

Smart Licensing für Catalyst Switching verstehen

Inhalt

[Einleitung](#)

[Zweck](#)

[Smart Licensing mithilfe von Richtlinien](#)

[Terminologie](#)

[Warum diese Veränderung?](#)

[Verfügbare Lizenzen](#)

[Base-Lizenzen](#)

[Add-on-Lizenzen](#)

[Die neuen Komponenten](#)

[Richtlinie](#)

[RUM-Berichte](#)

[Fertigungsablauf für Greenfield-Bereitstellungen](#)

[CSLU](#)

[SLP = Direct Connect](#)

[Lizenzberichte](#)

[Direct Connect - Smart Transport](#)

[Direct Connect - Call-Home-Transport](#)

[SLP - CSLU](#)

[Installation und Konfiguration von CSLU](#)

[CSLU im PUSH-Modus](#)

[Automatische CSLU-Erkennung](#)

[CSLU im PULL-Modus](#)

[PULL-Modus mit RESTAPI](#)

[CSLU - Prozedur für die Einrichtung](#)

[PULL-Modus mit RESTCONF](#)

[CSLU - Prozedur für die Einrichtung](#)

[PULL-Modus mit NETCONF](#)

[CSLU - Prozedur für die Einrichtung](#)

[CSLU im getrennten Modus](#)

[SLP = Offline-Modus](#)

[Verhaltensänderungen](#)

[Fehlerbehebung](#)

[Allgemeiner Fragebogen zur Fehlerbehebung](#)

[PI debuggen](#)

[CSLU debuggen](#)

[Verwandte Referenzen](#)

Einleitung

In diesem Dokument wird die Smart Licensing-Funktion unter Verwendung der Richtlinie für Catalyst Switching-Plattformen und der unterstützten Bereitstellung beschrieben.

Zweck

Ab den Versionen 17.3.2 und 17.4.1, ab Cisco IOS® XE unterstützen alle Catalyst Switching-Plattformen der Produktfamilie für Cat9k ein neues Lizenzierungsmodell von SLP (Smart Licensing using Policy). In diesem Dokument werden die verschiedenen unterstützten Modelle für die Implementierung und Bereitstellung von SLP vorwiegend für neuartige Bereitstellungen erläutert.

Smart Licensing mithilfe von Richtlinien

Bei SLP sind alle Lizenzen sofort einsatzbereit. Die früheren Konzepte, der Evaluierungsmodus, die Registrierung und die Reservierung gehen mit SLP einher. Bei SLP dreht sich alles um das Reporting der Lizenzen und ihrer Nutzung. Die Lizenzen werden immer noch nicht erzwungen, und die Lizenzierungsstufen bleiben unverändert. Für Catalyst Switch-Plattformen gibt es außer der Lizenz HSECK9 keine exportkontrollierten Lizenzstufen. Die einzige Änderung betrifft die Informationen zur Lizenznutzung und -nachverfolgung. In diesem Abschnitt werden die Terminologie, die Gründe für die Änderungen, die neuen Komponenten im Lieferumfang von SLP, CSLU (Cisco Smart Licensing Utility) und der Ablauf der Produktbestellung im Detail beschrieben.

Terminologie

- CSSM oder SSM - Cisco Smart Software Manager
- SA - Smart Account
- VA - Virtuelles Konto
- SL - Smart Licensing
- PLR = Permanent License Reservation
- SLR = Smart License Reservation
- PIDs - Produkt-IDs
- SCH = Smart Call Home
- PI - Produktinstanzen
- CSLU - Cisco Smart Licensing Utility
- RUM = Resource Utilization Measurement
- Bestätigung - Bestätigung
- UDI = Unique Device Identification - PID + SN
- SLP = Smart Licensing using Policy

Warum diese Veränderung?

Mit der Einführung des Smart Licensing-Modells `trust and verify` unterstützt Cisco verschiedene

Bereitstellungsmechanismen zur Nachverfolgung und Meldung der Lizenznutzung an den CSSM. Es war jedoch nicht einfach für alle Arten von Bereitstellungen zu adaptieren - es gab Feedback und Anforderungen aus der Praxis, um die Einführung von Smart Licensing zu erleichtern. Zu den Herausforderungen gehören:

- Mit SL-Registrierung - Geräte müssen immer mit dem Internet verbunden sein, um CSSM zu erreichen, was bei der Bereitstellung Probleme bereitet.
- Standortbasierte Satellitenserver verursachen höhere Bereitstellungs- und Wartungskosten.
- SLR unterstützt nur Air-Gap-Netzwerke.
- Alle Bereitstellungen, die keines dieser Modelle unterstützen, müssen ihre Geräte auch nach dem Erwerb der Lizenzen im Unregistered/Eval expired Status ausführen.

SLP wird eingeführt, um solche Anfragen aus dem Feld zu vereinfachen. Bei SLP müssen Sie das Produkt nicht bei CSSM registrieren. Alle erworbenen Lizenzstufen sind sofort einsatzbereit. Dadurch wird die Day-0-Reibung des Geräts aufgehoben. SLP minimiert außerdem den Workflow bei der Lizenzbereitstellung und reduziert die Anzahl überflüssiger Berührungspunkte. Es ist nicht erforderlich, das Gerät rund um die Uhr mit dem CSSM zu verbinden. SLP bietet außerdem die Möglichkeit, Lizenzen im getrennten Netzwerk zu verwenden, die Lizenznutzung offline zu melden und die Lizenz in Intervallen zu melden, die von den Kundenrichtlinien bestimmt werden.

Verfügbare Lizenzen

Die verfügbaren Softwarefunktionen fallen unter Basis- oder Zusatzlizenzen. Base-Lizenzen sind unbefristete Lizenzen, und Add-on-Lizenzen sind mit Laufzeiten von drei, fünf und sieben Jahren erhältlich.

Base-Lizenzen

- Grundlagen des Netzwerks
- Netzwerkvorteil
- HSECK9

Add-on-Lizenzen

- Grundlagen der DNA
- DNA-Vorteil



Hinweis: HSECK9 ist eine exportkontrollierte Lizenz. Zur Aktivierung der Lizenz und der entsprechenden Funktion ist ein SLAC erforderlich.

Die neuen Komponenten

Richtlinie

Die Richtlinie legt fest, wie das Standardverhalten für die PI aussehen muss. Sie enthält die Attribute für die Berichterstattungsanforderungen für die Lizenzierung für verschiedene Lizenzstufen und -bedingungen. Die Richtlinie legt außerdem fest, ob die ACK-Nachricht für jeden an CSSM gesendeten Bericht an PI zurückgesendet werden muss. Die Richtlinie enthält auch den Namen der Richtlinie und den Zeitpunkt, an dem die Richtlinie installiert wird. Die Standardrichtlinie von Cisco ist allgemein gültig und gilt für alle Catalyst-Produkte. Die vom Kunden definierte Richtlinie ist jedoch auch zulässig, wenn Sie unterschiedliche Berichtsintervalle und ACK-Antwortausfälle wünschen.


Die Richtlinie kann bei verschiedenen Gelegenheiten auf einem PI installiert werden.

- Standard-Policy in der Software vorhanden
- Installierte Richtlinien von Cisco Manufacturing
- Richtlinie über ACK-Antwort installiert
- Manuelle Installation der Richtlinie über CLI
- Richtlinie wird mit Yang-Anforderung verschoben

Diese Ausgabe zeigt, wie eine Standardrichtlinie aussieht.

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)

 **Hinweis:** Eine Richtlinie kann nicht gelöscht werden, wenn Sie eine Systemkonfiguration löschen/ändern, nvram löschen oder den Flash-Speicher formatieren: filesystem. Die Richtlinie wird auf den Cisco Standard beim **intelligenten Zurücksetzen der Lizenz auf die Werkseinstellungen festgelegt**.

RUM-Berichte


RUM sind von der PI generierte und gespeicherte Nutzungsberichte. Die ISO19770-4 Standard-RUM-Berichte sind für SLP abgeschlossen. In den RUM-Berichten werden alle in der PI vorgenommenen Änderungen an der Lizenznutzung als Berichtsdateien gespeichert. Die Nutzungsdaten für die einzelnen Lizenzebenen werden in separaten RUM-Berichten gespeichert. RUM-Berichtsmessungen werden in regelmäßigen Abständen erfasst und in PI gespeichert. Bei jeder Änderung der Lizenznutzung der PI oder bei Auslösung einer Nutzungsmeldung bzw. bei Erreichen der maximalen Größe/Samples werden neue RUM-Reports für alle Lizenzstufen generiert. In anderen

Fällen können die vorhandenen RUM-Berichte mit einem neuen Beispiel und einem aktualisierten Zeitstempel überschrieben werden. Die standardmäßige Messung im Dienstprogramm für den RUM-Bericht erfolgt alle 15 Minuten. In jedem Berichtsintervall werden RUM-Berichte an Cisco CSSM gesendet.

Alle RUM-Berichte werden vom PI signiert und vom CSSM verifiziert. Wenn CSSM die RUM-Berichtsdaten von der PI empfängt, wird der Bericht validiert, der Zeitplan für die Lizenznutzungsänderung überprüft und die CSSM-Daten entsprechend aktualisiert. Anschließend bestätigt CSSM die Antwort über die ACK-Antwortnachricht an die PI.

RUM-Berichte können auf verschiedene Weise an den CSSM gesendet werden:

- PI sendet RUM-Berichte direkt nach dem Berichtsintervall an CSSM.
- PI überträgt den RUM-Bericht an die CSLU.
- Das CSLU ruft in regelmäßigen Abständen RUM-Berichte von PI über RESTAPI und YANG Modelle ab.
- RUM-Berichte werden über die Kommandozeile manuell auf der PI gespeichert und manuell in CSSM hochgeladen.

 **Hinweis:** RUM-Berichte können nicht gelöscht werden, wenn Sie eine Systemkonfiguration löschen/ändern, nvram löschen oder den Flash-Speicher formatieren: filesystem. Alle RUM-Berichte können bei "license smart factory reset" aus PI entfernt werden.



Hinweis: Das Standard-Berichtsintervall beträgt 30 Tage.

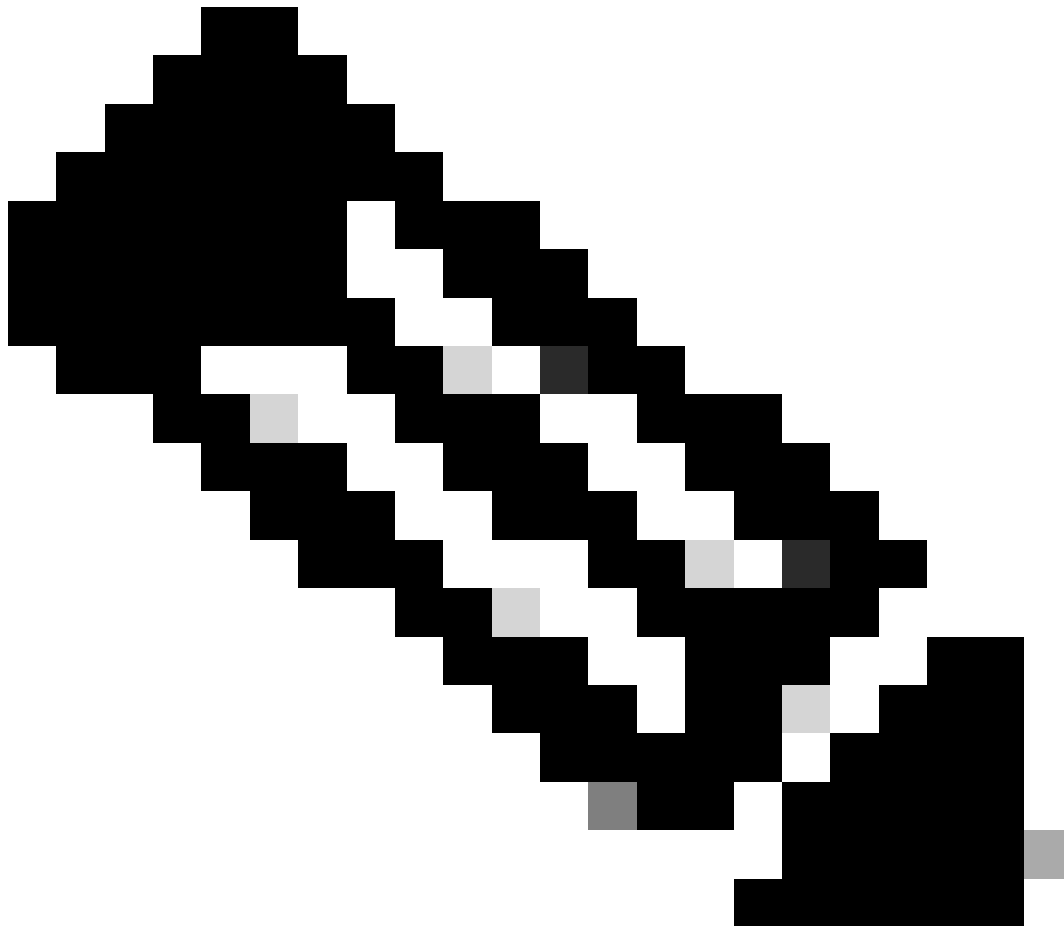
Fertigungsablauf für Greenfield-Bereitstellungen

Sobald eine neue Produktbestellung bei Cisco CCW (Cisco Commerce Workspace) aufgegeben wurde, durchläuft die PI den vom Produktionsteam durchgeführten Workflow. Dies erleichtert die sichere Unterzeichnung von RUM-Berichten und beseitigt die Day-0-Friction bei der Registrierung der PI. Sobald die Bestellung aufgegeben wurde, werden alle vorhandenen SA/VA oder neu erstellten SA/VA mit dem Produkt verknüpft. Das Cisco Produktionsteam kümmert sich um diese Abläufe, bevor es das Produkt an Sie versendet:

- Installieren Sie den Vertrauenscode auf dem Gerät. Die Signatur des vertrauenswürdigen Codes wird basierend auf der Geräte-UDI installiert. Es wird auf jedem Produkt installiert.

- Einkaufscode installieren: Hier erhalten Sie Informationen zu den Lizenzstufen, die zusammen mit dem Produkt erworben wurden. Es wird auf jedem Produkt installiert.
- SLAC - Smart License Auth Code - Nicht zutreffend für Catalyst Plattformen.
- Richtlinie installieren - Standard- oder benutzerdefinierte Richtlinie auf Grundlage Ihrer Eingabe.
- Melden Sie die Lizenznutzung an CSSM - SA/VA.

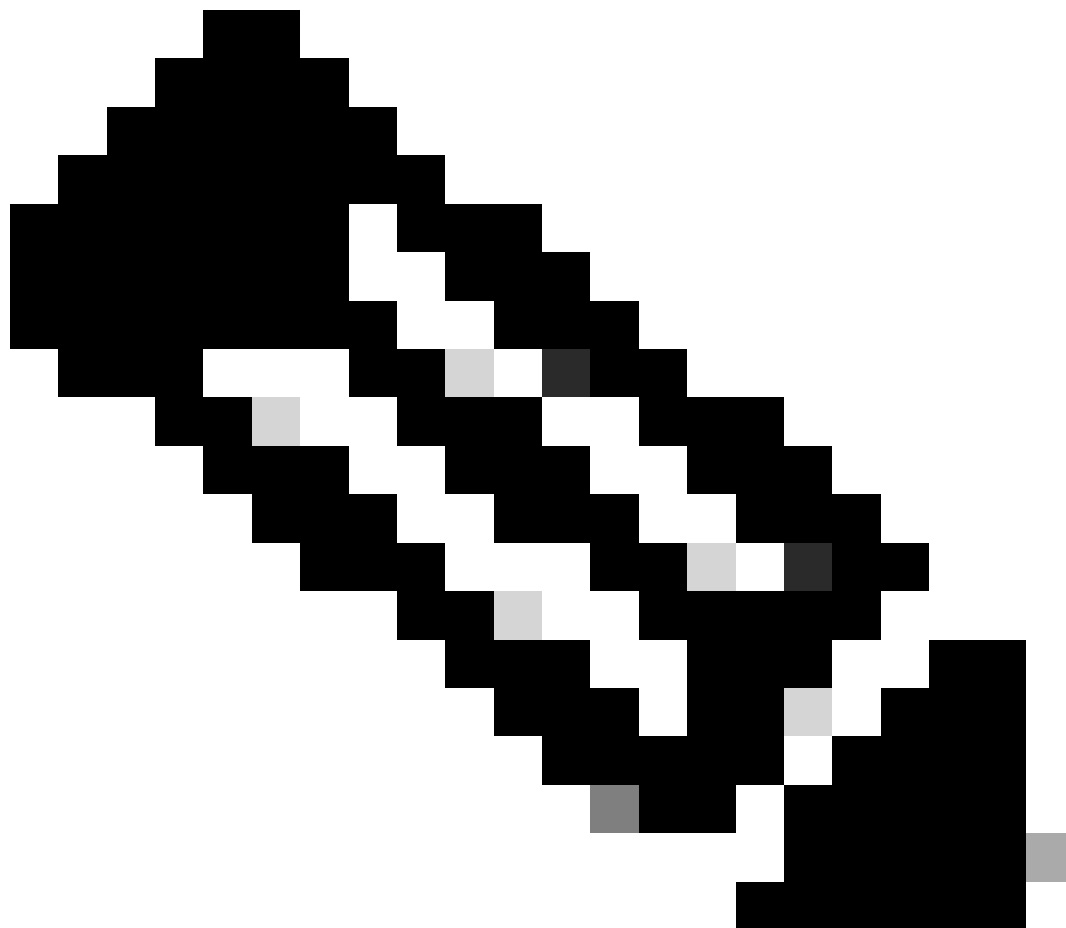
 **Hinweis:** Mit der Version 17.3.3 wird dieser Fluss für alle Catalyst Switching-Plattformen mit Ausnahme von C9200/C9200L befolgt.



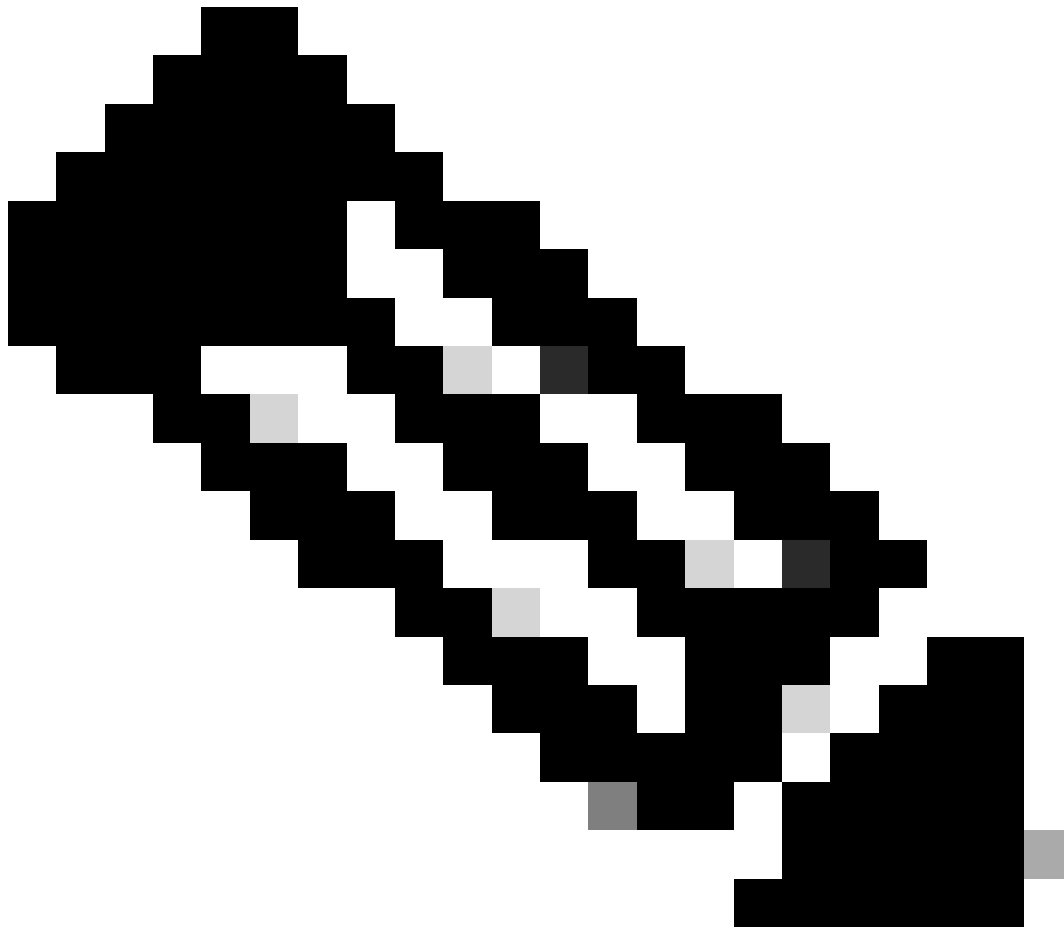
Hinweis: Der Vertrauenscode ist nur in der Fertigung mit der Version 17.7.1 für alle Catalyst Switching-Plattformen mit Ausnahme von C9200/C9200L installiert.

CSLU

SLP bringt ein neues einfaches, aber leistungsstarkes Tool CSLU. CSLU ist ein GUI-basiertes Tool, das unter Windows 10 oder Linux auf Basis von RHEL/Debian läuft. Das CSLU, das auf Ihrem lokalen privaten Netzwerk ausgeführt werden kann, ist dafür verantwortlich, die RUM-Ports von den PIs zu sammeln, die mit dem CSSM verbunden sind. CSLU muss so bereitgestellt werden, dass RUM-Berichte über PIs im lokalen Netzwerk gesammelt und regelmäßig über das Internet an den CSSM gesendet werden können. CSLU ist ein einfaches Tool, das nur die Details der UDIs der bereitgestellten Geräte anzeigt. Alle Lizenzverwendungsdaten für PIs, gekaufte Lizenzen und nicht verwendete Lizenzen im Pool werden nur in SA/VA von CSSM angezeigt, was Sie überprüfen müssen. Es ist leistungsstark, da es Nutzungsberichte von bis zu 10.000 PIs erfassen kann. CSLU ist auch dafür verantwortlich, die ACK-Nachrichten vom CSSM an PI zurückzugeben.



Hinweis: Detaillierte Informationen zur Konfiguration und den unterstützten Betriebsmodi von CSLU finden Sie im Abschnitt "CSLU-basierte Topologie".

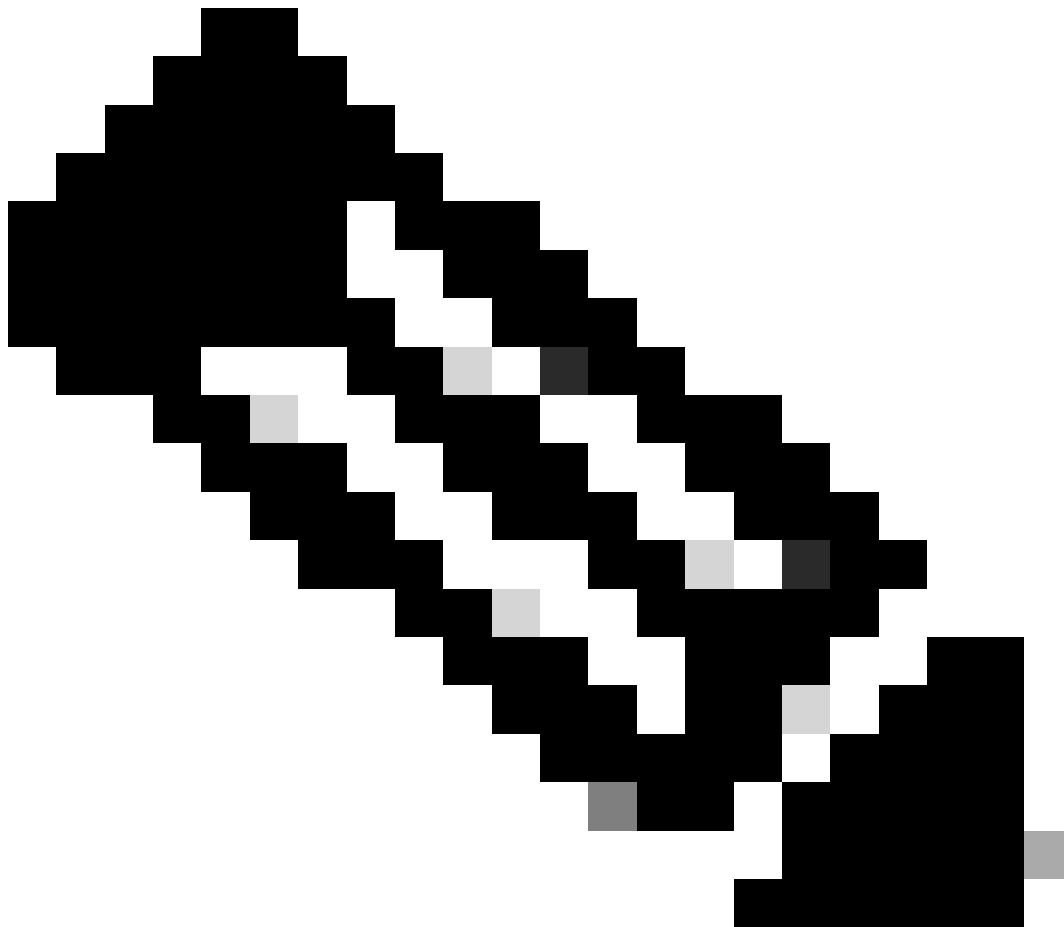
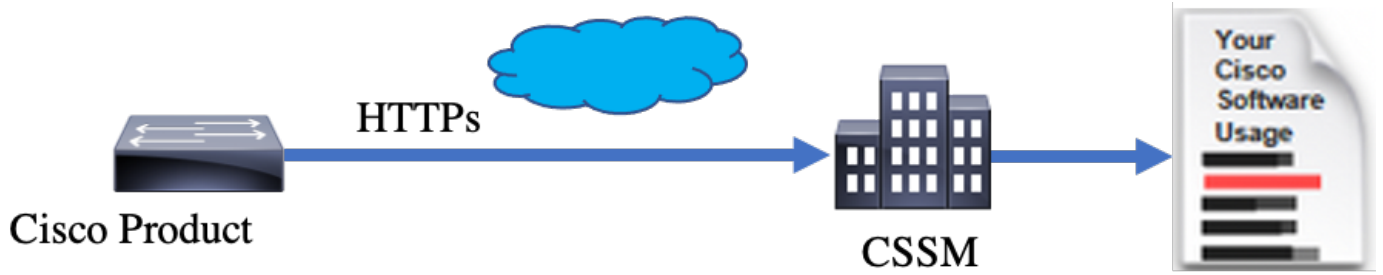


Hinweis: Ab Version 17.7.1 wird die Linux-Version von CSLU unterstützt.

SLP = Direct Connect

Bei einem werkseitig ausgelieferten Produkt ist der Standardtransportmodus auf CSLU konfiguriert. Wenn Sie die Direct Connect-Methode verwenden möchten, müssen Sie den Transportmodus je nach Anforderung in Call-Home oder SMART ändern. Die Hauptanforderung für die Direct Connect-Topologie ist die Verfügbarkeit einer Internetverbindung, damit CSSM erreichbar ist. Darüber hinaus muss sichergestellt werden, dass für die Verbindung mit dem CSSM die erforderlichen L3-Konfigurationen, DNS- und Domänenkonfigurationen im Gerät

vorhanden sind.




Hinweis: Smart Transport ist die empfohlene Transportmethode, wenn Sie direkt eine Verbindung mit CSSM herstellen.

Lizenzberichte

Bei einer Direct Connect-Topologie werden die RUM-Berichte direkt an CSSM gesendet. Für Lizenzberichte muss auf dem Gerät ein erfolgreicher Vertrauenscode installiert sein. Der Vertrauenscode wird von der Cisco Fertigung auf dem Gerät installiert, bevor es versendet wird. Sie können den Vertrauenscode auch auf dem Gerät installieren.

Der Vertrauenscode ist eine Tokenzeichenfolge aus CSSM auf der Seite Virtuelles Konto - Allgemein. Der Vertrauenscode kann über die CLI installiert werden.

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

 **Hinweis:** Alle Optionen müssen für HA oder Stacking-Back-System verwendet werden. Bei einem Standalone-Gerät kann die lokale Option verwendet werden.

```
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

Sobald der Vertrauenscode erfolgreich installiert wurde, kann die PI die Verwendung direkt an CSSM melden. Diese Bedingungen führen zu einer Lizenzmeldung:

- Erfolgreiche Installation des Vertrauenscodes
- Für jedes Standard-Berichtsintervall
- Neuladen/Hochfahren des Geräts
- Ein Switchover
- Hinzufügen oder Entfernen von Stapелеlementen
- Manueller Trigger der Lizenzsynchronisierung

Die Lizenzberichterstattung für CSSM kann über die folgende CLI ausgelöst werden:

Switch#license smart sync all

Im Abschnitt Usage Reporting (Nutzungsberichte) in der show license status werden die Zeitpläne für die letzte erhaltene ACK, die nächste ACK-Frist, die nächste Berichtsweiterleitung und die letzte Berichtsweiterleitung angezeigt.

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

Bei Verwendung von SMART Transport sind dies in einer Direct Connect- oder Direct Cloud Access-Topologie die erforderlichen Konfigurationen auf dem Gerät.

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
```

!

Direct Connect - Call-Home-Transport

Wenn in einer Topologie mit Direktverbindung oder direktem Cloud-Zugriff Call-Home-Transport verwendet wird, sind dies die erforderlichen Konfigurationen auf dem Gerät.


Configure the desired Transport mode using below CLI.

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

Running config on Smart Transport Mode:

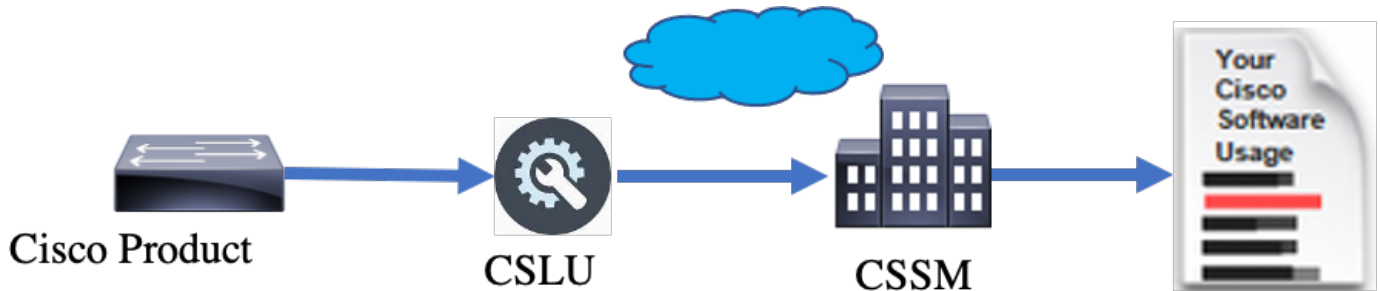
!

```
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  
!
```

 **Hinweis:** Standardmäßig wird die Zieladresse für Call-Home als CSSM-URL konfiguriert. Dies kann in der show run all Konfiguration überprüft werden.

SLP - CSLU

Der CSLU-Modus ist der Standardtransportmodus auf den werkseitig gelieferten Geräten mit der Version 17.3.2 oder höher. Wenn Sie von abgelaufenen Eval/Eval-Lizenzen migrieren, lautet der Transportmodus nach dem Wechsel auf SLP außerdem CSLU. In der CSLU-basierten Topologie befindet sich die CSLU zwischen PI und CSSM. CSLU vermeidet, dass Benutzer nicht über eine direkte Netzwerkverbindung mit der Cisco Cloud - CSSM verfügen. CSLU kann lokal in einem privaten Netzwerk ausgeführt werden und Nutzungsberichte von allen zugehörigen PIs herunterladen. Die Nutzungsberichte werden lokal auf dem Windows-PC gespeichert, bevor sie über das Internet an den CSSM gesendet werden. CSLU ist ein leichtes Tool. Es wird nur die Liste der zugehörigen PIs angezeigt, und es kann anhand von UDIs identifiziert werden. CSLU kann die Redundanzinformationen von PI oder Lizenzstufen oder Lizenznutzung nicht anzeigen oder enthalten.

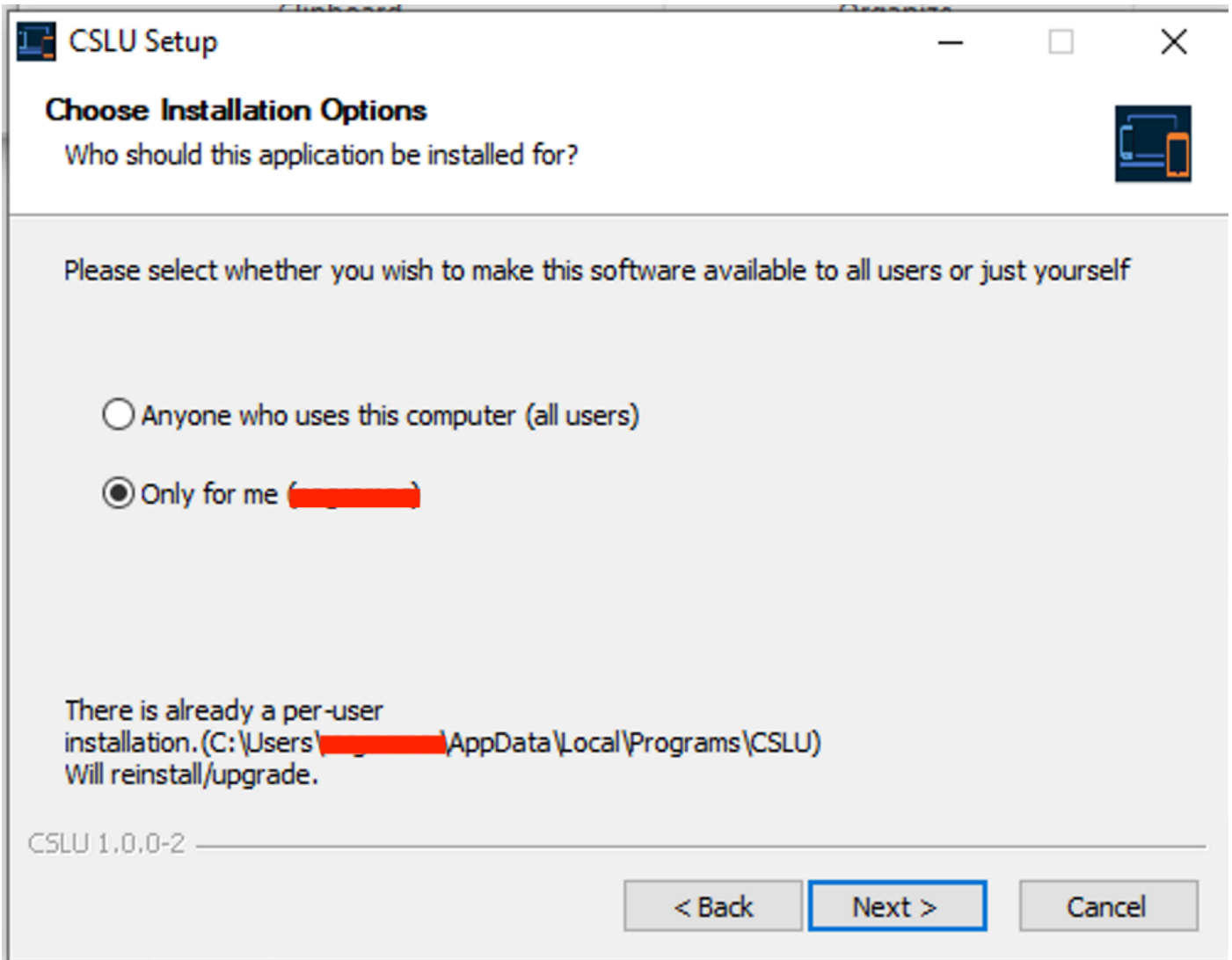


Installation und Konfiguration von CSLU

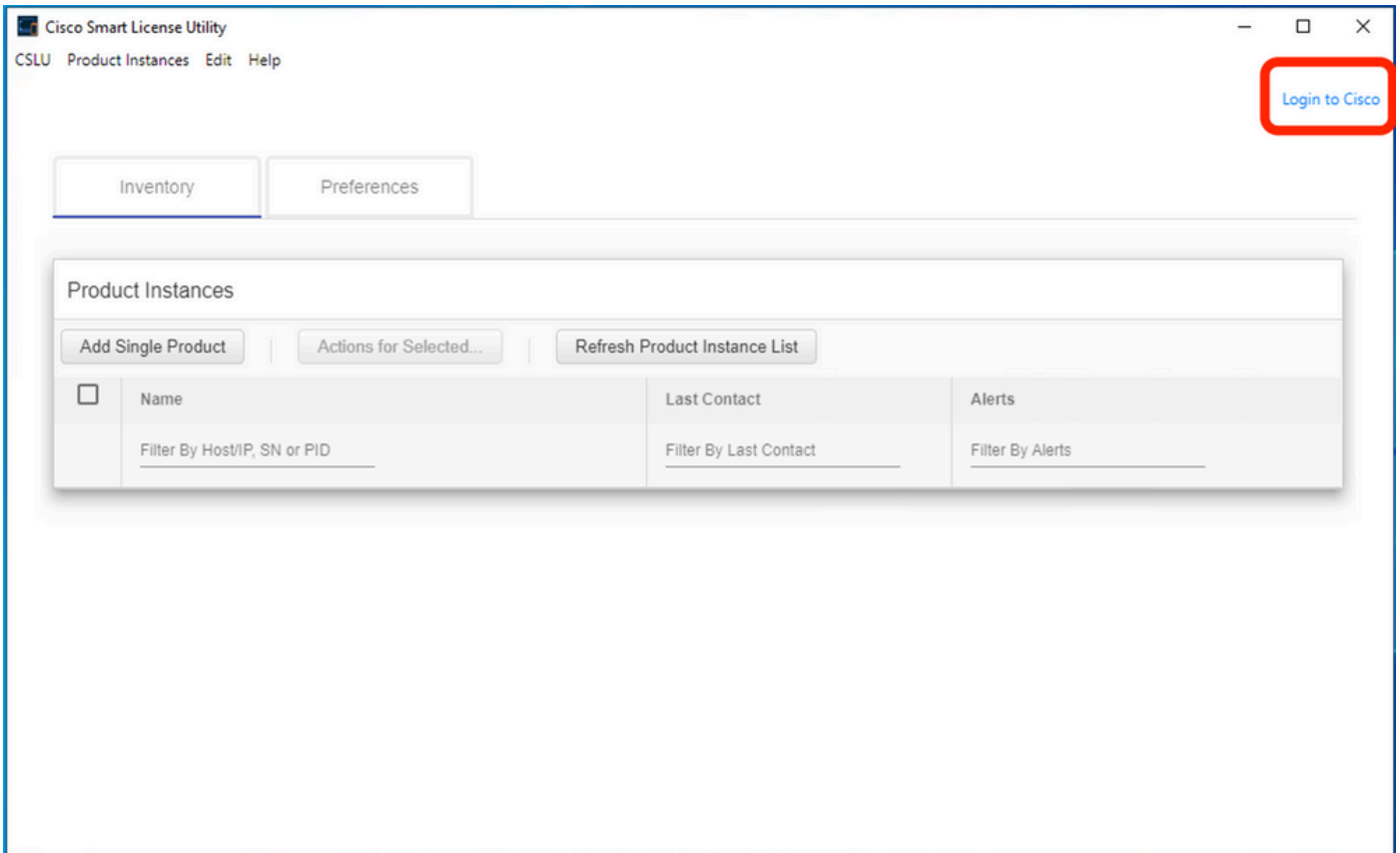
Das CSLU-Tool wird auf Windows 10-Computern installiert und betrieben. Die Software ist im CCO zum Download und kostenlosen Gebrauch erhältlich. Nach der Installation des Tools können die Schnellstartanleitung/das Benutzerhandbuch vom Menü Hilfe heruntergeladen werden. Navigieren Sie zu Help > Download Help Manual.

Bei der Installation von CSLU müssen Sie die Lizenzvereinbarung akzeptieren.

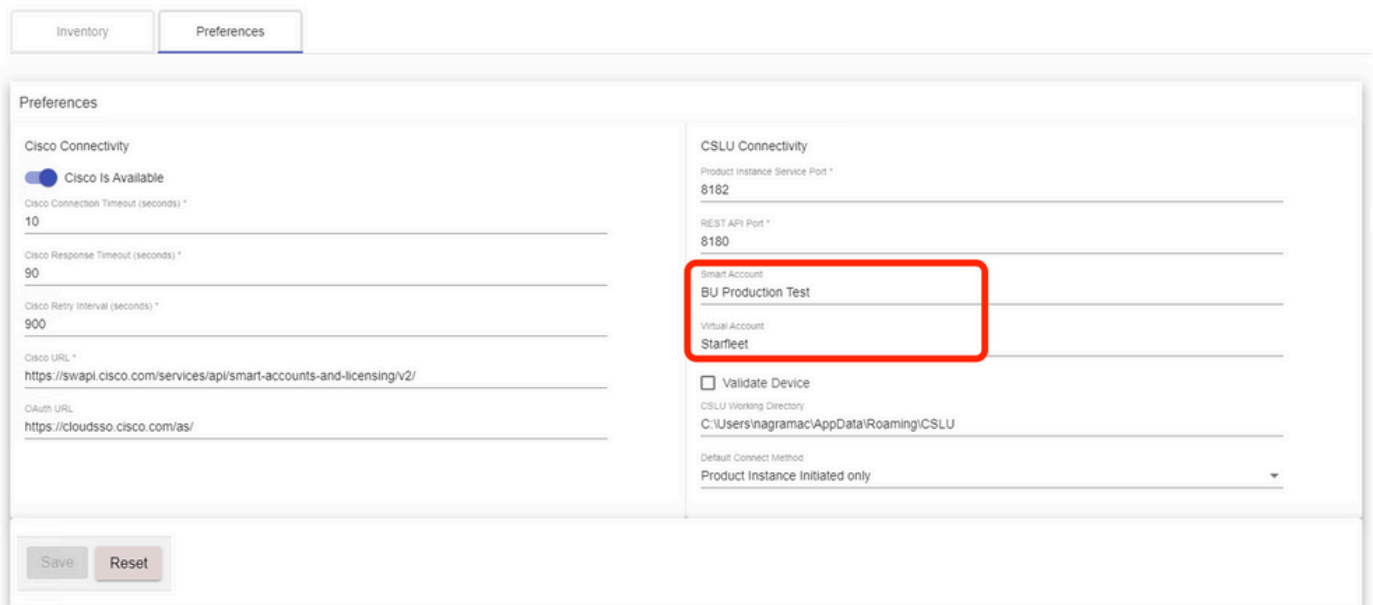
Es wird empfohlen, die Anwendung nur für den aktuellen Benutzer und nicht für alle Benutzer zu installieren, die am Computer arbeiten. Wenn bereits eine frühere Version von CSLU auf dem PC vorhanden ist, empfiehlt es sich, diese zuvor zu deinstallieren. Trotzdem sorgt die Neuinstallation dafür, dass die Software aufgerüstet wird.



Melden Sie sich nach der Installation bei Cisco an, und verwenden Sie die Anmeldeoption oben rechts in der Anwendung. Hierfür werden Ihre CEC-Anmeldeinformationen verwendet. Durch die Anmeldung wird eine Vertrauensstellung zwischen CSLU und CSSM hergestellt.



Nachdem Sie sich bei Cisco angemeldet haben, stellen Sie sicher, dass die SA- und VA-Details im Dropdown-Menü im Bereich "Voreinstellungen" des Tools korrekt ausgewählt sind. Speichern Sie die Konfigurationen.



Registerkarte "Geplant" auf CSLU - Über die Registerkarte "Geplant" auf CSLU können Sie Folgendes konfigurieren:

- CSSM für verfügbare Daten abfragen: Zeigt die Job-Timings, die letzte Pull-Zeit und die nächste Pull-Zeit für Daten von CSSM an.
- Bereinigen gelöschter Daten - Entfernt alle gelöschten Daten aus dem CSLU-Datenspeicher. Sie kann auch manuell ausgelöst werden.

- Gerätedaten abrufen: Löst den CSLU-Abrufmodus aus.

Scheduler				
Refresh Job Information				
System Jobs				
Name	Status	Next Execution Time	Start	
Poll CSM 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	

CSLU im PUSH-Modus

CSLU wird standardmäßig im PUSH-Modus ausgeführt. Im PUSH-Modus sendet der PI die Nutzungsberichte in regelmäßigen Abständen an die CSLU. Vom Gerät aus müssen Sie sicherstellen, dass das L3-Netzwerk über CSLU erreichbar ist. Damit die PI mit CSLU kommunizieren kann, muss die IP-Adresse des Windows-Computers, auf dem CSLU ausgeführt wird, konfiguriert werden.

```
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

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>

Berichte werden unter den folgenden Bedingungen von PI an die CSLU gesendet:

- Bei jedem Standard-Berichtsintervall
- Neuladen/Hochfahren des Geräts
- Beim Switchover
- Hinzufügen oder Entfernen von Stapelementen
- Manueller Auslöser der Lizenz-Synchronisierung

In CSLU werden auf der Inventarseite die Geräte aufgeführt, die aktuell mit CSLU verknüpft sind. Die Geräte in der Liste können mithilfe der UDI identifiziert werden. Die Geräte können anhand der PID oder SN aus der Liste gefiltert werden, um bestimmte Geräte zu identifizieren.

Die CSLU-Bestandsseite hat noch zwei weitere Spalten:

- Die Spalte **Letzter Kontakt** - Zeigt den letzten Zeitstempel an, wenn sich der Status der Berichterstellung geändert hat.
- Die **Warnmeldungsspalte** - Zeigt den aktuellen Berichtsstatus der PI an.

Sobald der PI den Bericht an die CSLU sendet, erstellt die CSLU den PI-Eintrag in CSSM. Der TS für den letzten Kontakt sowie der Status der Warnungen werden aktualisiert.

Inventory		Preferences	
Product Instances			
Add Single Product		Refresh Product Instance List	
Name	Last Contact	Alerts	
Filter By Host/IP, SN or PID	Filter By Last Contact	Filter By Alerts	
<input type="checkbox"/> UDI_PID:C9500-32QC; UDI_SN:CAT2148L15K	08-Nov-2020 06:37	COMPLETE: Usage report from product instance	
<input type="checkbox"/> UDI_PID:C9500-24Y4C; UDI_SN:CAT2344L4GH	03-Nov-2020 18:27	COMPLETE: Usage report acknowledgement to product instance	
Items per page: 5 1 - 2 of 2 < < > >			

Inventory		Preferences	
Product Instances			
Add Single Product		Refresh Product Instance List	
Name	Last Contact	Alerts	
Filter By Host/IP, SN or PID	Filter By Last Contact	Filter By Alerts	
<input type="checkbox"/> UDI_PID:C9500-32QC; UDI_SN:CAT2148L15K	08-Nov-2020 06:37	COMPLETE: Usage report uploaded to CSSM	
<input type="checkbox"/> UDI_PID:C9500-24Y4C; UDI_SN:CAT2344L4GH	03-Nov-2020 18:27	COMPLETE: Usage report acknowledgement to product instance	
Items per page: 5 1 - 2 of 2 < < > >			

CSSM verarbeitet die von CSLU gesendeten Berichte und fügt die Produktinstanz in CSSM hinzu bzw. aktualisiert sie je nach Lizenznutzung. Sobald der CSSM das Datum verarbeitet und aktualisiert, sendet er die ACK-Nachricht an die CSLU zurück. Die CSLU wiederum speichert die Nachricht und leitet sie an die PI weiter.

Die ACK-Nachricht besteht aus:

- Bestätigung aller gesendeten Berichte
- Richtlinie
- Treuhandcode


Wenn Ihnen im CSSM eine neue Richtlinie zur Verfügung steht, wird sie jetzt auch auf die PI aktualisiert. Wenn die Richtlinie unverändert bleibt, wird sie an die PI weitergegeben.



Hinweis: Wenn gemäß Ihrer Richtlinie keine ACK-Meldungsberichte erforderlich sind, wird die ACK-Meldung nicht gesendet.

Die Warnmeldungsspalte kann einen der folgenden Status haben:

- Nutzungsbericht aus Produktinstanz
- An Cisco hochgeladener Nutzungsbericht
- Synchronisierungsanforderung von Produktinstanz
- Synchronisierungsanforderung in CSSM hochgeladen
- Bestätigung von CSSM empfangen
- Bestätigung des Nutzungsberichts für die Produktinstanz

 **Hinweis:** In CSLU auf einem HA-System wird der Eintrag immer nur für UDI des Aktiven angezeigt. Nur in CSSM sind alle UDIs für einzelne Geräte im System aufgeführt.

Automatische CSLU-Erkennung

Zur Unterstützung skalierbarer Bereitstellungen mit minimalen Konfigurationen wird die automatische Erkennung der CSLU unterstützt. Das bedeutet, dass Sie die IP-Adresse/URL der CSLU nicht speziell konfigurieren müssen. Um dies zu erreichen, müssen Sie nur einen Eintrag zu ihrem DNS-Server hinzufügen. Dadurch kann das Gerät, das den Transportmodus als CSLU hat (dies ist die Standardeinstellung), automatisch CSLU erkennen und Berichte senden.

Hier einige Punkte:

- Erstellen Sie einen Eintrag im DNS-Server. Die IP-Adresse der CSLU muss dem Namen `cslu-local` zugeordnet werden.
- Stellen Sie sicher, dass die Namenserver- und DNS-Konfigurationen auf dem Gerät vorhanden sind, um erreichbar zu sein.

Dadurch können die Geräte im Netzwerk ohne zusätzliche Konfigurationen in regelmäßigen Abständen auf die CSLU zugreifen und RUM-Berichte senden.

CSLU im PULL-Modus

Im PULL-Modus initiiert die CSLU den Prozess zum Abrufen der RUM-Berichte von den Geräten. Hier werden die Gerätedetails zur CSLU hinzugefügt, und die CSLU ruft die Daten auf allen hinzugefügten Geräten in regelmäßigen Abständen ab. Der PULL aus der CSLU kann auch manuell ausgelöst werden. Die CSLU sendet wiederum den RUM-Bericht an den CSSM, und ACK-Nachrichten, die vom CSSM zurückgesendet werden, werden an die PI gesendet. Der PULL-Modus wird auf drei verschiedene Arten unterstützt: RESTAPI, NETCONF und RESTCONF.

PULL-Modus mit RESTAPI

Für den PULL-Modus RESTAPI sind folgende Konfigurationen vom Gerät und von der CSLU erforderlich:

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  
!
```



Hinweis: Der Benutzer muss über Zugriffsrechte der Stufe 15 verfügen.

CSLU - Prozedur für die Einrichtung

CSLU muss beim CSSM angemeldet sein, damit Berichte automatisch synchronisiert werden können.

Schritt 1: Add Single Product Wählen Sie auf der Inventarseite die Option aus.

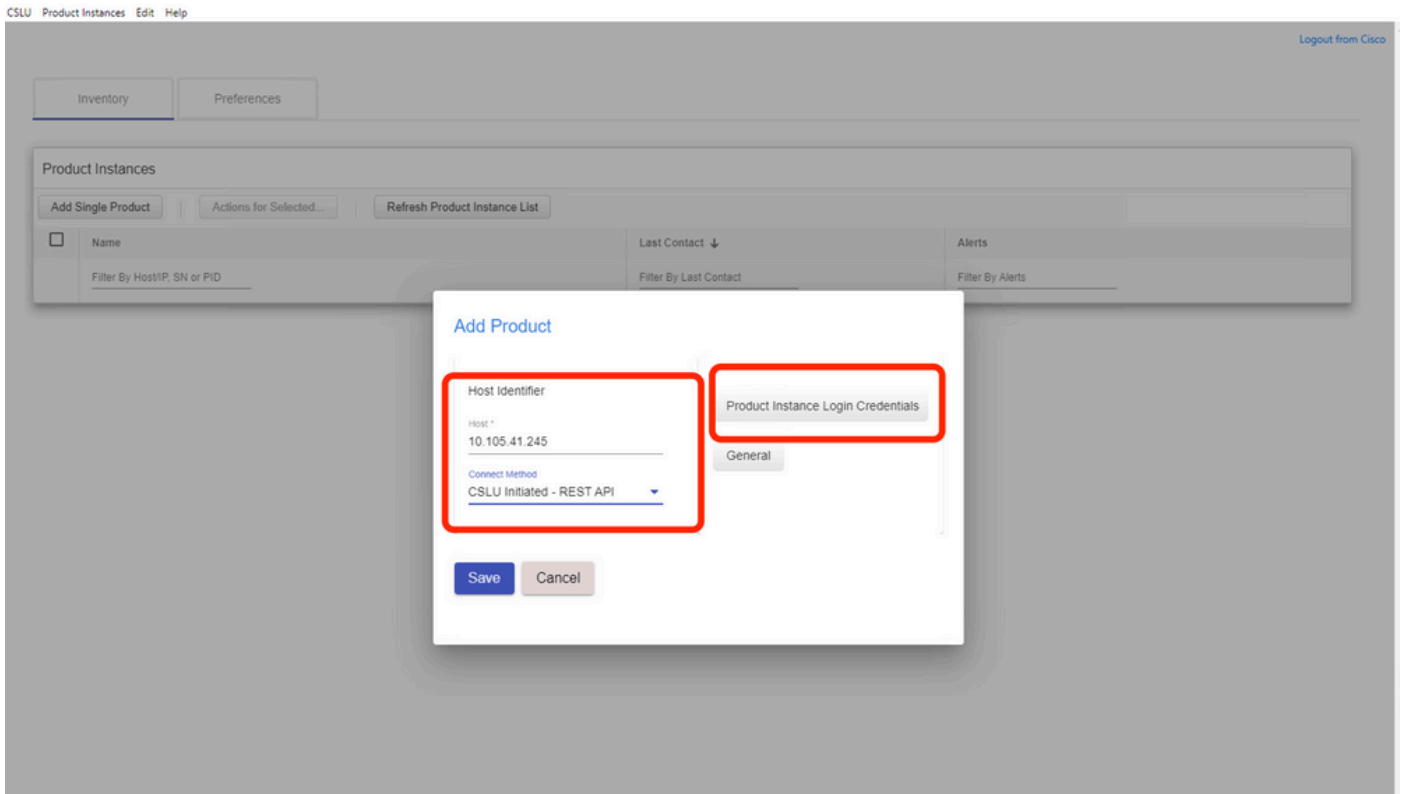
Schritt 2: Geben Sie die Geräte-IP ein.

Schritt 3: Wählen Sie die Verbindungsmethode als RestAPI aus.

Schritt 4: Wählen Sie Anmeldeinformationen für Produktinstanzen aus.

Schritt 5: Geben Sie die Anmeldeinformationen des Benutzers mit Priv. 15-Zugriff ein.

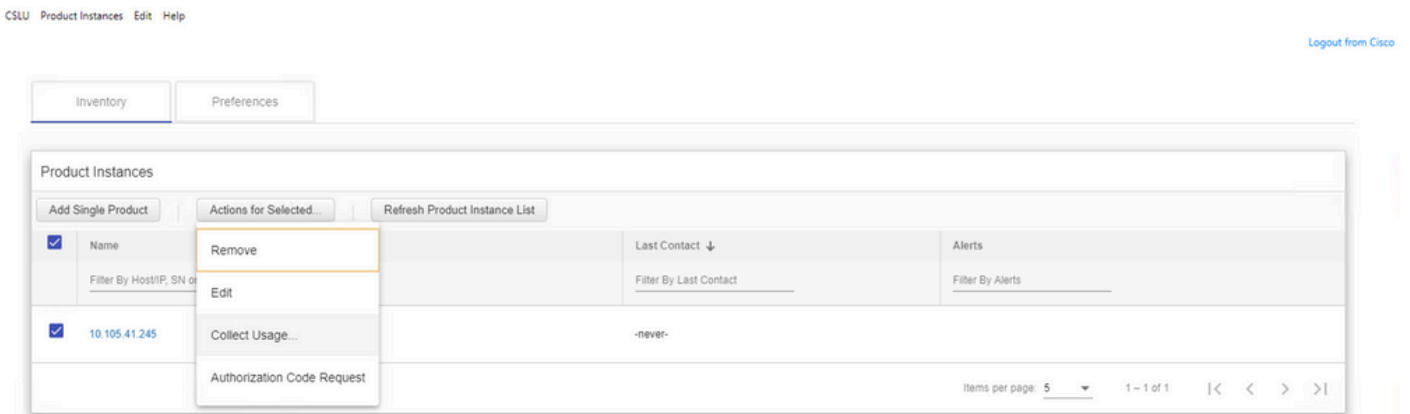
Schritt 6: Speichern der Konfigurationen



Das Gerät wird mit einer einzigen IP-Adresse im Namensfeld hinzugefügt.

Wählen Sie das Gerät aus, und navigieren Sie zu Actions for Selected > Collect Usage.

Sobald die Nutzungsdaten erfolgreich erfasst wurden, wird das Feld Name auf die UDI der PI aktualisiert, und der Zeitstempel wird ebenfalls aktualisiert. Das Warnungsfeld gibt den aktuellen Status wieder.



Inventory		Preferences	
Product Instances			
<input type="button" value="Add Single Product"/> <input type="button" value="Actions for Selected..."/> <input type="button" value="Refresh Product Instance List"/>			
<input checked="" type="checkbox"/>	Name	Last Contact ↓	Alerts
	Filter By Host/IP, SN or PID	Filter By Last Contact	Filter By Alerts
<input checked="" type="checkbox"/>	UDI_PID:C9500-32QC; UDI_SN:CAT2148L15K	11-Nov-2020 23:53	COMPLETE: Usage report uploaded to CSSM
			Items per page: 5 1 - 1 of 1 < > >> <<

Wenn das Gerät auch dann noch verfügbar ist, wenn die ACK-Nachricht vom CSSM empfangen wird, wird die ACK an PI zurückgesendet. Andernfalls wird ACK beim nächsten Pull-Intervall gesendet.

PULL-Modus mit RESTCONF

Für den PULL-Modus RESTCONF sind folgende Konfigurationen vom Gerät und Schritte vom CSLU-Modul erforderlich:

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
!
```



Hinweis: Diese Konfigurationen gelten für die lokale Authentifizierung. Die Remote-Authentifizierung kann ebenfalls verwendet werden.

CSLU - Prozedur für die Einrichtung

CSLU muss beim CSSM angemeldet sein, damit Berichte automatisch synchronisiert werden können. Die CSLU-Einrichtung entspricht der RESTAPI für die RUM-Berichtserfassung und -berichterstattung.

Schritt 1: Add Single Product Wählen Sie auf der Inventarseite die Option aus.

Schritt 2: Geben Sie die Geräte-IP ein.

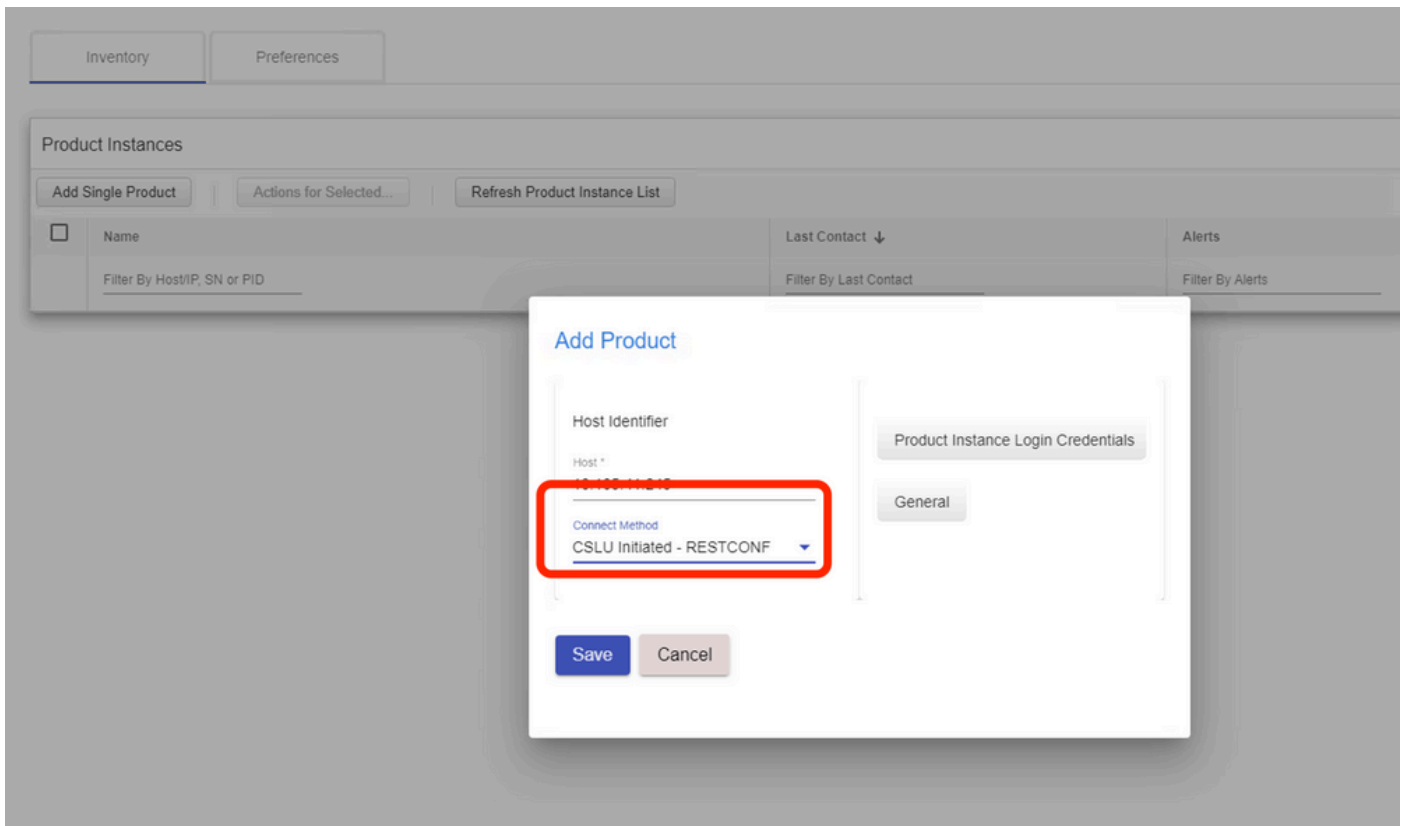
Schritt 3: Wählen Sie die Verbindungsmethode als RESTCONF aus.

Schritt 4: Wählen Sie Anmeldedaten für Produktinstanzen aus.

Schritt 5: Geben Sie die Anmeldeinformationen des Benutzers mit Priv. 15-Zugriff ein.

Schritt 6: Speichern der Konfigurationen

Schritt 7. Erfassen Sie Nutzungsdaten für das ausgewählte Gerät.



PULL-Modus mit NETCONF

Für den PULL-Modus NETCONF sind folgende Konfigurationen vom Gerät und Schritte von CSLU erforderlich:


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

 **Hinweis:** Diese Konfigurationen gelten für die lokale Authentifizierung. Die Remote-Authentifizierung kann ebenfalls verwendet werden.

CSLU - Prozedur für die Einrichtung

CSLU muss beim CSSM angemeldet sein, damit Berichte automatisch synchronisiert werden können. Die CSLU-Einrichtung entspricht der RESTAPI für die RUM-Berichtserfassung und -berichterstattung.

Schritt 1: Add Single Product Wählen Sie auf der Inventarseite die Option aus.

Schritt 2: Geben Sie die Geräte-IP ein.

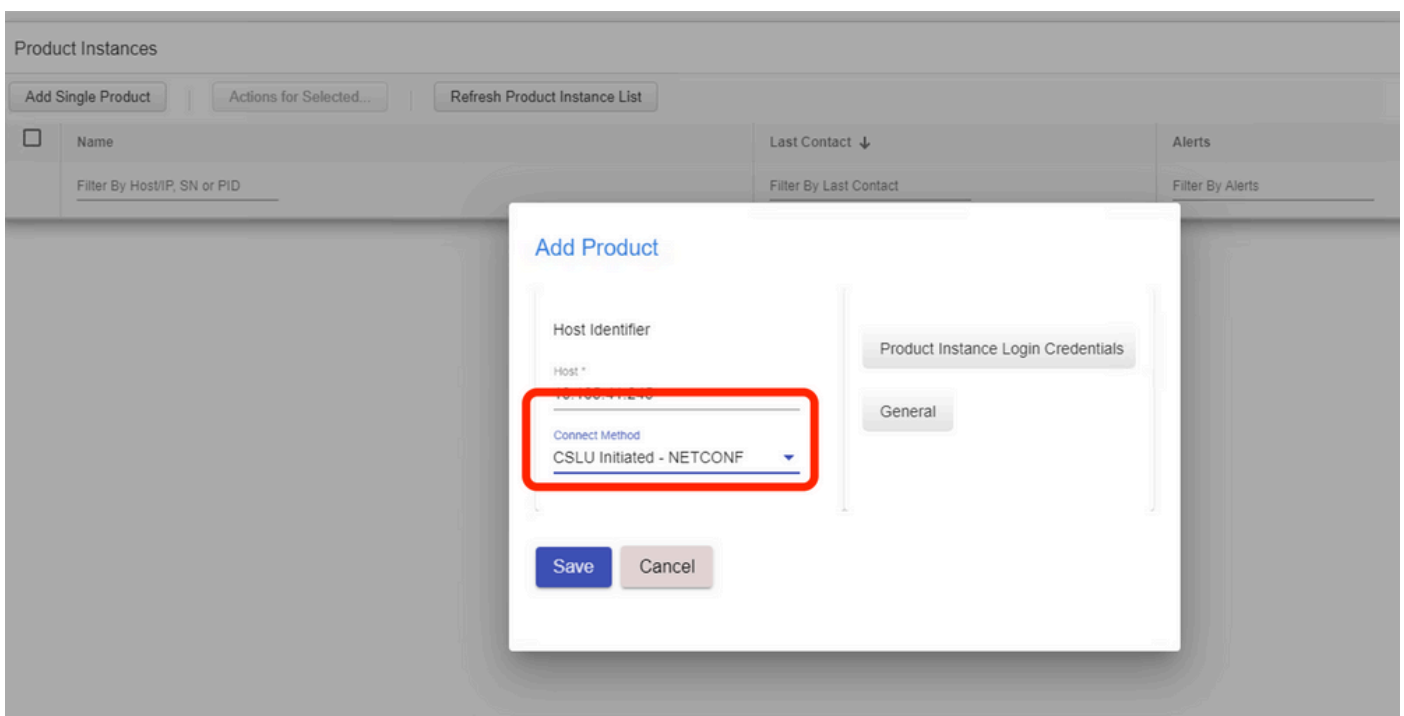
Schritt 3: Wählen Sie die Verbindungsmethode als NETCONF aus.

Schritt 4: Wählen Sie Anmeldedaten für Produktinstanzen aus.

Schritt 5: Geben Sie die Anmeldeinformationen des Benutzers mit Priv. 15-Zugriff ein.

Schritt 6: Speichern der Konfigurationen

Schritt 7. Erfassen Sie Nutzungsdaten für das ausgewählte Gerät.



Product Instances

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

<input type="checkbox"/>	Name	Last Contact ↓	Alerts
	Filter By Host/IP, SN or PID	Filter By Last Contact	Filter By Alerts

Add Product

Host Identifier


Host *

Connect Method
CSLU Initiated - NETCONF

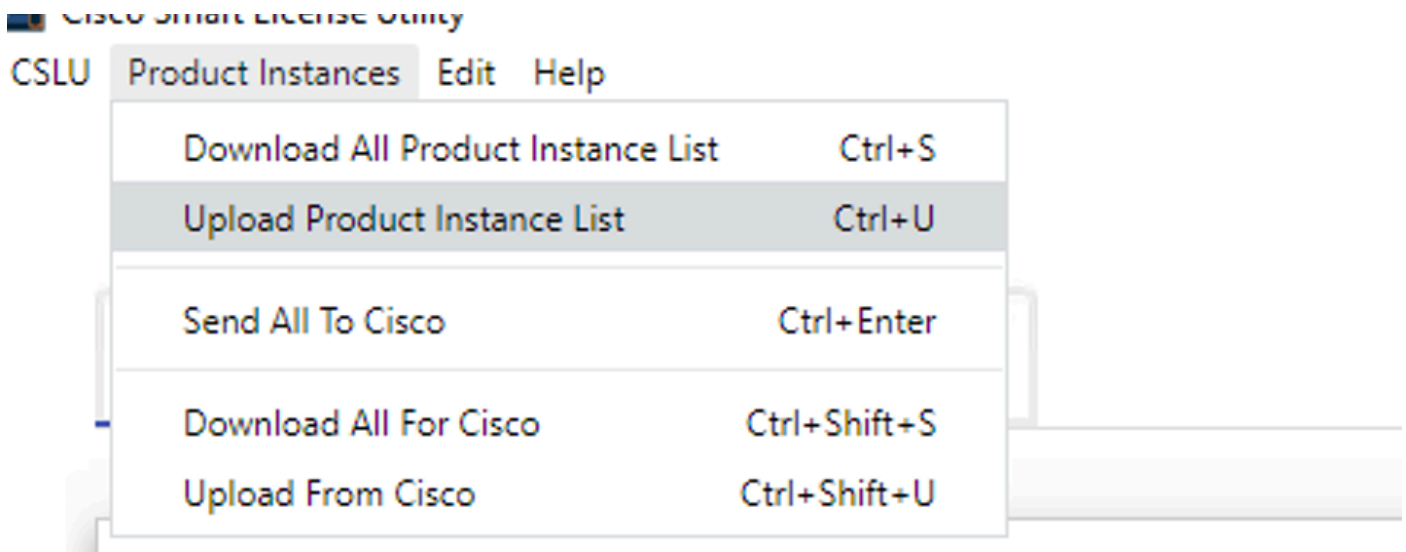
Product Instance Login Credentials

General

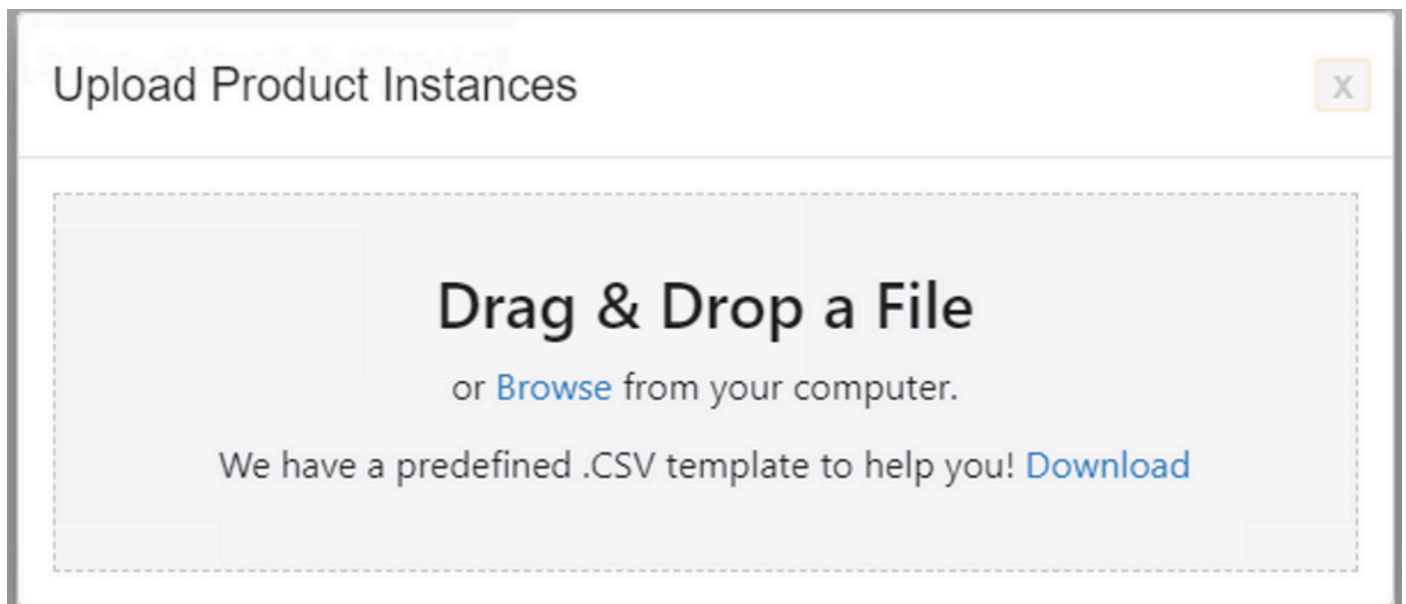
Save Cancel


 **Hinweis:** Die Geräteliste kann für alle Modelle NETCONF, RESTCONF, und RESTAPI in großen Mengen hinzugefügt werden.

Um den Massen-Upload durchzuführen, navigieren Sie auf der Menü Leiste zu Product Instance > Upload Product Instance List, wie in diesem Bild dargestellt.



Ein neues Popup-Fenster wird geöffnet. Die Vorlagendatei kann heruntergeladen werden. Tragen Sie in der CSV-Formatdatei die Gerätedetails der Geräteliste ein, und laden Sie die Daten zur CSLU hoch, um mehrere Geräte hinzuzufügen.



 **Hinweis:** Für alle Typen des CSLU-PULL-Modus wird empfohlen, den Transportsatz für die PI auf Off (Aus) zu setzen. Dies kann über die CLI erfolgen.

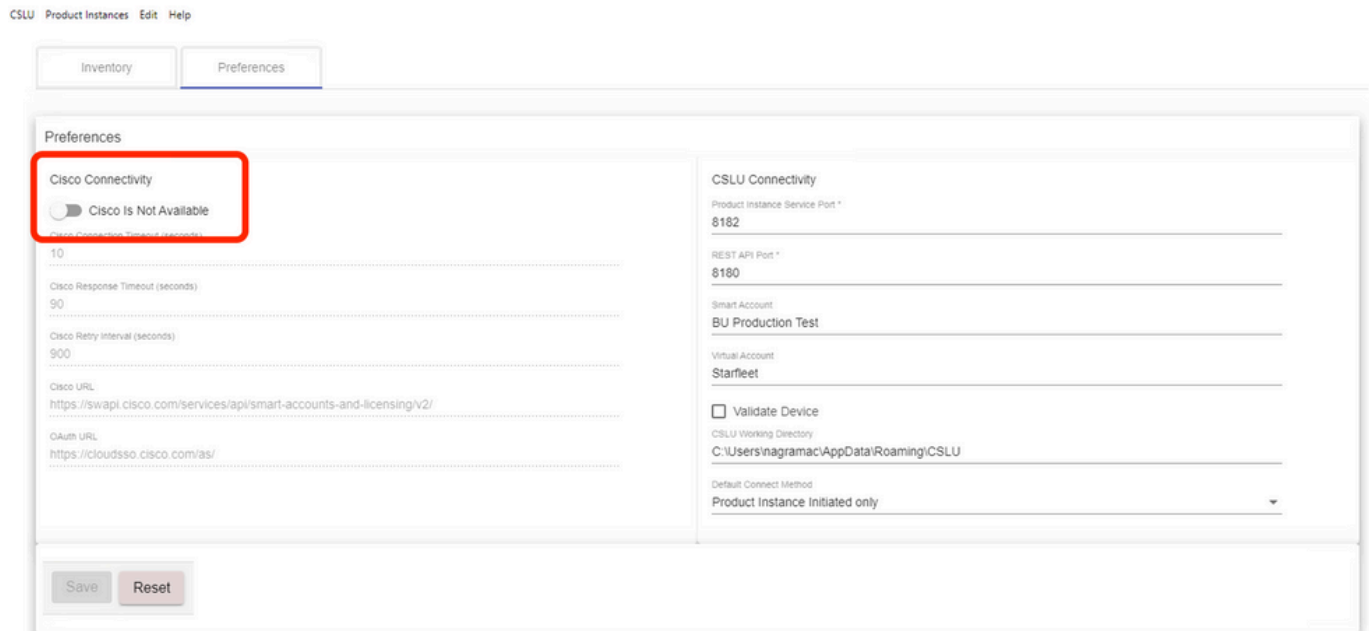
```
Switch(config)#license smart transport off
```

CSLU im getrennten Modus

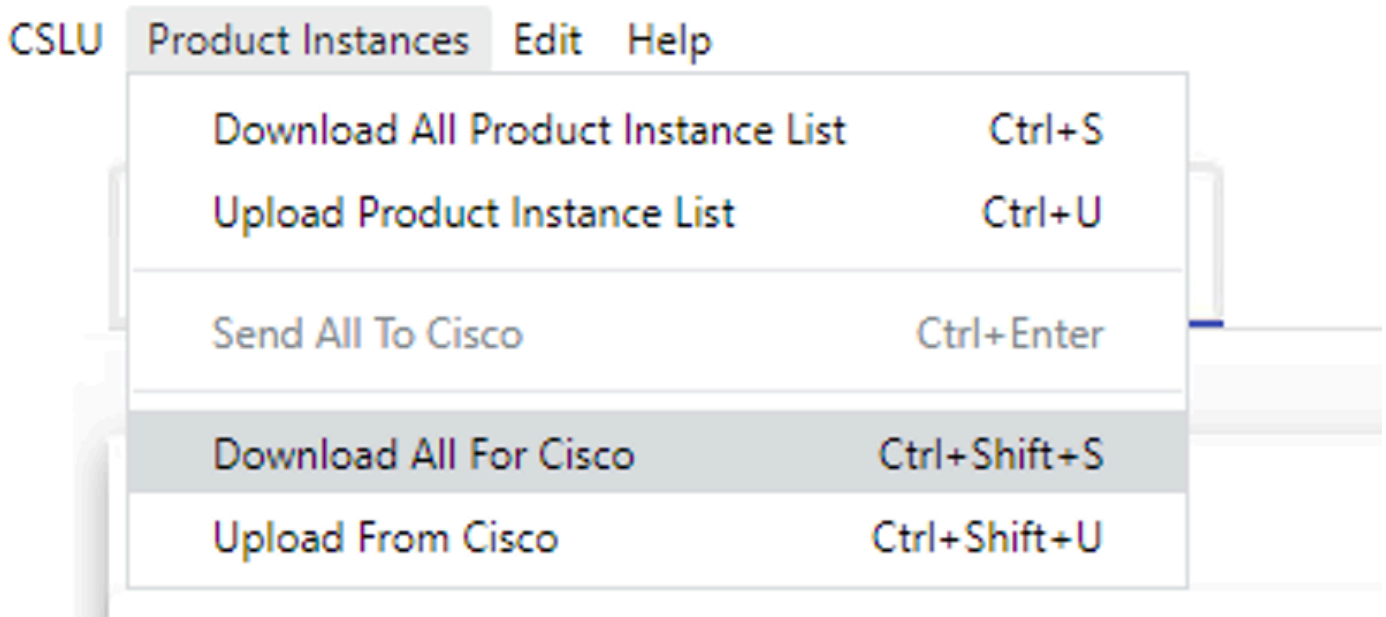
CSLU kann im getrennten Modus von CSSM ausgeführt werden. Dies gilt für Bereitstellungen, bei denen die Verbindung der CSLU mit dem Internet nicht möglich ist. Im getrennten Modus werden die Berichte aller Geräte manuell von CSLU heruntergeladen und in CSSM hochgeladen. ACK-Nachrichten werden wiederum von CSSM heruntergeladen und auf CSLU hochgeladen. Die CSLU führt weiterhin PULL/PUSH-Nutzungsdaten von PIs aus und sendet außerdem die ACK-Nachricht an PI zurück.

Schritt 1: Deaktivieren Sie auf CSLU Preference Seite die Option Cisco Connectivity. Dies bestätigt, dass Cisco nicht verfügbar ist.

Schritt 2: Speichern der Einstellungen



Schritt 3: Klicken Sie in der Menu Leiste auf Product Instances > Download All for Cisco. Dadurch wird eine tar.gz Datei auf die CSLU heruntergeladen.



Schritt 4: Laden Sie die Datei in CSSM hoch. Navigieren Sie auf der Seite "CSSM Smart Account" zu Report > Usage Data Files > Upload usage data. Laden Sie die tar.gz Datei in das Popup-Fenster hoch.

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

Schritt 5: Sobald die Daten verarbeitet sind, wird die Bestätigung generiert. Laden Sie die ACK-Datei herunter, und laden Sie sie in die CSLU-Datei hoch.

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

Schritt 6: Importieren Sie in CSLU die ACK-Datei aus der Menüleiste, und navigieren Sie zu Product Instances > Upload from Cisco, wie in diesem Bild dargestellt.

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)**

Schritt 7. Nach dem Hochladen der ACK wird die Nachricht an die PIs gesendet. Dasselbe kann in der Spalte "Alerts" (Warnungen) überprüft werden.

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_C9500-320C; UDI_SN_CAT2148L15K	12-Nov-2020 01:10	COMPLETE: Usage report acknowledgement to product instance

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

SLP = Offline-Modus

SLP kann auch im gesamten Offline-Modus verwendet werden. Dies gilt vor allem für Air-Gap-Netzwerke, die keine Internetverbindung bevorzugen und auch nicht CSLU verwenden. Im Offline-Modus wird der Transport auf Off gesetzt.

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>

Wenn Sie die Nutzungsdaten an CSSM melden möchten, müssen die Nutzungsberichte als Datei heruntergeladen und manuell in CSSM hochgeladen werden. In einem HA-System erfasst Active die Nutzung für Standby-/Mitgliedsgeräte.

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

Nun muss dieser Bericht manuell in CSSM hochgeladen werden.

Exportieren Sie die gespeicherten Nutzungsdaten von PI auf den Desktop.

Navigieren Sie auf der CSSM Smart Account-Seite zu Report > Usage Data Files > Upload usage data. Wählen Sie im Popup-Fenster den Nutzungsbericht aus, und klicken Sie auf upload.

Nachdem die Datei hochgeladen wurde, müssen Sie die richtige VA auswählen, der das Gerät zugeordnet ist.

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

Sobald die Daten vollständig verarbeitet sind und die Bestätigung bereit ist, laden Sie die Datei herunter und laden Sie sie auf die PI.

```
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

Verhaltensänderungen

Diese Änderungen werden bei Versionen der Smart Licensing-Funktion vorgenommen:

- **Trust Sync** - Ab 17.7.1 ist Trust Code auf dem Switch in allen unterstützten Topologien wie CSLU und Offline-Methoden installiert.
- **Datenschutzänderungen** - Ab 17.7.1 sind Versionszeichenfolgen- und Hostnameninformationen von 17.9.1 in den an CSSM gesendeten RUM-Berichten enthalten, wenn die entsprechenden Datenschutzeinstellungen deaktiviert sind.
- **Kontodetails** - Ab 17.7.1 enthält die ACK-Nachricht von CSSM die Kontoinformationen und SA/VA-Details.
- **RUM-Berichtsdrosselung** - Ab 17.9.1 wird das Berichtsintervall gedrosselt, in dem der PI die Kommunikation initiiert. Die minimale Berichtshäufigkeit wird auf einen Tag gedrosselt. Das bedeutet, dass die Produktinstanz nicht mehr als einmal täglich RUM-Berichte sendet.

Fehlerbehebung

Allgemeiner Fragebogen zur Fehlerbehebung

Szenario 1: Einige Protokolle (d. h. HSRP) funktionieren nach einem Upgrade von Cisco IOS XE von einer sehr frühen Version (d. h. 16.9.x) nicht mehr.

Überprüfen Sie die Lizenz-Bootstufe, um festzustellen, ob diese mit der Version vor dem Upgrade von Cisco IOS XE übereinstimmt. Es ist möglich, dass die Lizenz-Bootstufe auf Networking-Essentials zurückgesetzt wurde, das möglicherweise die fehlerhaften Protokolle (d. h. HSRP) nicht unterstützt.

Szenario 2: Lizenzstatus mit Meldungen "Fehlergrund: Senden von HTTP-Nachricht für Call Home fehlgeschlagen" oder "Letzter Kommunikationsversuch: AUSSTEHEND"

Dies kann mit grundlegenden Verbindungsproblemen zusammenhängen. So lösen Sie die Prüfung:

- Netzwerkverbindung zum Erreichen von CSSM - IP-Adresse, Routen usw.
- Das ip http client source interface ist korrekt konfiguriert.
- Zeitunterschied. (NTP muss so konfiguriert werden, dass Uhrzeit/Zone richtig angegeben werden)
- Wenn die interne Firewall-Konfiguration den Datenverkehr zum CSSM blockiert

Szenario 3: Was geschieht, wenn der Protokollfehler "%SMART_LIC-3-AUTH_RENEW_FAILED: Authorization Renewal with the Cisco Smart Software Manager (CSSM): undefined method 'each' for nil:NilClass" nach einem Jahr der Registrierung angezeigt wird?

Registrieren Sie das Produkt erneut. Generieren Sie eine neue Token-ID für CSSM, und registrieren Sie die Produktinstanz erneut für CSSM.

Szenario 4: Fehlermeldung "%SMART_LIC-3-COMM_FAILED: Communications failure", wenn keine Verbindungsfehler mit Cisco auftreten.

Wenn es keine Verbindungsprobleme mit CSSM gibt und wenn auf PI weiterhin der genannte Fehler auftritt, kann dies daran liegen, dass das Zertifikat durch das letzte Server-Upgrade entfernt wurde. Das Zertifikat ist für die TLS-Authentifizierung der beiden kommunizierenden Seiten erforderlich. Konfigurieren Sie in diesem Fall CLI auf der PI, ip http client secure-trustpoint SLA-TrustPoint und versuchen Sie es erneut.

PI debuggen

Die von PI gesammelten Befehle zur Fehlerbehebung sind:

```
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 debuggen

Wenn ein Problem mit CSLU gedebuggt wird, ist es wichtig, dass die Protokolldatei aus diesem Verzeichnis auf einem CSLU-installierten PC erstellt wird.

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

Verwandte Referenzen

- Migration zu SL mithilfe der Richtlinie - [Migration älterer SL/SLR/PLR-Lizenzen zu SL mithilfe der Richtlinie](#)
- Versionshinweise: [RN-9200](#), [RN-9300](#), [RN-9400](#), [RN-9500](#), [RN-9600](#)
- Konfigurationsanleitungen: [Cat9200-CG](#), [Cat9300-CG](#), [Cat9400-CG](#), [Cat9500-CG](#), [Cat9600-CG](#)
- Befehlsreferenzen: [Cat9200-CR](#), [Cat9300-CR](#), [Cat9400-CR](#), [Cat9500-CR](#), [Cat9600-CR](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.