

# Comprensión de Smart Licensing para Catalyst Switching

## Contenido

---

[Introducción](#)

[Propósito](#)

[Licencias inteligentes mediante políticas](#)

[Terminology](#)

[¿Por qué este cambio?](#)

[Licencias disponibles](#)

[Licencias básicas](#)

[Licencias de complementos](#)

[Los nuevos componentes](#)

[Política](#)

[Informes RUM](#)

[Flujo de fabricación para un caso de implementación nuevo](#)

[CSLU](#)

[SLP - Conexión directa](#)

[Informes de licencias](#)

[Conexión directa: Smart Transport](#)

[Conexión directa: transporte desde casa](#)

[SLP - CSLU](#)

[Instalación y configuración de CSLU](#)

[CSLU con el modo PUSH](#)

[Detección automática de CSLU](#)

[CSLU mediante el modo PULL](#)

[Modo PULL con RESTAPI](#)

[CSLU: procedimiento de configuración](#)

[Modo PULL con RESTCONF](#)

[CSLU: procedimiento de configuración](#)

[Modo PULL con NETCONF](#)

[CSLU: procedimiento de configuración](#)

[CSLU con modo desconectado](#)

[SLP - Modo sin conexión](#)

[Cambios de comportamiento](#)

[Troubleshoot](#)

[Cuestionario genérico de resolución de problemas](#)

[Depurar PI](#)

[Debug CSLU](#)

[Referencias relacionadas](#)

---

# Introducción

Este documento describe la función de licencia inteligente que utiliza la política en las plataformas de switching Catalyst y la implementación admitida.

## Propósito

A partir de las versiones 17.3.2 y 17.4.1, de Cisco IOS® XE, todas las plataformas de switching Catalyst de la familia Cat9k admiten un nuevo modelo de licencia de SLP (licencia inteligente mediante políticas). El objetivo de este documento es comprender los diferentes modelos admitidos de implementación e implementación de SLP, principalmente para implementaciones nuevas.

## Licencias inteligentes mediante políticas

Con SLP, el dispositivo tiene todas las licencias "en uso" listas para usar. Los conceptos anteriores, el modo de evaluación, el registro y la reserva desaparecen con SLP. Con SLP, todo gira en torno a la generación de informes sobre las licencias y su uso. Las licencias siguen sin aplicarse y los niveles de licencia siguen siendo los mismos. Para las plataformas de switches Catalyst, no hay niveles de licencias controladas por exportación, aparte de la licencia HSECK9. El único cambio se produce en el infra de los informes de uso y seguimiento de licencias. En esta sección se tratan en detalle las terminologías, los motivos de los cambios, los nuevos componentes que se incluyen con SLP, CSLU (Cisco Smart Licensing Utility) y el flujo de pedidos de productos.

## Terminology

- CSSM o SSM: Cisco Smart Software Manager
- SA - Cuenta inteligente
- VA - Cuenta virtual
- SL - Licencias inteligentes
- PLR - Reserva de licencia permanente
- SLR - Reserva de licencia inteligente
- PID: ID de productos
- SCH: Smart Call Home
- PI - Instancias de productos
- CSLU: Cisco Smart Licensing Utility
- RUM - Medición de utilización de recursos
- ACK: confirmación
- UDI - Identificación exclusiva de dispositivos - PID + SN
- SLP - Licencias inteligentes mediante políticas

## ¿Por qué este cambio?

Con la introducción del modelo de licencia inteligente de trust and verify, Cisco ha admitido varios mecanismos de

implementación para realizar un seguimiento del uso de licencias y generar informes al CSSM. Sin embargo, no era fácilmente adaptable para todo tipo de implementaciones: había información y requisitos de campo para que las licencias inteligentes fueran más favorables para su adopción. Algunos de los desafíos son:

- Con registro de nivel de servicio: los dispositivos deben estar siempre conectados a Internet para llegar a CSSM, lo que supone un problema de implementación.
- Los servidores satélite in situ suponen un mayor coste de implementación y mantenimiento.
- SLR facilita solo las redes con espacios de ventilación.
- Las implementaciones que no admitan ninguno de estos modelos deben ejecutar sus dispositivos en el Unregistered/Eval expired estado, incluso después de adquirir las licencias.

La SLP se introduce para facilitar diversas solicitudes de este tipo desde el terreno. Con SLP, no es necesario registrar el producto en CSSM. Todos los niveles de licencia que se adquieren están "en uso" desde el primer momento. Esto elimina la fricción del día 0 presente en el dispositivo. SLP también minimiza el flujo de trabajo del aprovisionamiento de licencias y reduce el exceso de puntos de contacto. No es necesario que el dispositivo esté conectado al CSSM las 24 horas del día. SLP también ofrece la posibilidad de utilizar licencias en la red desconectada, informar del uso de la licencia sin conexión e informar de la licencia a intervalos determinados por las políticas del cliente.

#### Licencias disponibles

Las funciones de software disponibles se encuentran en los niveles de licencia base o complementaria. Las licencias básicas son licencias perpetuas y las licencias complementarias están disponibles en plazos de tres, cinco y siete años.

#### Licencias básicas

- Network Essentials
- Ventaja de red
- HSECK9

#### Licencias de complementos

- DNA Essentials
- Ventaja del ADN



**Nota:** HSECK9 es una licencia de exportación controlada. Requiere un SLAC para habilitar la licencia y la función respectiva.

---

Los nuevos componentes

Política

La política decide cuál debe ser el comportamiento predeterminado para el PI. Indica los atributos de los requisitos de informes de licencias para los diferentes niveles y condiciones de licencia. La política también determina si el mensaje ACK debe ser enviado de vuelta a PI, para cada informe que se envía a CSSM o no. La directiva también contiene el nombre de la directiva y cuándo se instala. La política predeterminada de Cisco es común y estándar para todos los productos Catalyst. Sin embargo, la política definida por el cliente también se permite si desea tener diferentes intervalos de informes y omisión de respuesta ACK.

La política se puede instalar en un PI en varias ocasiones.

- Política predeterminada presente en el software
- Política instalada por el fabricante de Cisco
- Política instalada mediante respuesta ACK
- Directiva instalada manualmente a través de CLI
- Política impulsada mediante solicitud Yang

Este resultado muestra el aspecto de una política predeterminada.

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)

---

 **Nota:** Una política no se puede borrar cuando borra/modifica una configuración del sistema, borra nvram o formatea flash: filesystem.  
La política se establece en Cisco default, en el **restablecimiento de fábrica inteligente de la licencia**.

---

Informes RUM

RUM son informes de uso generados y almacenados por PI. Los informes de RUM estándar ISO19770-4 se completan para SLP. Los informes de RUM almacenan todos y cada uno de los cambios en el uso de licencias realizados en PI como archivos de informe. Los datos de uso de cada nivel de licencia se almacenan en informes RUM independientes. Las mediciones del informe RUM se recogen y almacenan en PI a intervalos regulares. Siempre que se produce un cambio en el uso de la licencia de PI o se ha generado un informe de uso o cuando los informes han alcanzado el tamaño máximo/muestras, se generan nuevos informes de RUM para todos los niveles de licencia. En otros casos, los informes RUM existentes se pueden sobrescribir con una nueva muestra y una marca de tiempo actualizada. La medición predeterminada de la utilidad de

informes RUM es cada 15 minutos. En cada intervalo de informe, los informes RUM se envían a Cisco CSSM.

Todos los informes RUM están firmados por el IP y verificados por el CSSM. Cuando CSSM recibe los datos del informe RUM de PI, valida el informe, comprueba la línea de tiempo del cambio de uso de la licencia y actualiza los datos CSSM en consecuencia. El CSSM entonces reconoce al IP a través del mensaje de respuesta ACK.

Los informes RUM se pueden enviar al CSSM de varias maneras:

- PI envía informes RUM al CSSM directamente en el intervalo de informes.
- PI envía el informe RUM a la CSLU.
- CSLU extrae informes RUM de PI a intervalos regulares a través de RESTAPI y YANG modelos.
- Los informes de RUM se guardan manualmente en la API a través de CLI y se cargan manualmente en CSSM.

---

 **Nota:** Los informes de RUM no se pueden borrar cuando borra/modifica una configuración del sistema, borra nvram o formatea flash: filesystem. Todos los informes de RUM se pueden eliminar de PI, en 'restablecimiento de fábrica inteligente de licencias'.

---



**Nota:** El intervalo de informes predeterminado es de 30 días.

---

#### Flujo de fabricación para un caso de implementación nuevo

Una vez que se realiza un nuevo pedido de producto en Cisco CCW (Cisco Commerce Workspace), el PII pasa por el flujo de operaciones que realiza el equipo de fabricación. Esto es para facilitar el proceso seguro de firma de informes RUM y eliminar la fricción del día 0 en el registro de la PI. Una vez realizado el pedido, cualquier SA/VA existente o nueva SA/VA que se cree se asociará al producto. El equipo de fabricación de Cisco se encarga de estas operaciones antes de enviarle el producto:

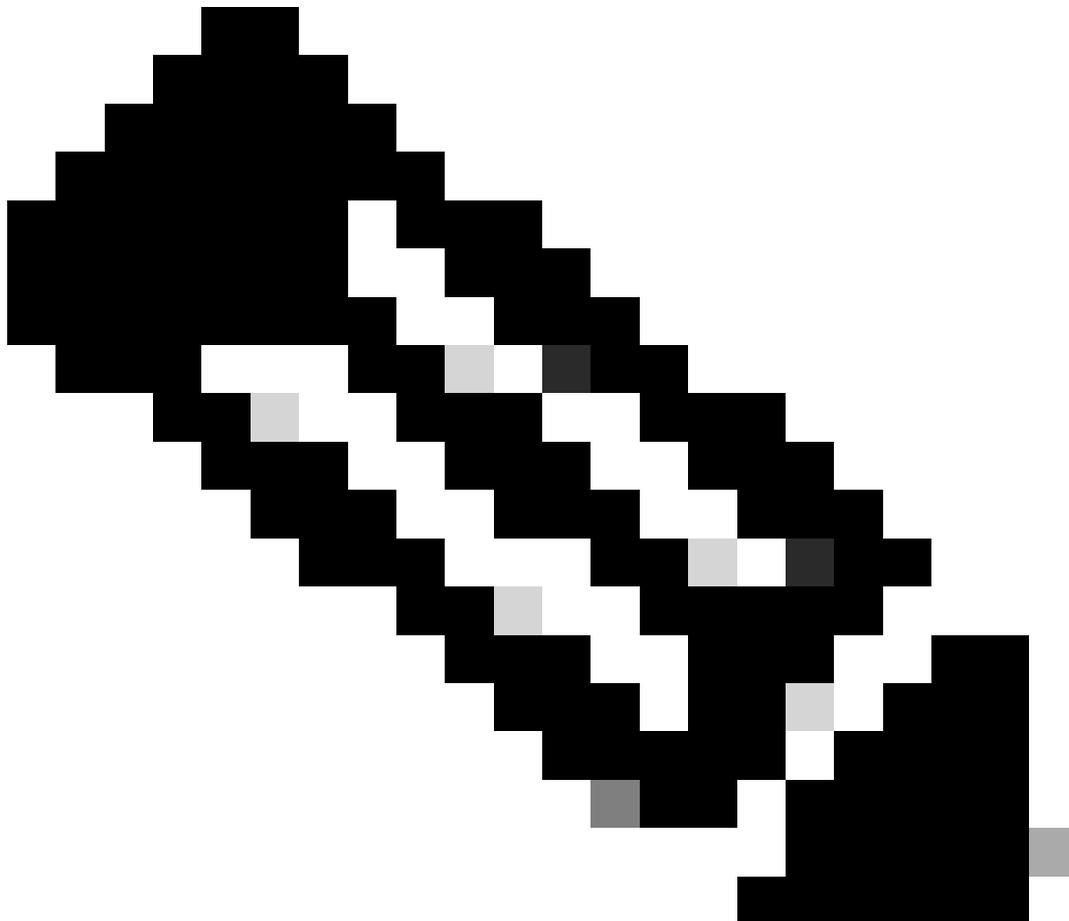
- Instale el código de confianza en el dispositivo. La firma del código de confianza se instala en función del UDI del dispositivo. Se instala en todos los productos.

- Instalar código de compra: información sobre los niveles de licencia que se adquieren junto con el producto. Se instala en todos los productos.
- SLAC - Código de autenticación de licencia inteligente - No aplicable para plataformas Catalyst.
- Directiva de instalación: Política predeterminada o personalizada basada en los datos introducidos.
- Informe del uso de la licencia a CSSM - SA/VA.



**Nota:** Con la versión 17.3.3, este flujo se sigue para todas las plataformas de switching Catalyst excepto para C9200/C9200L.

---



**Nota:** El código de confianza se instala solamente en la fabricación con 17.7.1 para todas las plataformas de switching de Catalyst excepto C9200/C9200L.

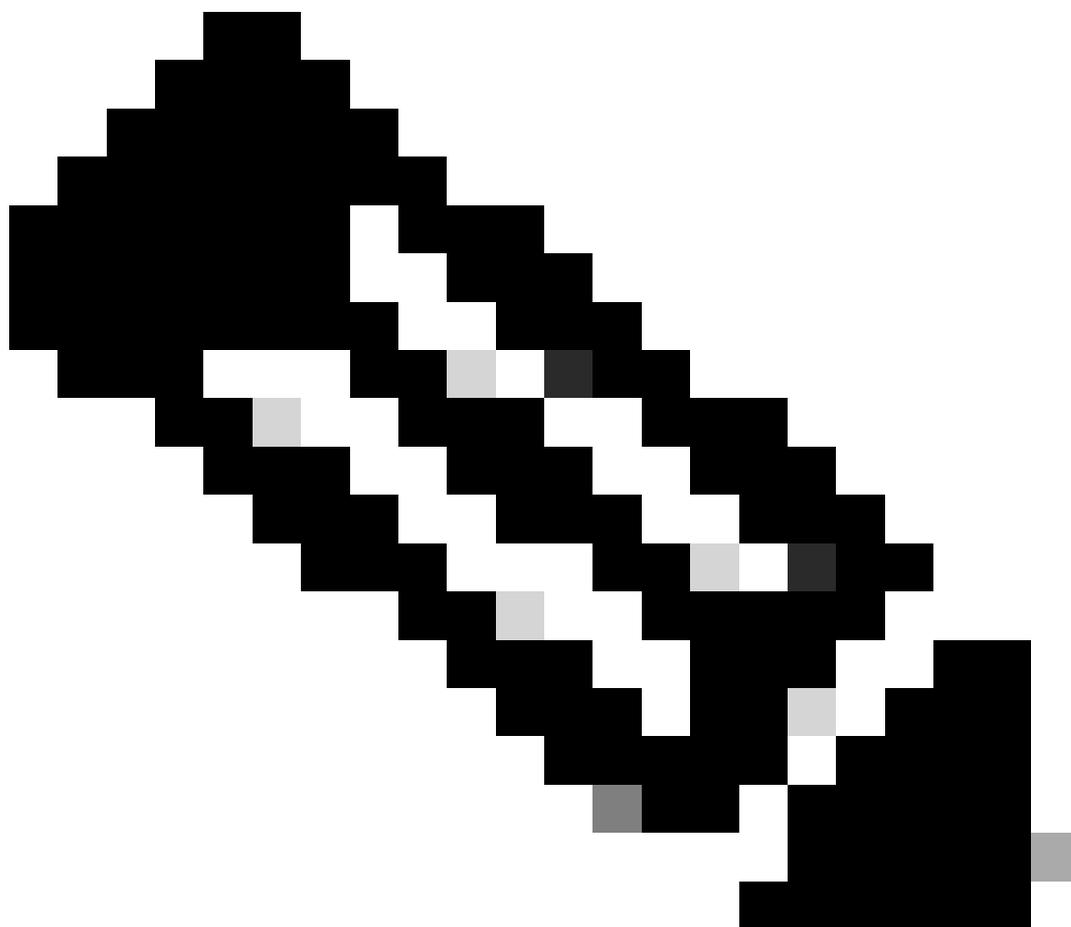
---

---

## CSLU

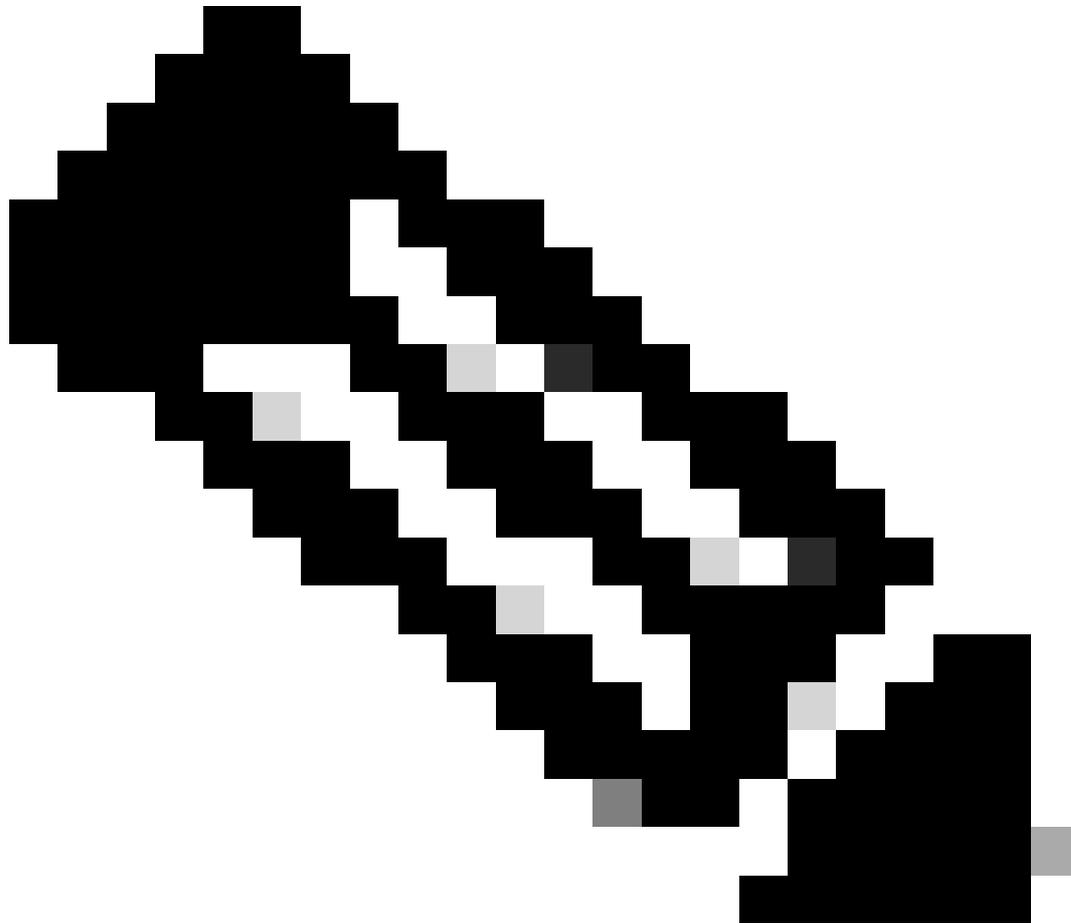
SLP presenta una nueva CSLU de herramientas sencilla pero potente. CSLU es una herramienta basada en GUI, que se ejecuta en el sistema operativo Windows 10 o en la versión Linux basada en RHEL/Debian. La CSLU, que se puede ejecutar en su red privada local, es responsable de recopilar los puertos RUM de las IP asociadas con CSSM. La CSLU se debe aprovisionar de manera que recopile los informes RUM sobre los IP en la red local y también para enviar periódicamente el informe RUM a CSSM a través de Internet. CSLU es una sencilla herramienta que muestra solo los detalles de los UDI de los dispositivos suministrados. Todos los datos de Uso de licencias para PI, Licencias adquiridas y Licencias no utilizadas del grupo solo se ven en SA/VA de CSSM, para que pueda verificarlos. Es muy eficaz porque puede recopilar informes de uso de hasta 10 000 IP. CSLU también es responsable de enviar los mensajes ACK de CSSM nuevamente a PI.

---



**Nota:** Consulte la sección Topología basada en CSLU para obtener información detallada sobre la configuración y los modos de funcionamiento admitidos de CSLU.

---

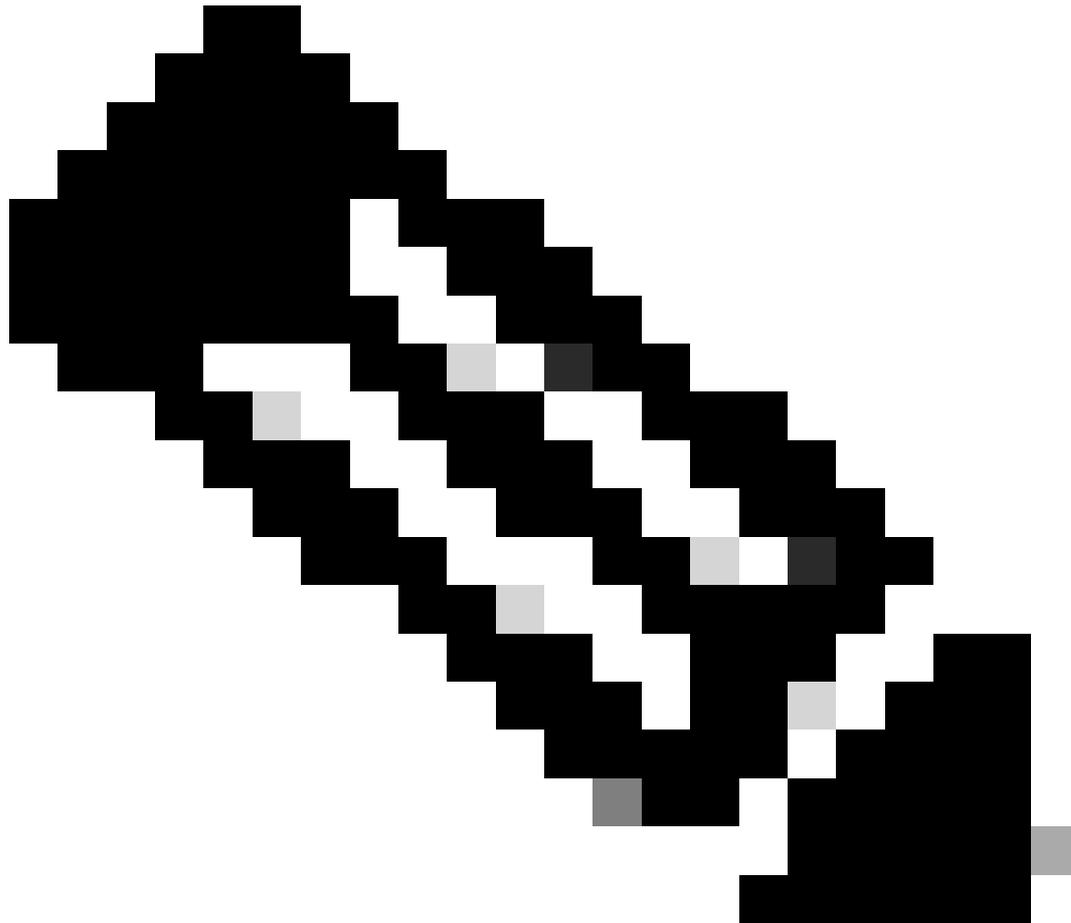
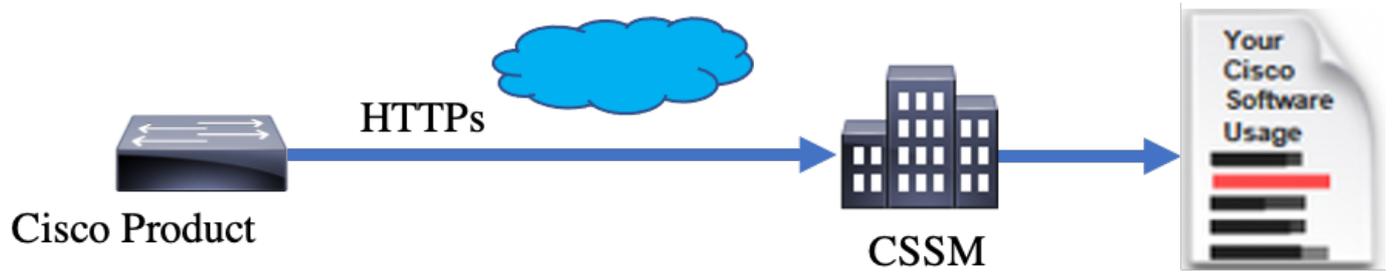


**Nota:** La versión Linux de CSLU es compatible con la versión 17.7.1.

---

#### SLP - Conexión directa

En un producto enviado de fábrica, el modo de transporte predeterminado se configura en CSLU. Si desea utilizar el método de conexión directa, debe cambiar el modo de transporte a Call-home o SMART según los requisitos. El requisito básico para el método de topología de conexión directa es disponer de conectividad a Internet para el alcance al CSSM. Además, se debe garantizar que, para la conectividad con CSSM, las configuraciones L3, DNS y configuraciones de dominio necesarias estén presentes en el dispositivo.



**Nota:** el transporte inteligente es el método de transporte recomendado cuando se conecta directamente a CSSM.

En la topología de conexión directa, los informes de RUM se envían directamente a CSSM. Los informes de licencias requieren que el código de confianza se instale correctamente en el dispositivo. El fabricante de Cisco instala el código de confianza en el dispositivo antes de enviarlo. También puede instalar el código de confianza en el dispositivo.

El código de confianza es una cadena de token tomada de CSSM, en la página Cuenta virtual - General. El código de confianza se puede instalar mediante la CLI.

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

---

 **Nota:** todas las opciones deben utilizarse para sistemas HA o Stacking Back. Para un dispositivo autónomo, se puede utilizar la opción local.

---

```
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

Una vez que el código de confianza se ha instalado correctamente, el IP puede informar del uso al CSSM directamente. Estas condiciones dan como resultado la generación de informes de licencias:

- Instalación correcta del código de confianza
- En cada intervalo de informes predeterminado
- Recarga/Arranque en el dispositivo
- Un switchover
- Incorporación o eliminación de un miembro de la pila
- Activación manual de sincronización de licencias

Los informes de licencias para CSSM se pueden activar con la siguiente CLI:

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

La sección Informes de uso de la show license status le indica las fechas del último ACK recibido, la siguiente fecha límite de ACK, la siguiente transferencia de informe y la última transferencia de informe.

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>

Conexión directa: Smart Transport

En una topología de modo Direct Connect o Direct Cloud Access, si se utiliza SMART Transport, estas son las configuraciones necesarias en el dispositivo.

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
```

!

Conexión directa: transporte desde casa

En una topología de modo Direct Connect o Direct Cloud Access, si se utiliza Call-home Transport, estas son las configuraciones necesarias en el dispositivo.

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
!
```

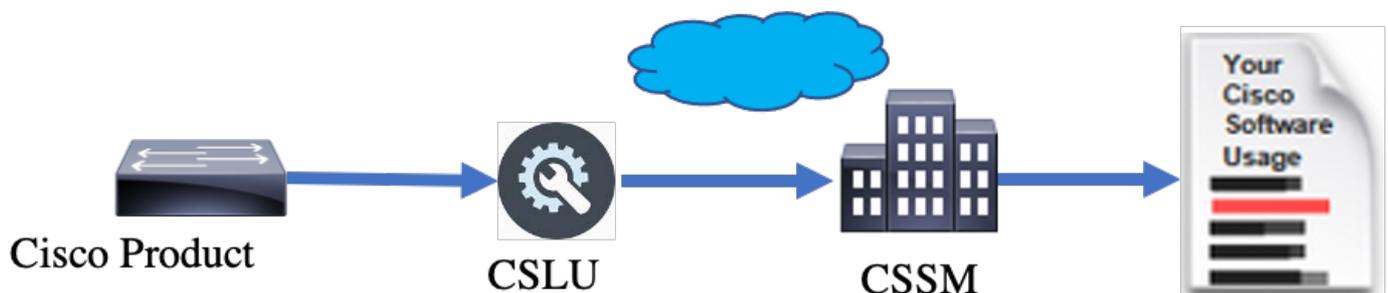
---

 **Nota:** de forma predeterminada, la dirección de destino para Call-home se configura en CSSM URL. Esto se puede verificar en la show run all configuración.

---

## SLP - CSLU

El modo CSLU es el modo de transporte predeterminado en los dispositivos enviados de fábrica que ejecutan 17.3.2 o posterior. Además, si migra desde licencias que han caducado Eval/Eval, el modo de transporte después de pasar a SLP es CSLU. En la topología basada en CSLU, la CSLU se sitúa entre el PI y el CSSM. CSLU evita que los usuarios tengan conectividad de red directa con Cisco Cloud - CSSM. La CSLU puede ejecutarse localmente en una red privada y descargar informes de uso de todas las PI asociadas. Los informes de uso se guardan localmente en el PC con Windows antes de enviarse al CSSM a través de Internet. CSLU es una herramienta ligera. Sólo puede ver la lista de IP asociados a ella y puede identificarse mediante el uso de UDI. La CSLU no puede mostrar ni contener la información de redundancia de los niveles de licencia o PI ni el uso de licencias.

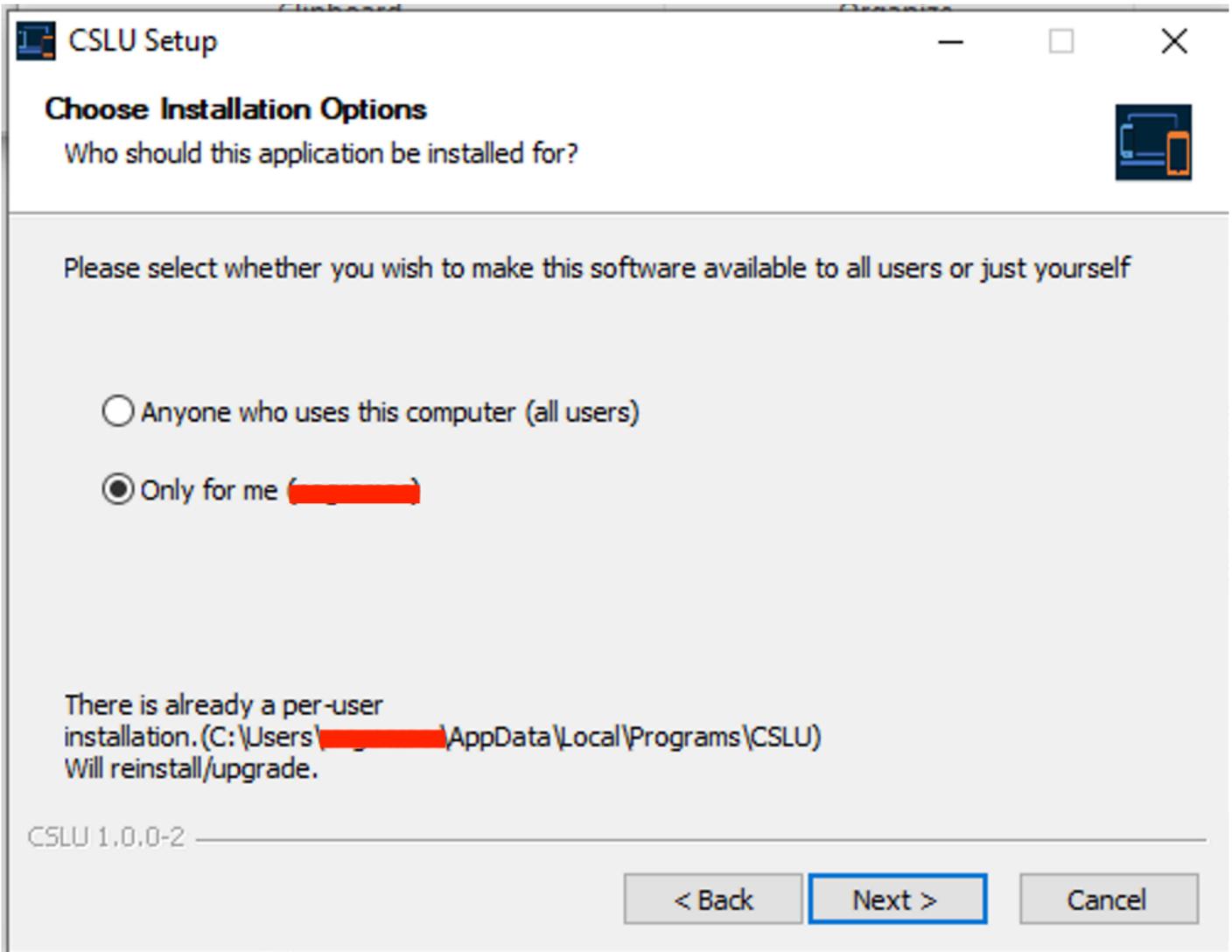


## Instalación y configuración de CSLU

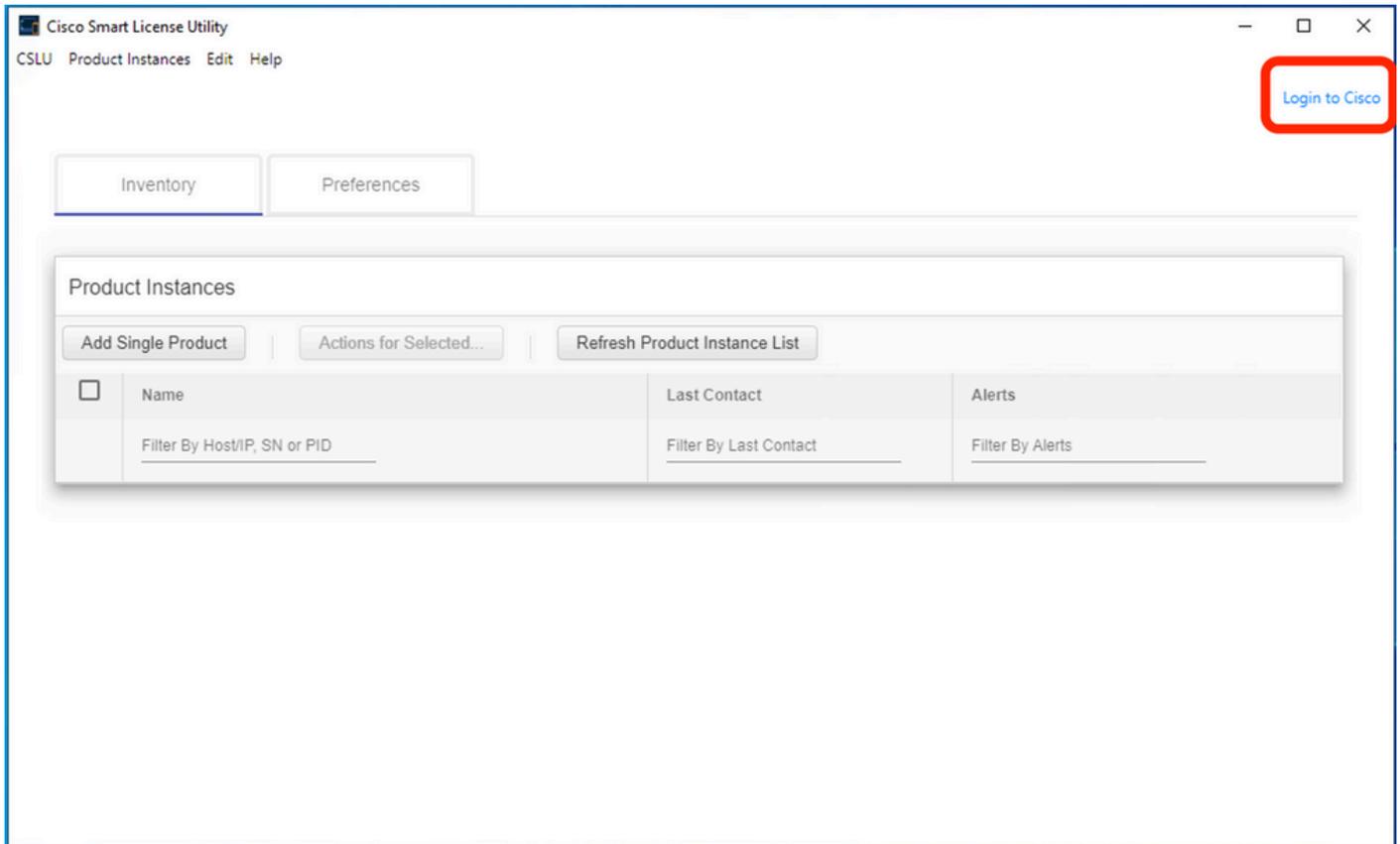
La herramienta CSLU está instalada y funciona en equipos con Windows 10. El software está disponible en CCO para su descarga y uso sin coste alguno. Una vez instalada la herramienta, puede descargar la guía de inicio rápido/manual del usuario desde el menú de ayuda y navegar hasta Help > Download Help Manual.

La instalación de la CSLU requiere que acepte el Acuerdo de licencia.

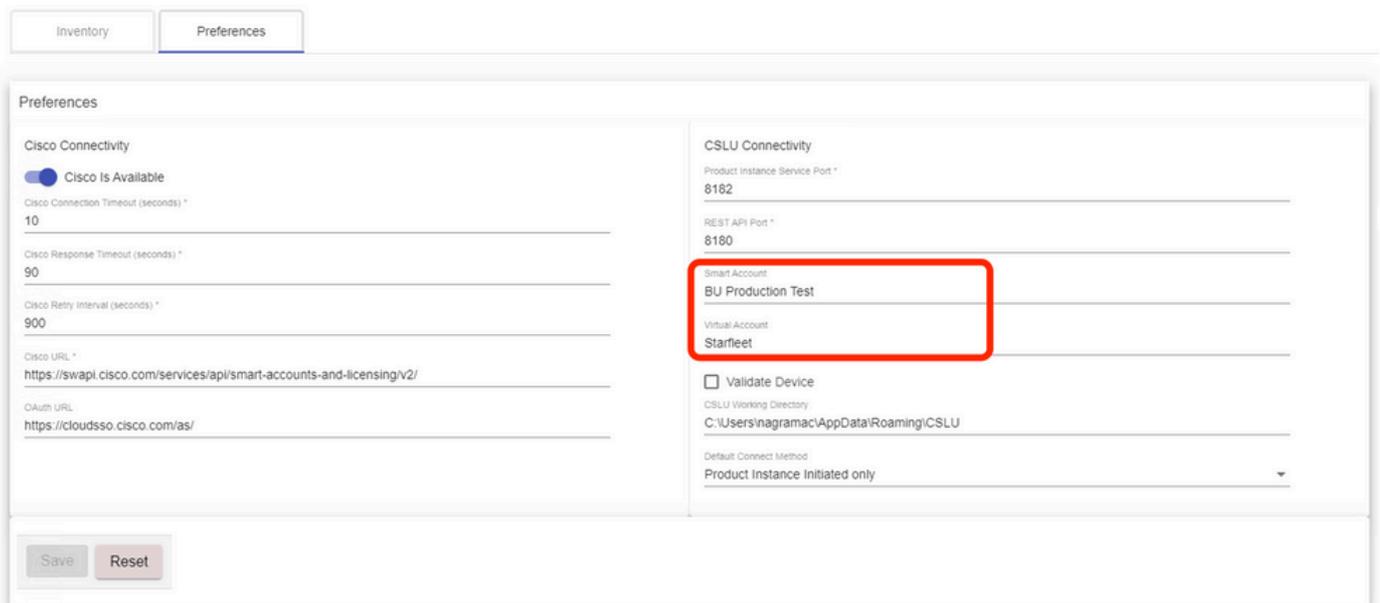
Se recomienda que la aplicación se instale únicamente para el usuario actual y no para todos los usuarios que trabajen en el equipo. Si una versión anterior de CSLU ya está presente en la PC, es recomendable desinstalarla de antemano. Sin embargo, la nueva instalación se encarga de actualizar el software.



Después de la instalación, inicie sesión en Cisco, con el uso de la opción de inicio de sesión presente en la esquina superior derecha de la aplicación. Utiliza sus credenciales de CEC. Y a través del login, se establece la confianza entre CSLU y CSSM.



Después de iniciar sesión en Cisco, asegúrese de que los detalles de SA y VA se han seleccionado correctamente en el menú desplegable del panel de preferencias de la herramienta. Asegúrese de guardar las configuraciones.



Ficha Programar en CSLU: a través de la ficha Programar en CSLU, puede configurar lo siguiente:

- Sondar CSSM para obtener los datos disponibles: muestra los tiempos de trabajo, la última hora de extracción y la siguiente hora de extracción de datos desde CSSM.
- Limpiar datos depurados: elimina todos los datos depurados del almacén de datos CSLU. También se puede activar manualmente.

- Datos del dispositivo de extracción: activa el modo de extracción CSLU.

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	<a href="#">Start</a>	
Operational Jobs				
Name	Status	Next Execution Time	Start	
Pull Device Data	scheduled	24-Feb-2023 01:14	<a href="#">Start</a>	

### CSLU con el modo PUSH

La CSLU funciona de forma predeterminada en el modo PUSH. En el modo PUSH, el PI envía los informes de uso a la CSLU a intervalos regulares. Desde el dispositivo, debe asegurarse de que el alcance de la red L3 a CSLU esté disponible. Para que el PI pueda comunicarse con la CSLU, se debe configurar la dirección IP de la máquina Windows que ejecuta la CSLU.

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>

Los informes se envían a la CSLU desde PI en las siguientes condiciones:

- En cada intervalo de informes predeterminado
- Recarga/Arranque en el dispositivo
- En Switchover
- Al agregar o quitar un miembro de la pila
- Al activar manualmente la sincronización de licencias

En la CSLU, la página de inventario enumera los dispositivos asociados actualmente con la CSLU. Los dispositivos de la lista se pueden identificar mediante el UDI. Los dispositivos se pueden filtrar según la PID o el SN de la lista para identificar cualquier dispositivo en particular.

La página de inventario de CSLU también tiene otras dos columnas:

- La columna **Último contacto** muestra la última marca de tiempo cuando el estado de los informes ha cambiado.
- La **Columna de Alerta** - Muestra el último estado del informe de PI.

Una vez que el PI envía el informe a la CSLU, la CSLU crea la entrada del PI en el CSSM. Se actualiza el TS del último contacto y el estado de las alertas.

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

CSSM procesa los informes enviados por CSLU y agrega/actualiza la instancia del producto en CSSM, en función del uso de la licencia. Una vez que el CSSM procesa y actualiza la fecha, devuelve el mensaje ACK a la CSLU. A su vez, la CSLU almacena y reenvía el mensaje de vuelta a PI.

El mensaje ACK consta de:

- Confirmación de todos los informes enviados
- Política
- Código de confianza

Si hay una nueva política disponible en el CSSM, ahora también se actualiza a la PI. Si la política no se modifica, se envía la misma a PI.



**Nota:** si no se requiere la notificación de mensajes ACK según su política, el mensaje ACK no se envía.

La columna de mensaje de alerta puede tener uno de estos estados:

- Informe de uso de la instancia del producto
- Informe de uso cargado en Cisco
- Solicitud de sincronización de la instancia del producto
- Solicitud de sincronización cargada en CSSM
- Reconocimiento recibido de CSSM
- Reconocimiento de informe de uso para instancia de producto



**Nota:** En CSLU en un sistema HA, siempre la entrada se ve solamente para UDI del activo. Solo CSSM tiene todos los UDI para dispositivos individuales en el sistema enumerado.

---

#### Detección automática de CSLU

Para permitir implementaciones a escala con configuraciones mínimas, se admite la detección automática de la CSLU. Esto significa que no tiene que configurar la dirección IP/URL de la CSLU específicamente. Para lograr esto, solo tiene que agregar una entrada a su servidor DNS. Esto permite que el dispositivo, que tiene el modo de transporte como CSLU (que es el predeterminado), detecte automáticamente CSLU y envíe informes.

Un par de cosas para asegurar aquí:

- Cree una entrada en el servidor DNS. La dirección IP de la CSLU debe asignarse al nombre `cslu-local`.
- Asegúrese de que el servidor de nombres y las configuraciones DNS están presentes en el dispositivo para que sean accesibles.

Con esto, sin ninguna configuración adicional, los dispositivos en la red pueden alcanzar CSLU y enviar informes RUM a intervalos regulares.

#### CSLU mediante el modo PULL

El modo PULL es donde la CSLU inicia el proceso para obtener los informes RUM de los dispositivos. Aquí los detalles del dispositivo se agregan a la CSLU y la CSLU obtiene los datos de todos los dispositivos agregados a intervalos regulares. La EXTRACCIÓN desde CSLU también se puede activar manualmente. La CSLU, a su vez, envía el informe RUM al CSSM, y los mensajes ACK que se reciben de vuelta desde el CSSM se envían a la PI. El modo PULL se admite por tres medios diferentes: RESTAPI, RESTCONF, y RESTCONF.

#### Modo PULL con RESTAPI

Para que el modo PULL funcione RESTAPI, las configuraciones requeridas del dispositivo y la CSLU son:

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  
!
```



**Nota:** el usuario debe tener acceso de nivel de privacidad 15.

---

CSLU: procedimiento de configuración

CSLU debe estar conectado a CSSM para que los informes se sincronicen automáticamente.

Paso 1. Seleccione Add Single Product en la página de inventario.

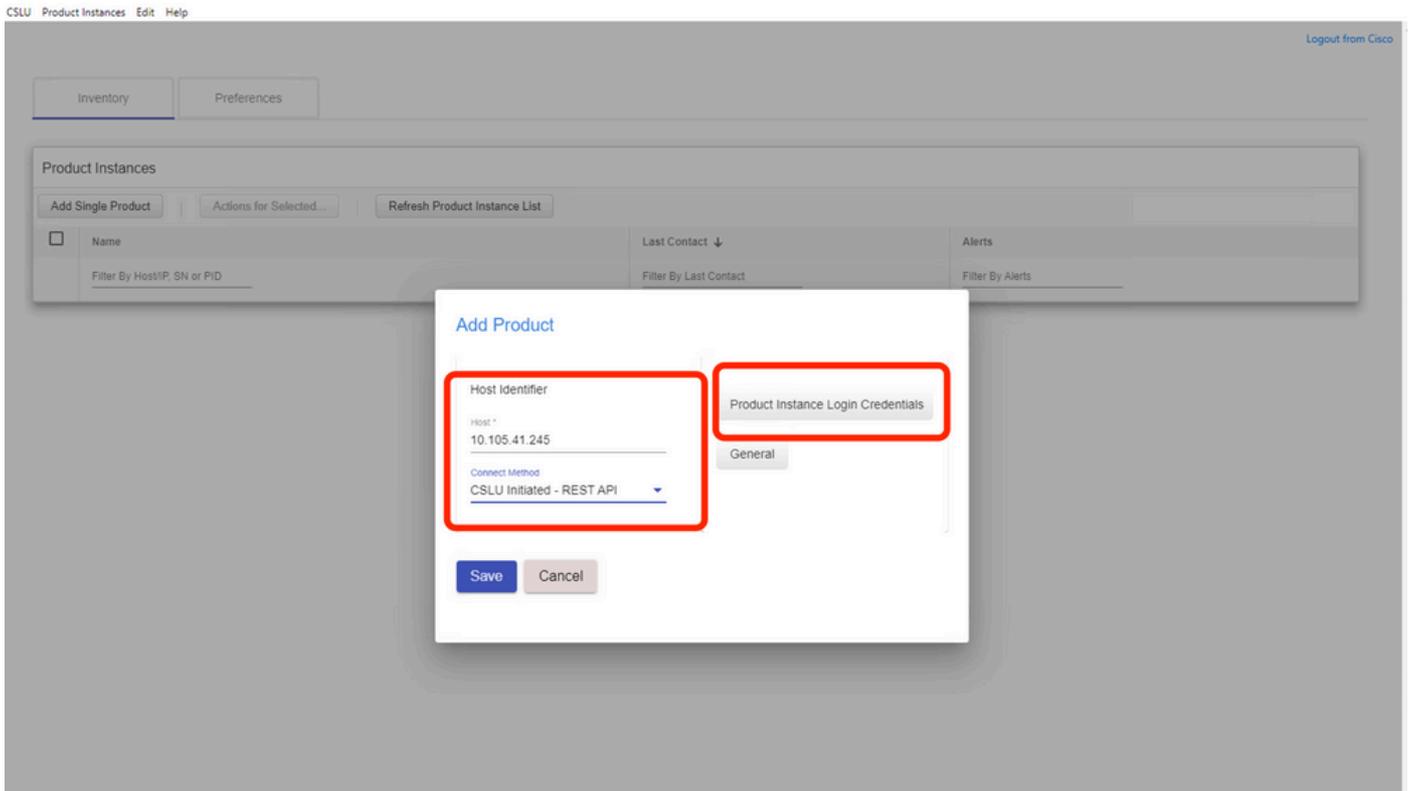
Paso 2. Introduzca la IP del dispositivo.

Paso 3. Elija el método de conexión como RestAPI.

Paso 4. Elija las credenciales de inicio de sesión de la instancia del producto.

Paso 5. Introduzca las credenciales del usuario con acceso Priv 15.

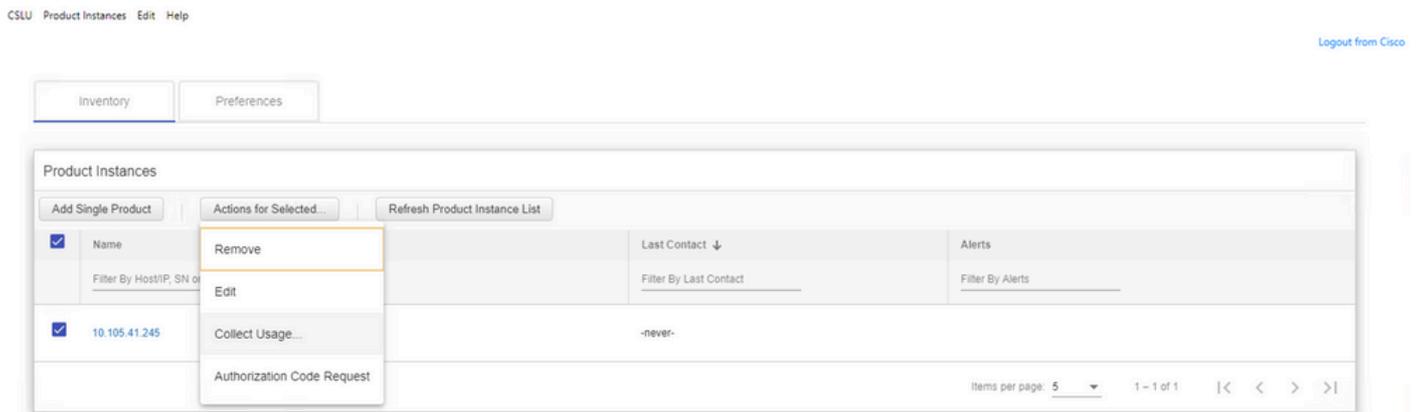
Paso 6. Guarde las configuraciones.



El dispositivo se agrega con una única dirección IP en el campo Nombre.

Elija el dispositivo y desplácese hasta **Actions for Selected > Collect Usage**.

Una vez recopilados correctamente los datos de uso, el campo Nombre se actualiza con el UDI de la PI y también se actualiza la marca de tiempo. El campo de alerta refleja el último estado.



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"/>			
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

Si el dispositivo sigue disponible cuando se recibe el mensaje ACK del CSSM, el ACK se devuelve al PI. De lo contrario, ACK se envía en el siguiente intervalo de extracción.

Modo PULL con RESTCONF

Para que el modo PULL funcione RESTCONF, las configuraciones requeridas del dispositivo y los pasos de la CSLU son:

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
!
```



**Nota:** Estas configuraciones son para la autenticación local. También se puede utilizar la autenticación remota.

CSLU: procedimiento de configuración

CSLU debe estar conectado a CSSM para que los informes se sincronicen automáticamente. La configuración de CSLU es la misma que RESTAPI para la recopilación y generación de informes de RUM.

Paso 1. Seleccione Add Single Product en la página de inventario.

Paso 2. Introduzca la IP del dispositivo.

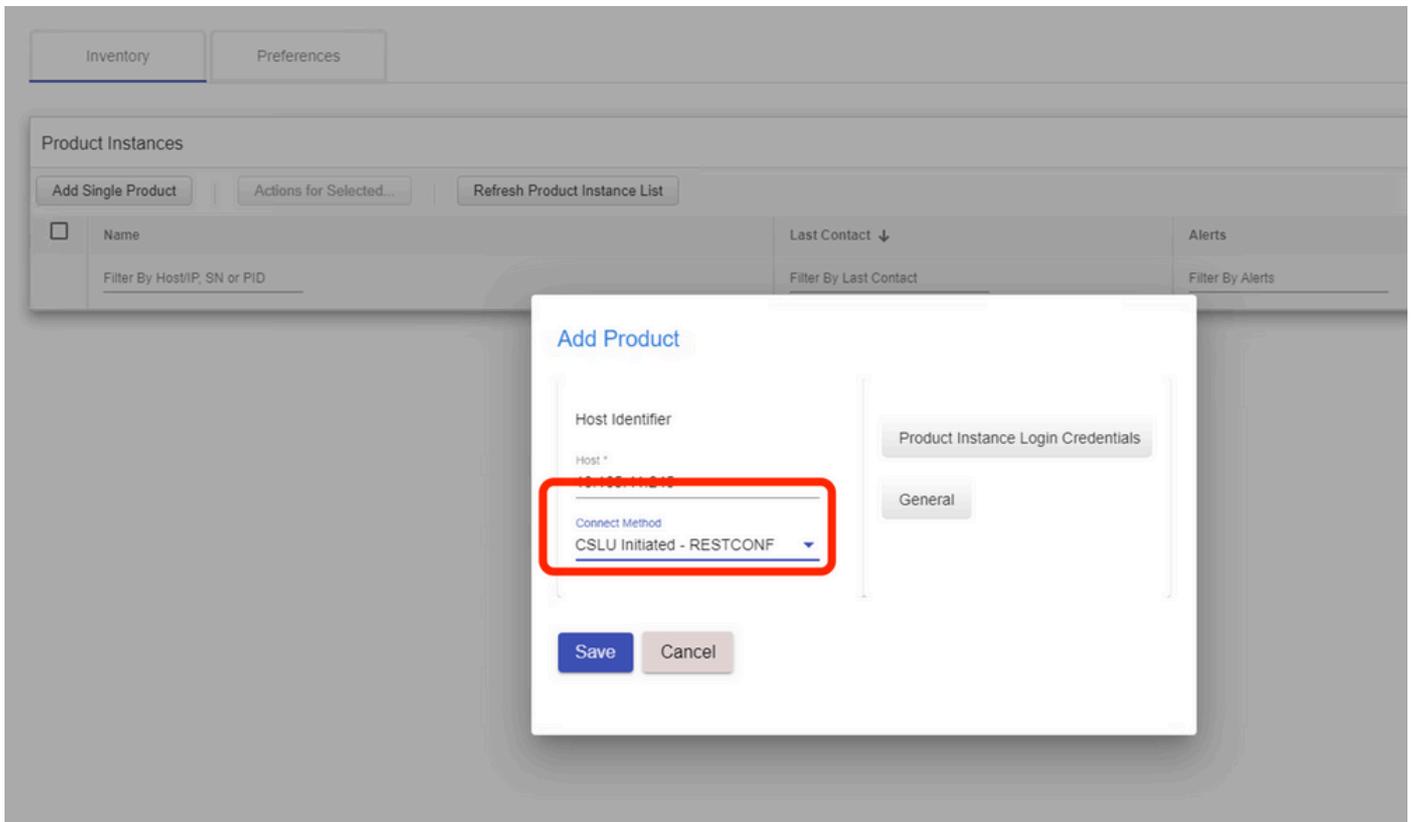
Paso 3. Elija el método de conexión como RESTCONF.

Paso 4. Elija las credenciales de inicio de sesión de la instancia del producto.

Paso 5. Introduzca las credenciales del usuario con acceso Priv 15.

Paso 6. Guarde las configuraciones.

Paso 7. Recopile los datos de uso del dispositivo seleccionado.



Modo PULL con NETCONF

Para que el modo PULL funcione NETCONF, las configuraciones requeridas del dispositivo y los pasos de la CSLU son:

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



**Nota:** Estas configuraciones son para la autenticación local. También se puede utilizar la autenticación remota.

CSLU: procedimiento de configuración

CSLU debe estar conectado a CSSM para que los informes se sincronicen automáticamente. La configuración de CSLU es la misma que RESTAPI para la recopilación y generación de informes de RUM.

Paso 1. Seleccione Add Single Product en la página de inventario.

Paso 2. Introduzca la IP del dispositivo.

Paso 3. Elija el método de conexión como NETCONF.

Paso 4. Elija las credenciales de inicio de sesión de la instancia del producto.

Paso 5. Introduzca las credenciales del usuario con acceso Priv 15.

Paso 6. Guarde las configuraciones.

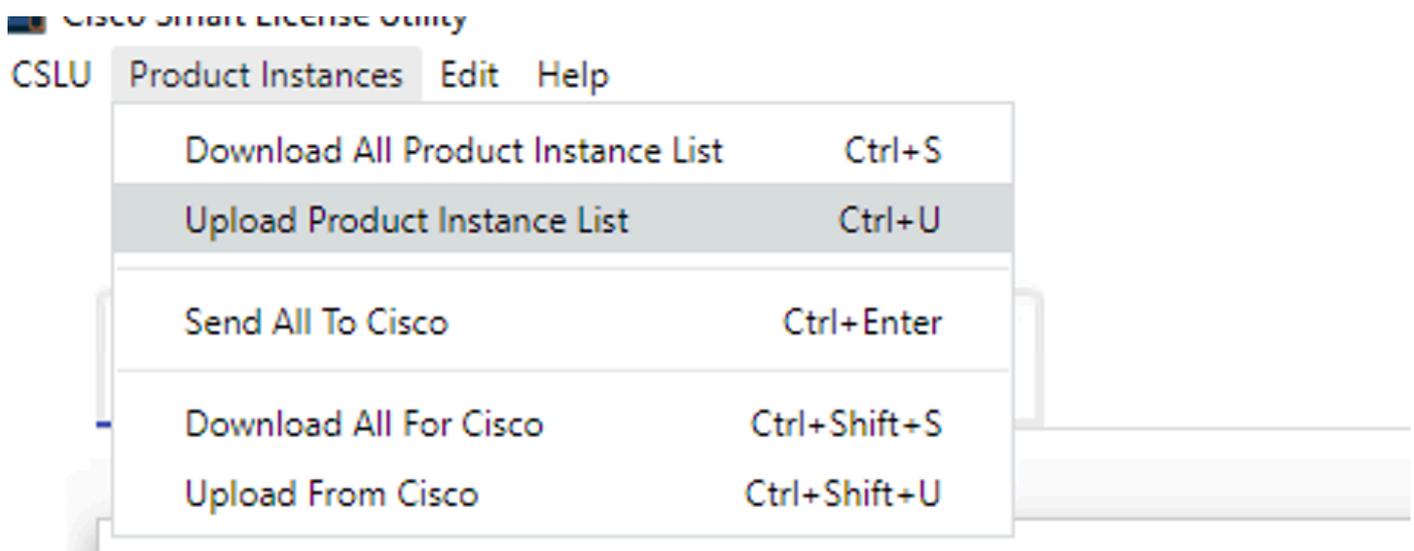
Paso 7. Recopile los datos de uso del dispositivo seleccionado.

The screenshot shows the 'Product Instances' management interface. At the top, there are buttons for 'Add Single Product', 'Actions for Selected...', and 'Refresh Product Instance List'. Below these are columns for 'Name', 'Last Contact', and 'Alerts', each with a filter option. A modal dialog titled 'Add Product' is open in the center. It has a 'Host Identifier' section with a 'Host \*' input field. Below that is a 'Connect Method' dropdown menu, which is highlighted with a red rectangular box. The dropdown shows 'CSLU Initiated - NETCONF' as the selected option. To the right of the dropdown are sections for 'Product Instance Login Credentials' and 'General'. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

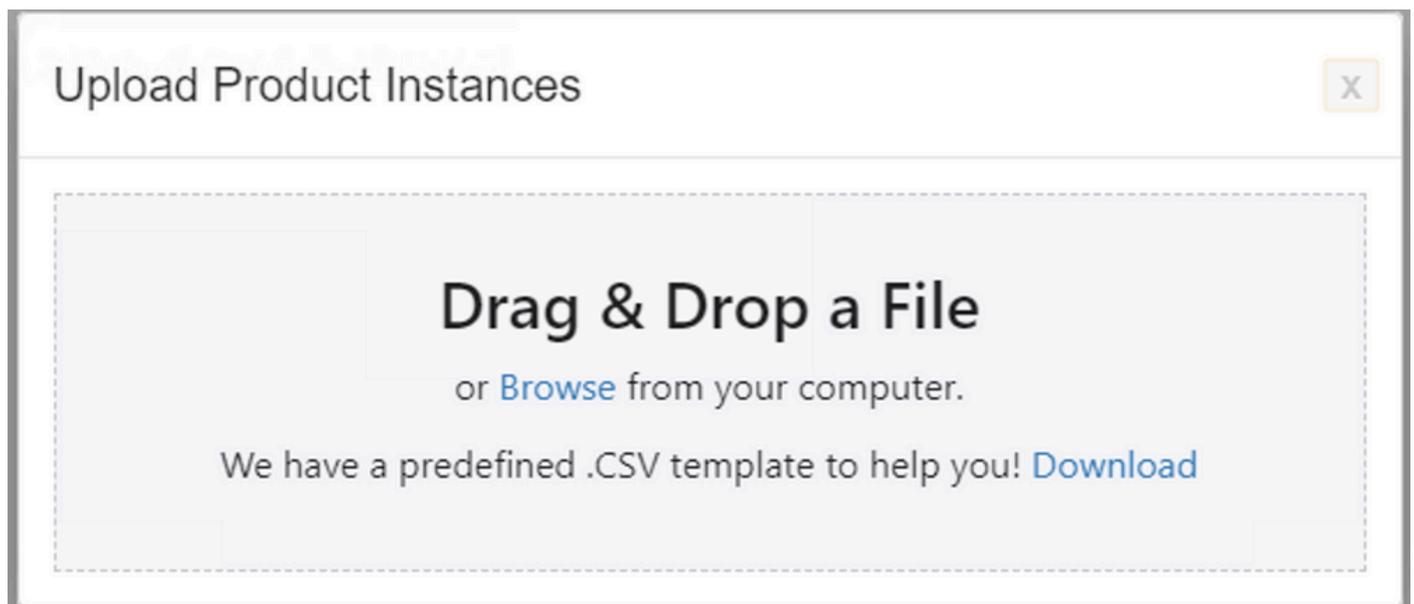


**Nota:** para todos los modelos, NETCONF, RESTCONF y RESTAPI, la lista de dispositivos se puede agregar de forma masiva.

Para realizar la carga masiva, en la Menu barra, navegue hasta Product Instance > Upload Product Instance List, como se muestra en esta imagen.



Se abre una nueva ventana emergente. El archivo de plantilla se puede descargar desde él. En el archivo con formato CSV, rellene los detalles del dispositivo de la lista de dispositivos y cárguelo en la CSLU para agregar varios dispositivos.



 **Nota:** Para todos los tipos de modo CSLU PULL, se recomienda configurar el transporte en Off en el PI. Esto se puede hacer con el uso de CLI.

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

CSLU con modo desconectado

La CSLU puede funcionar en modo desconectado desde el CSSM. Esto es para cualquier implementación que no permita que la CSLU esté conectada a Internet. En el modo desconectado, los informes de todos los dispositivos se descargan manualmente desde la CSLU y se cargan en

el CSSM. A su vez, los mensajes ACK se descargan desde CSSM y se cargan en CSLU. La CSLU continúa con las fechas de uso PULL/PUSH de los IP y también envía el mensaje ACK a PI.

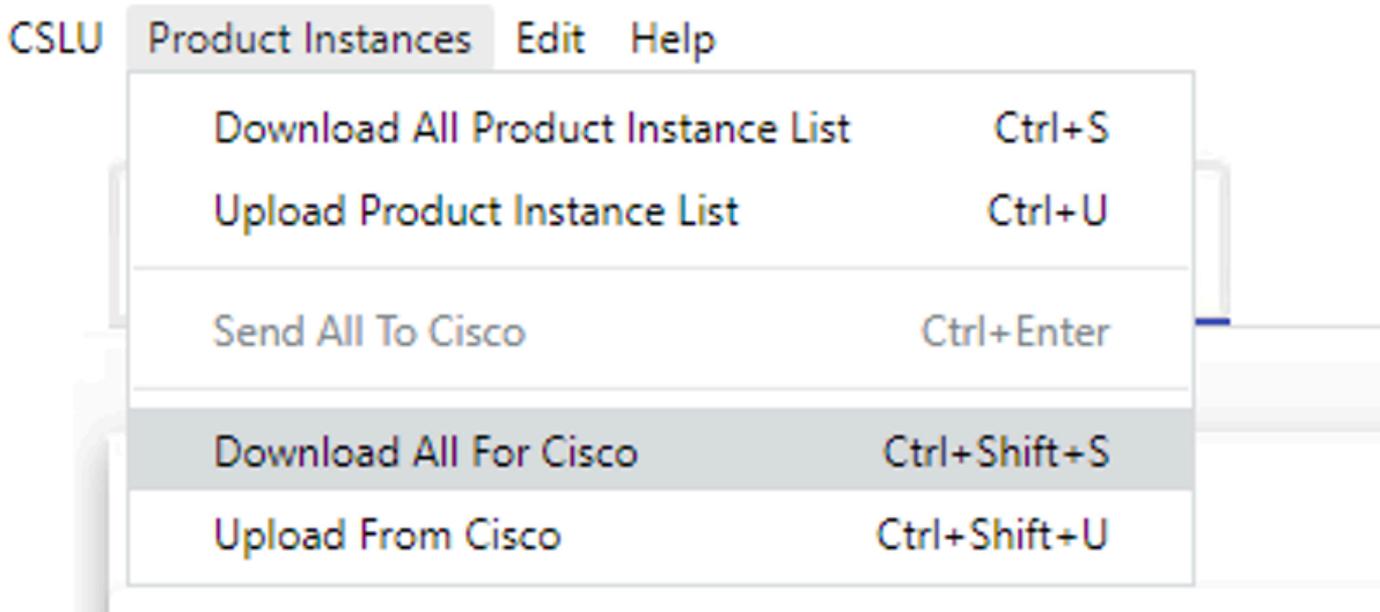
Paso 1. En la CSLU Preference página, desactive la opción Cisco Connectivity. Esto confirma que Cisco no está disponible.

Paso 2. Guarde las configuraciones.

CSLU Product Instances Edit Help

The screenshot shows the 'Preferences' page in the CSLU interface. The 'Cisco Connectivity' section is highlighted with a red box, showing a toggle switch for 'Cisco Is Not Available' which is currently turned off. Other settings include 'Cisco Response Timeout (seconds)' set to 10, 'Cisco Retry Interval (seconds)' set to 90, 'Cisco URL' as 'https://swapi.cisco.com/services/api/smart-accounts-and-licensing/v2/', and 'GAUTH URL' as 'https://cloudsso.cisco.com/as/'. The 'CSLU Connectivity' section on the right shows 'Product Instance Service Port' as 8182, 'REST API Port' as 8180, 'Smart Account' as 'BU Production Test', and 'Virtual Account' as 'Starfleet'. There is also a 'Validate Device' checkbox and a 'Default Connect Method' dropdown set to 'Product Instance Initiated only'. 'Save' and 'Reset' buttons are at the bottom left.

Paso 3. En la Menu barra, haga clic en Product Instances > Download All for Cisco. Esto descarga un tar.gz archivo a la CSLU.



Paso 4. Cargue el archivo en CSSM. En la página CSSM Smart Account, vaya a Report > Usage Data Files > Upload usage data. En la ventana emergente, cargue el tar.gz archivo.

## 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	<span style="color: blue;">i</span> No Errors	2	<a href="#">Download</a>
Usage_SLR.txt	2020-Oct-29	Quake	<span style="color: blue;">i</span> No Errors	1	<a href="#">Download</a>
<span style="color: blue;">+</span> UD_SA_BU_Production_Test_20Oct28_11_11_03	2020-Oct-28	DLC-VA1	<span style="color: blue;">i</span> No Errors	1	<a href="#">Download</a>
<span style="color: blue;">+</span> UD_SA_20Oct28_10_49_13_092.tar.gz	2020-Oct-28	DLC-VA1	<span style="color: blue;">i</span> No Errors	1	<a href="#">Download</a>
<span style="color: blue;">+</span> UD_SA_BU_Production_Test_20Oct28_10_46_25	2020-Oct-28	DLC-VA1	<span style="color: blue;">i</span> No Errors	1	<a href="#">Download</a>
Usage_17_3_2.txt	2020-Oct-28	Quake	<span style="color: blue;">i</span> No Errors	1	<a href="#">Download</a>
Usage_17_3_2.txt	2020-Oct-28	Quake	<span style="color: red;">x</span> Errors (1)	1	<a href="#">Download</a>
Usage_17_3_2.txt	2020-Oct-28	Quake	<span style="color: blue;">i</span> No Errors	1	<a href="#">Download</a>

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



Paso 5. Una vez que se procesan los datos, se genera el acuse de recibo. Descargue el archivo ACK y cárguelo en la CSLU.

## 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	<span style="color: blue;">i</span> No Errors	1	<a href="#">Download</a>

Paso 6. En CSLU, importe el archivo ACK desde la barra de menús y navegue hasta Product Instances > Upload from Cisco, como se muestra en esta imagen.

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)**

Paso 7. Una vez que se carga el ACK, el mensaje se envía a los IP. Lo mismo se puede comprobar en la columna Alertas.

CSLU | Product Instances | Edit | Help

Inventory | Preferences

Product Instances

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

Name	Last Contact ↓	Alerts
<input type="checkbox"/> UDI_PID:C9500-32QC; UDI_SN:CAT2148L15K	12-Nov-2020 01:10	<span style="color: green;">●</span> COMPLETE Usage report acknowledgement to product instance

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

## SLP - Modo sin conexión

SLP también puede funcionar en el modo sin conexión total. Esto es principalmente para las redes con espacios de ventilación, que no prefieren la conectividad a Internet y también optan por no utilizar CSLU. En el modo sin conexión, el transporte se establece en Off.

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>

Siempre que desee notificar los datos de uso a CSSM, los informes de uso deben descargarse como un archivo y cargarse manualmente en CSSM. En un sistema HA, active recopila el uso de los dispositivos miembro/en espera.

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

Ahora, este informe debe cargarse manualmente en CSSM.

Exporte los datos de uso guardados desde PI al escritorio.

En la página CSSM Smart Account, vaya a Report > Usage Data Files > Upload usage data. En la ventana emergente, seleccione el informe de uso y haga clic en upload.

Una vez cargado el archivo, debe elegir el dispositivo virtual correcto al que está asociado.

## 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

Una vez que los datos se procesan por completo y el reconocimiento está listo, descargue el archivo y cárguelo en el IP.

```
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

#### Cambios de comportamiento

Estos cambios se realizan en la función Smart Licensing en relación con las versiones:

- **Trust Sync:** desde la versión 17.7.1, Trust Code se instala en el switch en todas las topologías admitidas, como los métodos CSLU y Offline.
- **Cambios de privacidad** - Desde 17.7.1, la cadena de versión y la información del nombre de host desde 17.9.1 se incluyen en los informes RUM enviados a CSSM, si la configuración de privacidad respectiva está inhabilitada.
- **Detalles de la cuenta** - A partir de la 17.7.1, el mensaje ACK de CSSM incluye la información de la cuenta y los detalles de SA/VA.
- **Regulación de informes RUM** - A partir de la versión 17.9.1, se regula el intervalo de notificación de cuándo el IP inicia la comunicación. La frecuencia mínima de notificación se limita a un día. Esto significa que la instancia del producto no envía informes RUM más de una vez al día.

#### Troubleshoot

#### Cuestionario genérico de resolución de problemas

**Situación 1:** Algunos protocolos (es decir, HSRP) ya no funcionan después de actualizar el Cisco IOS XE desde una versión muy temprana (es decir, 16.9.x).

Verifique el nivel de arranque de la licencia para ver si sigue siendo el mismo que antes de actualizar Cisco IOS XE. Es posible que el nivel de arranque de la licencia se haya restablecido a Networking-Essentials, que posiblemente no admita los protocolos que fallan (es decir, HSRP).

**Situación 2:** estado de la licencia con los mensajes "Motivo del error: error al enviar el mensaje HTTP de Call Home" o "Último intento de comunicación: PENDIENTE"

Esto puede estar relacionado con problemas básicos de conectividad. Para resolver la comprobación:

- Conectividad de red para alcanzar el CSSM: dirección IP, rutas, etc.
- El ip http client source interface está configurado correctamente.
- Diferencia horaria. (El NTP debe configurarse para proporcionar una hora/zona de reloj correcta)
- Si la configuración interna del firewall bloquea el tráfico al CSSM

**Situación 3:** ¿Qué sucede si se observa el error de registro "%SMART\_LIC-3-AUTH\_RENEW\_FAILED: renovación de autorización con Cisco Smart Software Manager (CSSM): método no definido 'each' for nil:NilClass" después de un año de registro?

Vuelva a registrar el producto. Genere un nuevo ID de token en CSSM y registre de nuevo la instancia del producto en CSSM.

**Situación 4:** Mensaje de error "%SMART\_LIC-3-COMM\_FAILED: Error de comunicaciones", cuando no hay errores de conectividad con Cisco.

Cuando no hay problemas de conectividad con CSSM y si en PI, aún se ve el error mencionado, puede deberse a que la reciente actualización del servidor provocó la eliminación del certificado. El certificado es necesario para la autenticación TLS de los dos lados que se comunican. En ese caso, configure la CLI ip http client secure-trustpoint SLA-TrustPoint en la PI e inténtelo de nuevo.

Depurar PI

Para resolver cualquier problema, los comandos recopilados de PI son:

```
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

Debug CSLU

Si se depura algún problema en la CSLU, es importante que se tome el archivo de registro de este directorio en el equipo instalado en la CSLU.

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

Referencias relacionadas

- Migración a SL con políticas: [migración de licencias SL/SLR/PLR antiguas a SL con políticas](#)
- Notas de la versión: [RN-9200](#), [RN-9300](#), [RN-9400](#), [RN-9500](#), [RN-9600](#)
- Guías de configuración: [Cat9200-CG](#), [Cat9300-CG](#), [Cat9400-CG](#), [Cat9500-CG](#), [Cat9600-CG](#)
- Referencias de comandos: [Cat9200-CR](#), [Cat9300-CR](#), [Cat9400-CR](#), [Cat9500-CR](#), [Cat9600-CR](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).