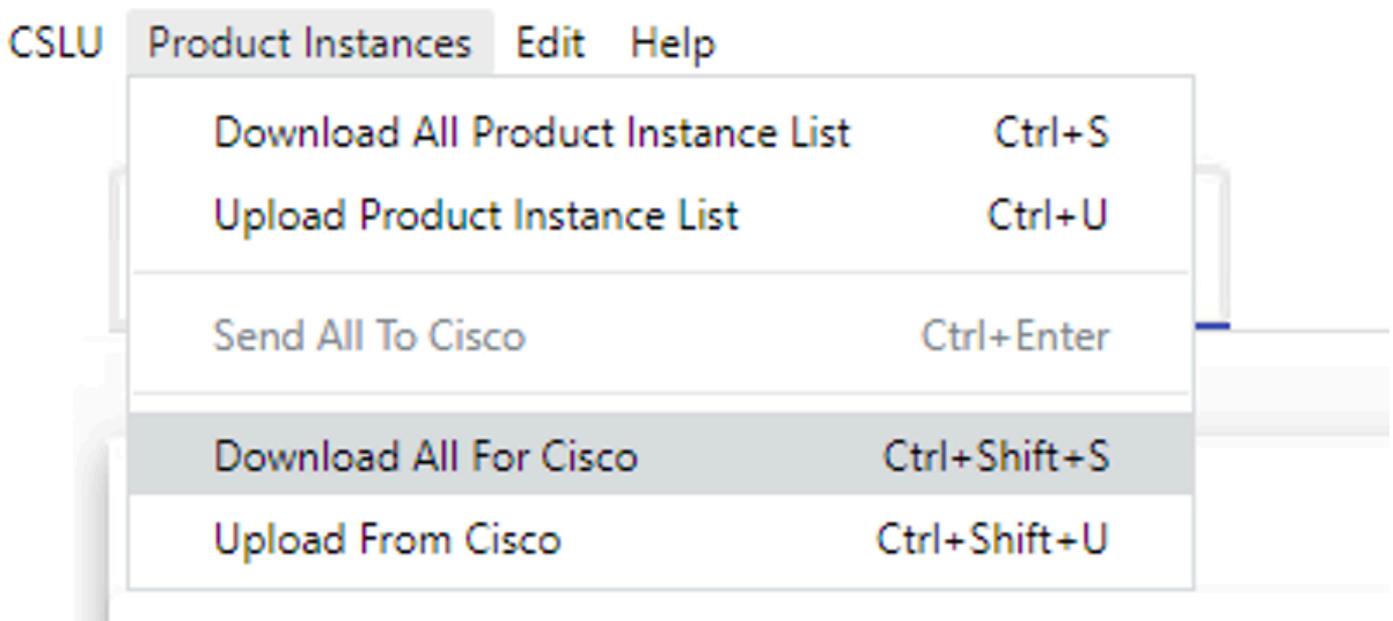
CSLU는 CSSM에서 연결 해제 모드로 작동할 수 있습니다. CSLU를 인터넷에 연결할 수 없는 구축을 위한 것입니다. 연결 해제 모드에서는 모든 디바이스의 보고서가 CSLU에서 수동으로 다운로드되고 CSSM에 업로드됩니다. 그러면 ACK 메시지가 CSSM에서 다운로드되어 CSLU에 업로드됩니다. CSLU는 여전히 PI에서 사용 날짜를 PULL/PUSH하고 PI에 ACK 메시지를 다시 보냅니다.

1단계. 페이지에서 CSLU Preference 옵션을 끕니다 Cisco Connectivity. Cisco를 사용할 수 없음을 확인합니다.

2단계. 설정을 저장합니다.



3단계. 막대에서 Menu 을 클릭합니다 Product Instances > Download All for Cisco. CSLU에 tar.gz 파일이 다운로드됩니다.



4단계. CSSM에 파일을 업로드합니다. CSSM Smart Account 페이지에서 Report > Usage Data Files > Upload usage data 이동합니다. 팝업창에서 파일을 tar.gz 업로드합니다.

Smart Software Licensing

Alerts | Inventory | Convert to Smart Licensing | **Reports** | Preferences | On-Prem Accounts | Activity

Reports

Report	Usage Data Files	Reporting Policy			
Devices can be configured to report the features that they are using. This usage then determines which licenses are needed, in order to be compliant.					
<input type="button" value="Upload Usage Data..."/>		<input type="text" value="Search by File Name, Virtual Account"/>			
Usage Data File	Reported	Virtual Account	Reporting Status	Devices	Acknowledgement
Usage_SLR_1.txt	2020-Oct-29	Quake	i No Errors	2	Download
Usage_SLR.txt	2020-Oct-29	Quake	i No Errors	1	Download
+ UD_SA_BU_Production_Test_20Oct28_11_11_03	2020-Oct-28	DLC-VA1	i No Errors	1	Download
+ UD_SA_20Oct28_10_49_13_092.tar.gz	2020-Oct-28	DLC-VA1	i No Errors	1	Download
+ UD_SA_BU_Production_Test_20Oct28_10_46_25	2020-Oct-28	DLC-VA1	i No Errors	1	Download
Usage_17_3_2.txt	2020-Oct-28	Quake	i No Errors	1	Download
Usage_17_3_2.txt	2020-Oct-28	Quake	x Errors (1)	1	Download
Usage_17_3_2.txt	2020-Oct-28	Quake	i No Errors	1	Download

25 | Showing Page 1 of 3 (74 Records) | << >>

Upload Usage Data

Please select the Usage File you wish to upload.

* Usage Data File:

UD_SA_BU_Production_Test_20Nov12_01_01_02_466.tar.gz

5단계. 데이터가 처리되면 Acknowledgment 가 생성됩니다. ACK 파일을 다운로드하고 CSLU에 업로드합니다.

Reports

Report **Usage Data Files** Reporting Policy

Devices can be configured to report the features that they are using.
This usage then determines which licenses are needed, in order to be compliant.

Upload Usage Data... Search by File Name, Virtual Account

Usage Data File	Reported	Virtual Account	Reporting Status	Devices	Acknowledgement
UD_SA_BU_Production_Test_20Oct28_11_11_03	2020-Oct-28	DLC-VA1	No Errors	1	Download

6단계. CSLU의 메뉴 모음에서 ACK 파일을 가져온 다음 이 이미지에 나와 있는 것처럼 로 이동합니다 Product Instances > Upload from Cisco.

CSLU **Product Instances** Edit Help

- Download All Product Instance List Ctrl+S
- Upload Product Instance List Ctrl+U
- Send All To Cisco Ctrl+Enter
- Download All For Cisco Ctrl+Shift+S
- Upload From Cisco Ctrl+Shift+U**

7단계. ACK가 업로드되면 PI로 메시지가 전송됩니다. Alerts(경고) 열에서도 동일한 내용을 확인할 수 있습니다.

CSLU Product Instances Edit Help

Inventory Preferences

Product Instances

Add Single Product Actions for Selected... Refresh Product Instance List

Name	Last Contact ↓	Alerts
UDI_PID:C9500-32QC, UDI_SN:CAT2148L15K	12-Nov-2020 01:10	COMPLETE Usage report acknowledgement to product instance

Items per page: 5 1 - 1 of 1 |< < > >|

SLP - 오프라인 모드

SLP는 전체 오프라인 모드에서도 작업할 수 있습니다. 이는 주로 에어 갭(air-gapped) 네트워크를 위한 것으로, 인터넷 연결을 선호하지 않으며 CSLU를 사용하지 않는 것을 선택합니다. 오프라인 모드에서는 전송이 로 Off 설정됩니다.

Switch(config)#license smart transport off

Same can be verified through, 'show license status'

Switch#show license status

Utility:

Status: DISABLED

Smart Licensing Using Policy:

Status: ENABLED

Data Privacy:

Sending Hostname: yes

Callhome hostname privacy: DISABLED

Smart Licensing hostname privacy: DISABLED

Version privacy: DISABLED

Transport:

Type: Transport Off

Policy:

Policy in use: Merged from multiple sources.

Reporting ACK required: yes (CISCO default)

Unenforced/Non-Export Perpetual Attributes:

First report requirement (days): 365 (CISCO default)

Reporting frequency (days): 0 (CISCO default)

Report on change (days): 90 (CISCO default)

Unenforced/Non-Export Subscription Attributes:

First report requirement (days): 90 (CISCO default)

Reporting frequency (days): 90 (CISCO default)

Report on change (days): 90 (CISCO default)

Enforced (Perpetual/Subscription) License Attributes:

First report requirement (days): 0 (CISCO default)

Reporting frequency (days): 0 (CISCO default)

Report on change (days): 0 (CISCO default)

Export (Perpetual/Subscription) License Attributes:

First report requirement (days): 0 (CISCO default)

Reporting frequency (days): 0 (CISCO default)

Report on change (days): 0 (CISCO default)

Miscellaneous:

Custom Id: <empty>

Usage Reporting:

Last ACK received: Nov 11 15:41:10 2020 EDT

Next ACK deadline: Dec 11 15:41:10 2020 EDT

Reporting push interval: 30 days

Next ACK push check: <none>

Next report push: Dec 07 21:42:30 2020 EDT

Last report push: Nov 07 21:42:30 2020 EDT

Last report file write: <none>

Trust Code Installed: <none>

사용 데이터를 CSSM에 보고하려면 항상 사용 보고서를 파일로 다운로드하여 CSSM에 수동으로 업로드해야 합니다. HA 시스템에서 active는 스탠바이/멤버 디바이스에 대한 사용량을 수집합니다.

To download the usage data from PI -

Switch#license smart save usage unreported file bootflash:<file-name>

Above option 'unreported' is recommended to use. This downloads only the files that are yet to be reported and discard old usage reports, that were Acknowledged.

However, there are other options available for the amount of data that needs to be reported.

For downloading all the available report use option all,
of daya can be specified

Switch#license smart save usage ?

all Save all reports

days Save reports from last n days

rum-Id Save an individual RUM report

unreported Save all previously un reported reports

이제 이 보고서를 CSSM에 수동으로 업로드해야 합니다.

PI에서 데스크톱으로 저장된 사용량 데이터를 내보냅니다.

CSSM Smart Account 페이지에서 로 Report > Usage Data Files > Upload usage data 이동합니다. 팝업 창에서 사용량 보고서를 선택하고 을 클릭합니다upload.

파일이 업로드되면 디바이스가 연결된 올바른 VA를 선택해야 합니다.

Upload Usage Data

Please select the Usage File you wish to upload.

* Usage Data File:

Browse

usage_report_5-nov

Upload Data

Cancel

Select Virtual Accounts



Some of the usage data files do not include the name of the virtual account that the data refers to, or the virtual account is unrecognized.

Please select an account:



Select one account for all files:



Select a virtual account per file:

Ok

Cancel

데이터가 완전히 처리되고 승인이 준비되면 파일을 다운로드하고 PI에 로드합니다.

```
To import the ACK to PI,  
Switch#license smart import bootflash:<file-name>  
Import Data Successful
```

```
Switch#  
Nov 11 20:23:06.783: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy was successfully installed  
Switch#
```

Policy Installed syslog is displayed on console if successful.

Also, the same can be verified using CLI, 'show license all'. The field 'Last ACK received' tells the last TimeStamp when ACK message was received.

```
Switch#show license all  
Load for five secs: 0%/0%; one minute: 1%; five minutes: 0%  
No time source, 16:23:22.294 EDT Wed Nov 11 2020
```

```
Smart Licensing Status  
=====
```

Smart Licensing is ENABLED

```
Export Authorization Key:  
Features Authorized:  
<none>
```

```
Utility:  
Status: DISABLED
```

```
Smart Licensing Using Policy:  
Status: ENABLED
```

Data Privacy:

Sending Hostname: yes
Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:

Type: Transport Off

Miscellaneous:

Custom Id: <empty>

Policy:

Policy in use: Installed On Nov 11 16:23:06 2020 EDT
Policy name: SLP Policy
Reporting ACK required: yes (Customer Policy)
Unenforced/Non-Export Perpetual Attributes:
First report requirement (days): 60 (Customer Policy)
Reporting frequency (days): 60 (Customer Policy)
Report on change (days): 60 (Customer Policy)
Unenforced/Non-Export Subscription Attributes:
First report requirement (days): 30 (Customer Policy)
Reporting frequency (days): 30 (Customer Policy)
Report on change (days): 30 (Customer Policy)
Enforced (Perpetual/Subscription) License Attributes:
First report requirement (days): 0 (CISCO default)
Reporting frequency (days): 90 (Customer Policy)
Report on change (days): 90 (Customer Policy)
Export (Perpetual/Subscription) License Attributes:
First report requirement (days): 0 (CISCO default)
Reporting frequency (days): 90 (Customer Policy)
Report on change (days): 90 (Customer Policy)

Usage Reporting:

Last ACK received: Nov 11 16:23:06 2020 EDT
Next ACK deadline: Dec 11 16:23:06 2020 EDT
Reporting push interval: 30 days
Next ACK push check: <none>
Next report push: Dec 07 21:42:30 2020 EDT
Last report push: Nov 07 21:42:30 2020 EDT
Last report file write: <none>

Trust Code Installed: <none>

License Usage

=====

network-advantage (C9500 Network Advantage):

Description: network-advantage
Count: 1
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: network-advantage
Feature Description: network-advantage
Enforcement type: NOT ENFORCED
License type: Perpetual

dna-advantage (C9500 32QC DNA Advantage):

Description: C9500-32QC DNA Advantage
Count: 1
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: dna-advantage
Feature Description: C9500-32QC DNA Advantage
Enforcement type: NOT ENFORCED
License type: Subscription

Product Information

=====

UDI: PID:C9500-32QC,SN:CAT2148L15K

Agent Version

=====

Smart Agent for Licensing: 5.0.6_rel/47

License Authorizations

=====

Overall status:

Active: PID:C9500-32QC,SN:CAT2148L15K

Status: NOT INSTALLED

Purchased Licenses:

No Purchase Information Available

동작 변경

이러한 변경은 릴리스에 걸쳐 Smart Licensing 기능에서 수행됩니다.

- **트러스트 동기화** - 17.7.1부터 CSLU 및 Offline 메서드와 같이 지원되는 모든 토폴로지의 스위치에 트러스트 코드가 설치됩니다.
- **개인 정보 변경** - 17.7.1부터 17.9.1의 버전 문자열 및 호스트 이름 정보는 개별 개인 정보 설정이 비활성화된 경우 CSSM으로 전송되는 RUM 보고서에 포함됩니다.
- **Account Details**(어카운트 세부사항) - 17.7.1부터 CSSM의 ACK 메시지에는 어카운트 정보 및 SA/VA 세부사항이 포함됩니다.
- **RUM Report Throttling(RUM 보고서 제한)** - 17.9.1부터 PI가 통신을 시작하는 보고 간격의 제한이 적용됩니다. 최소 보고 빈도는 1일로 제한됩니다. 이는 제품 인스턴스가 RUM 보고서를 하루에 두 번 이상 전송하지 않음을 의미합니다.

문제 해결

일반 문제 해결 질문서

시나리오 1: Cisco IOS XE를 초기 릴리스(즉, 16.9.x)에서 업그레이드한 후 일부 프로토콜(즉, HSRP)이 더 이상 작동하지 않습니다.

라이선스 부팅 수준을 확인하여 Cisco IOS XE를 업그레이드하기 전과 동일한지 확인합니다. 라이선스 부팅 수준이 Networking-Essentials로 재설정되었을 수 있습니다. 이는 실패한 프로토콜(즉, HSRP)을 지원하지 않을 수 있습니다.

시나리오 2: "실패 사유: Call Home HTTP 메시지 전송 실패" 또는 "마지막 통신 시도: 보류 중" 메시지가 있는 라이선스 상태

이는 기본 연결 문제와 관련될 수 있습니다. 확인을 해결하려면 다음을 수행합니다.

- CSSM에 연결하기 위한 네트워크 연결 - IP 주소, 경로 등
- 가 ip http client source interface 올바르게 구성되었습니다.
- 시차요. (올바른 클록 시간/영역을 제공하도록 NTP를 구성해야 함)
- 내부 방화벽 컨피그레이션이 CSSM에 대한 트래픽을 차단하는 경우

시나리오 3: 로그 오류 "%SMART_LIC-3-AUTH_RENEW_FAILED: CSSM(Cisco Smart Software Manager)을 사용한 권한 부여 갱신: 등록 후 1년 후에 nil:NilClass"에 대해 정의되지 않은 'each' 메서드가 관찰됩니다.

제품을 다시 등록합니다. CSSM에서 새 토큰 ID를 생성하고 제품 인스턴스를 CSSM에 다시 등록합니다.

시나리오 4: Cisco와의 연결 오류가 없는 경우 오류 메시지 "%SMART_LIC-3-COMM_FAILED: Communications failure".

CSSM에 연결 문제가 없고 PI에 계속 오류가 표시되면 최근 서버 업그레이드로 인해 인증서가 제거되었기 때문일 수 있습니다. 인증서는 두 통신 측의 TLS 인증에 필요합니다. 이 경우 PI에 CLip http client secure-trustpoint SLA-TrustPoint를 구성하고 다시 시도하십시오.

디버그 PI

문제를 해결하기 위해 PI에서 수집된 명령은 다음과 같습니다.

```
show license all
show license tech support
show license eventlog
show license history message
show license tech events
show license rum id all
```

For debugging Trust Installation/Sync -

```
Switch#show license tech support | s Trust
Trust Establishment:
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 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: No Trust Data
 Overall Trust: No ID

For debugging Usage reporting timers/intervals -

Switch#show license tech support | in Utility
 Utility:
 Start Utility Measurements: Nov 11 16:46:09 2020 EDT (7 minutes, 34 seconds remaining)
 Send Utility RUM reports: Dec 07 21:42:30 2020 EDT (26 days, 5 hours, 3 minutes, 55 seconds remaining)
 Process Utility RUM reports: Nov 12 15:32:51 2020 EDT (22 hours, 54 minutes, 16 seconds remaining)

For Collecting all btrace logs for debugging -

Step 1. Switch#request platform software trace rotate all
 Step 2. Switch#show logging process iosrp internal start last boot to-file bootflash:<file-name>

If there are any failues on PULL mode, ensure server SL_HTTP is Acive

```

HTTP server application session modules:
  Session module Name  Handle Status  Secure-status  Description
SL_HTTP                2      Active  Active        HTTP REST IOS-XE Smart License Server
HOME_PAGE              4      Active  Active        IOS Homepage Server
OPENRESTY_PKI         3      Active  Active        IOS OpenResty PKI Server
SSI7FBDE91B27B0-web   8      Active  Active        wsma infra
HTTP_IFS               1      Active  Active        HTTP based IOS File Server
BANNER_PAGE           5      Active  Active        HTTP Banner Page Server
WEB_EXEC              6      Active  Active        HTTP based IOS EXEC Server
SSI7FBDED27A1A8-lic   7      Active  Active        license agent app
SSI7FBDF0BD4CA0-web   9      Active  Active        wsma infra
NG_WEBUI              10     Active  Active        Web GUI
  
```

CSLU 디버그

CSLU에 문제가 있는 경우 CSLU 설치 PC에 있는 이 디렉토리의 로그 파일을 가져와야 합니다.

C:\Users\<user-name>\AppData\Roaming\CSLU\var\logs

관련 참조

- 정책을 사용하여 SL로 마이그레이션 - [정책을 사용하여 레거시 SL/SLR/PLR 라이선스를 SL로 마이그레이션](#)
- 릴리스 정보: [RN-9200](#), [RN-9300](#), [RN-9400](#), [RN-9500](#), RN-9600
- 컨피그레이션 가이드: [Cat9200-CG](#), [Cat9300-CG](#), [Cat9400-CG](#), [Cat9500-CG](#), Cat9600-CG
- 명령 참조: [Cat9200-CR](#), [Cat9300-CR](#), [Cat9400-CR](#), [Cat9500-CR](#), Cat9600-CR
- [기술 지원 및 문서 - Cisco Systems](#)

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.