

Solución de problemas de licencia inteligente con problemas de política en 9800

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Informes de uso de licencias](#)

[Informes RUM](#)

[Solución de problemas de comunicación de licencia inteligente 9800 con CSSM y servidor SSM en las instalaciones conectados directamente](#)

[Código de confianza](#)

[Inteligente con CSSM](#)

[Uso inteligente del proxy](#)

[SSM en las instalaciones](#)

[Transporte inteligente](#)

[SSM en las instalaciones](#)

[Probar conexión con Smart Receiver](#)

[Probar conexión al servidor SSM en las instalaciones](#)

[Buscar dirección IP del receptor](#)

[¿Cómo resuelve el sistema la dirección IP?](#)

[Código de confianza procesado desde CSSM no válido](#)

[Código de confianza válido procesado desde CSSM](#)

[Frecuencia de comunicación](#)

[Errores informados en el resultado de show license eventlog y/o show log](#)

[Depurar](#)

[Información Relacionada](#)

Introducción

Este documento describe los pasos avanzados de solución de problemas en la licencia inteligente mediante política (SLUP) en el controlador de LAN inalámbrica Catalyst 9800.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Licencias inteligentes mediante políticas (SLUP)

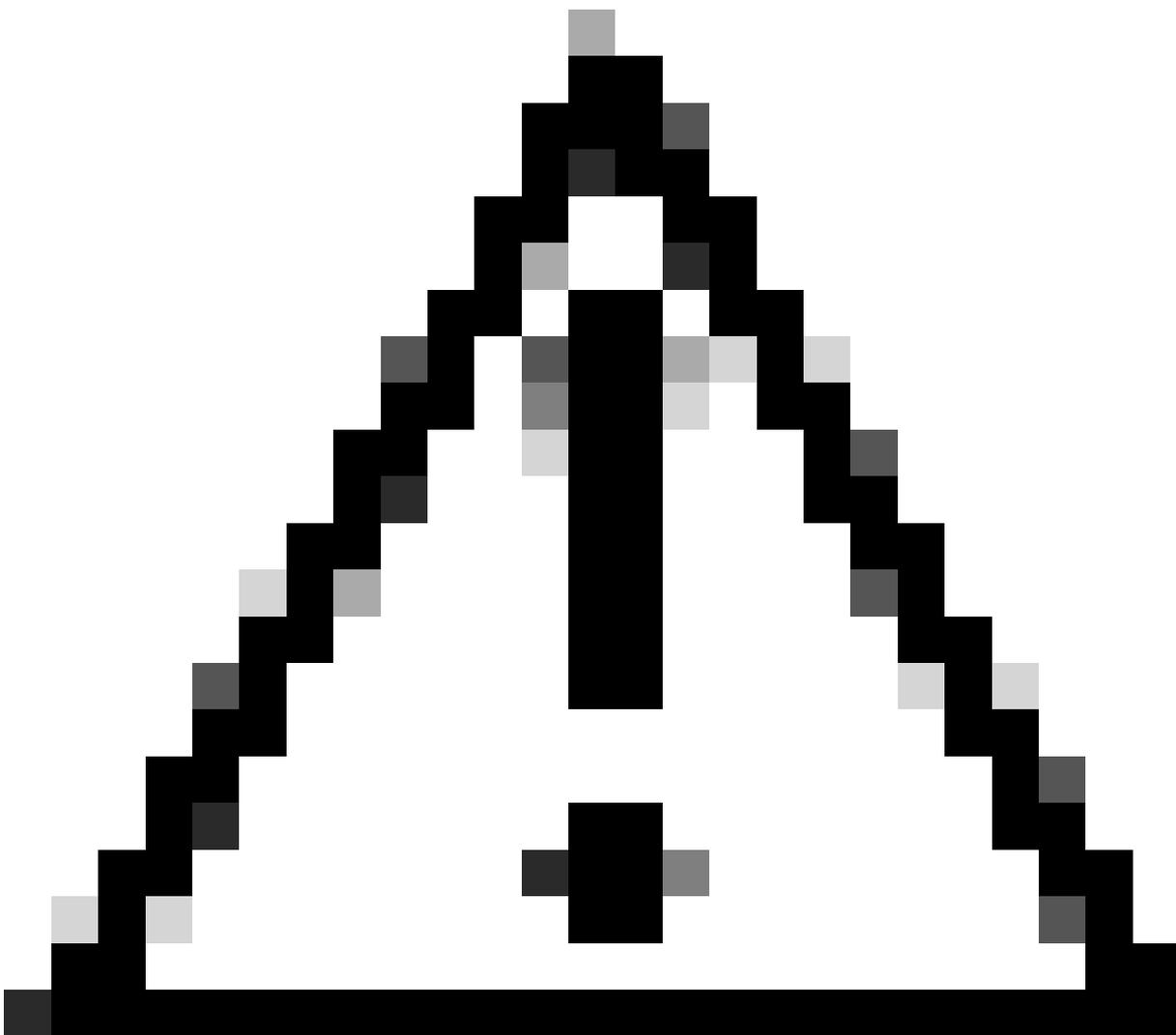
- Controlador de LAN inalámbrica (WLC) Catalyst 9800

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes



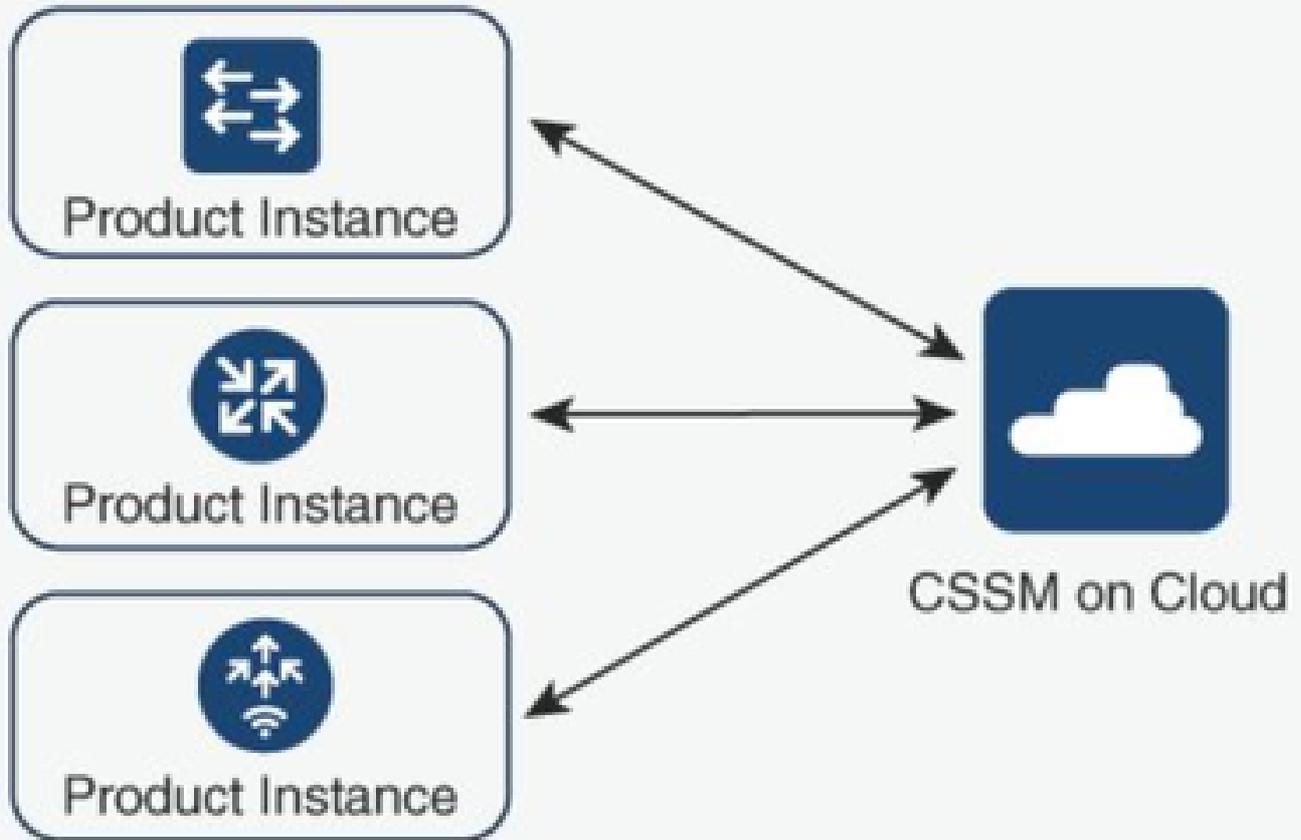
Precaución: Precaución: Las notas de este artículo contienen sugerencias útiles o referencias a material no incluido en el documento. Se recomienda que lea cada nota.

- **Uso:** No se aplican todas las licencias de los controladores inalámbricos Cisco Catalyst. Esto significa que no tiene que realizar ninguna operación específica de licencia, como registrar o generar claves antes de empezar a utilizar el software y las licencias vinculadas a él. El uso de la licencia se registra en su dispositivo con marcas de tiempo y los flujos de trabajo necesarios se pueden completar en una fecha posterior.
 - **Informe del uso de la licencia a CSSM:** Hay varias opciones disponibles para los informes de uso de licencias. Puede utilizar SSM On-Prem, Cisco Smart Licensing Utility (CSLU) o informar de la información de uso directamente a CSSM. En el caso de las redes con espacios aéreos, también está disponible una provisión para la generación de informes sin conexión en la que se descarga la información de uso y se carga en CSSM. El informe de uso está en formato XML de texto sin formato.
1. Conexión directa a [Cisco Smart Software Manager](#) Cloud (CSSM)
 2. Conectado a CSSM mediante [On-prem Smart Software Manager](#) (On-prem SSM)

Este artículo no cubre todos los escenarios de Smart Licensing en Catalyst 9800; consulte la [Guía de configuración de políticas de uso de Smart Licensing](#) para obtener información adicional. Sin embargo, este artículo proporciona una serie de comandos útiles para resolver problemas de conexión directa y SSM On-Prem Smart Licensing mediante problemas de política en el Catalyst 9800.

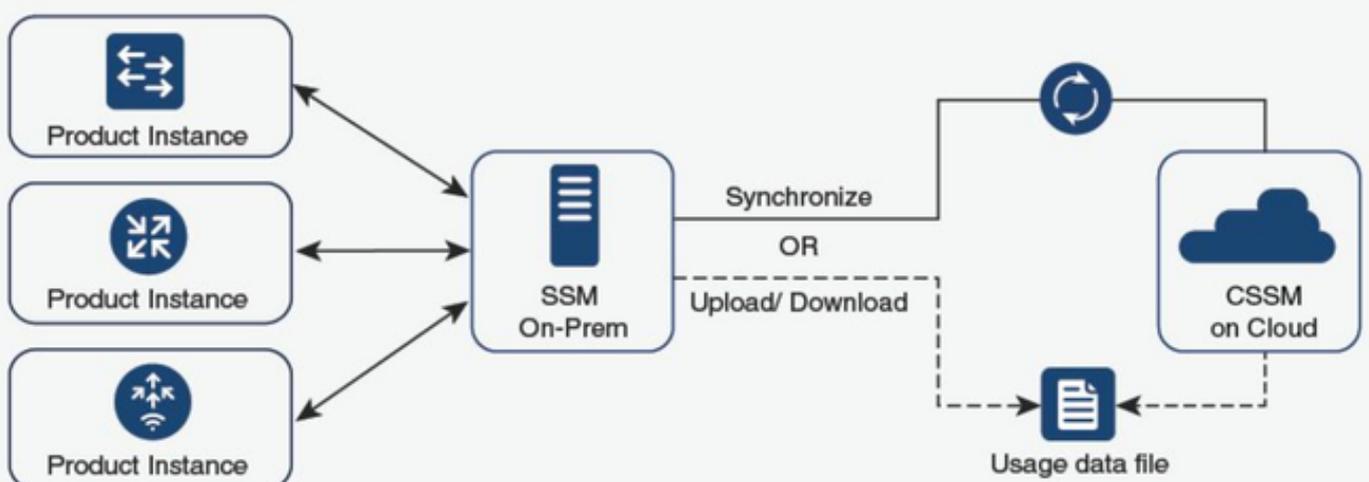
Opción 1. Conexión directa a Cisco Smart Licensing Cloud Servers (CSSM):

Directly Connected to CSSM



Opción 2. Conexión mediante On-prem Smart Software Manager (SSM in situ):

SSM On-Prem Deployment



Nota: Todos los comandos mencionados en este artículo son aplicables solamente a los WLC que ejecutan la versión 17.3.2 o posterior.

Informes de uso de licencias

Con SLP, la mayoría de las licencias no se aplican y se habilitarían en el dispositivo cuando se configure el paquete de funciones/tecnología. Las licencias correspondientes aparecerían en **show license summary** as **IN USE**.

9800-1#show license summary Account Information: Smart Account:

Virtual Account:

```
License Usage: License Entitlement Tag Count Status ----- lic_c9800l_perf
(LIC_C9800L_PERF) 1 IN USE air-network-advantage (DNA_NWStack) 2 IN USE air-dna-advantage (AIR-DNA-A) 2 IN USE
```

Los únicos 2 estados disponibles para una licencia son EN USO o NO EN USO. El estado viene determinado únicamente por la configuración y las funciones aplicadas en la instancia del producto.

Para cada licencia EN USO se crea un informe RUM independiente. Hay estados como CERRADO, ACK y ABIERTO para los informes de ron.

Opcional: Confirmado con un comando interno test license smart rum-report id:

```
Router(config)# service internal
```

```
Router# test license smart rum-report id
```

```
report_id:1624247687 state:SmartAgentRumStateOpen
```

a partir de las versiones 17.9: el comando show license rum id all:

```
Smart Licensing Usage Report: ===== Report Id, State, Flag, Feature Name 1682489268 CLOSED
P lic_c9800l_perf 1682489269 CLOSED P air-network-advantage 1682489270 CLOSED P air-dna-advantage 1682489271 CLOSED P air-
network-advantage 1682489272 CLOSED P air-dna-advantage 1682489273 ACK N lic_c9800l_perf
```

Informes RUM

Los informes de RUM o los informes de medición del uso de recursos son archivos de datos con información sobre el uso de licencias y la identidad de los dispositivos. Estos informes son informes de seguridad almacenados en el dispositivo y están firmados por el hardware.

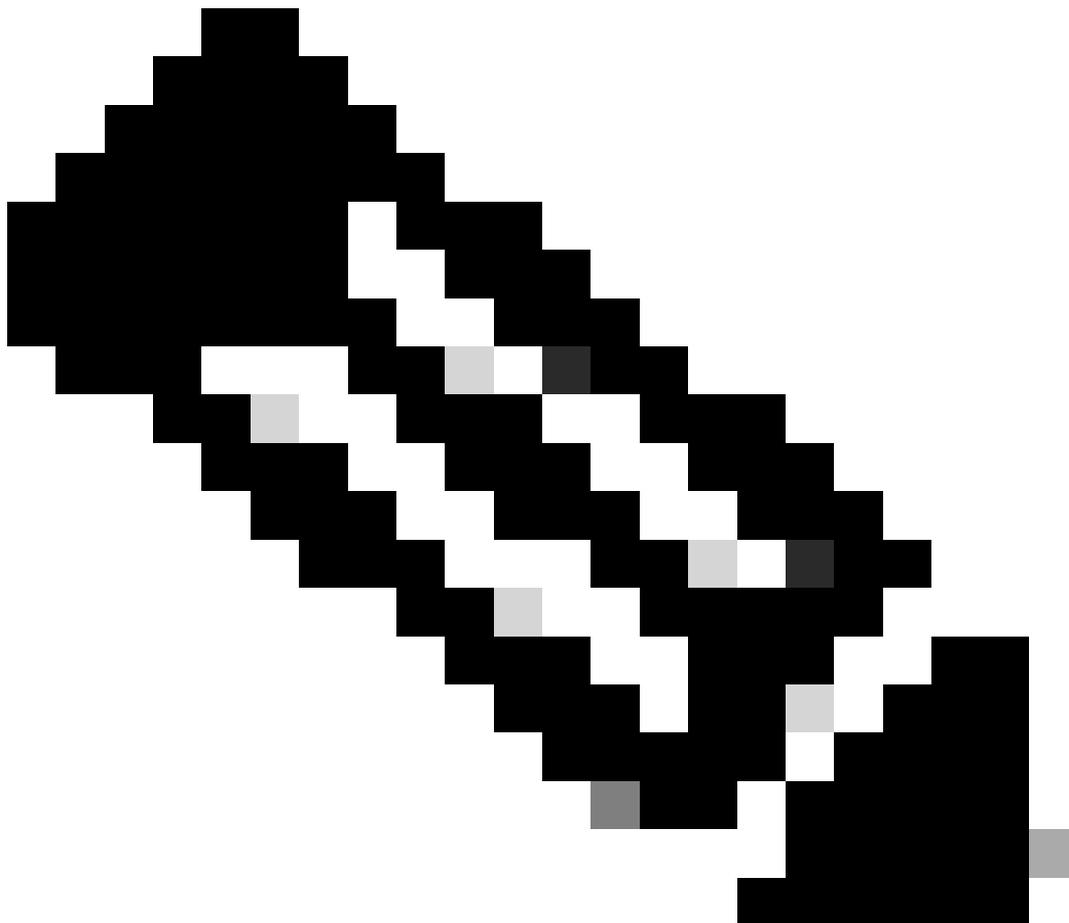
Los informes cambian de estado a lo largo de la comunicación entre la instancia del producto y CSSM.

Estado	Descripción
EstadoRumAgenteInteligenteAbierto	Nuevo informe creado por Smart Agent en el dispositivo
EstadoDeRumDeAgenteInteligenteCerrado	Informe RUM enviado al CSSM (las recargas también llevarían los informes abiertos al estado cerrado)
SmartAgentRumStateUnacknowledged	Informe RUM pendiente de confirmación de CSSM, ID de sondeo proporcionado
SmartAgentRumStateAcknowledged	Informe RUM enviado a CSSM y fue reconocido por ello

La función Smart Licensing Using Policy ha sido introducida en el Catalyst 9800 con la versión de código 17.3.2. La versión inicial 17.3.2 pierde el menú de configuración SLUP en el WLC webUI, que fue introducido con la versión 17.3.3. El SLUP es diferente de las licencias inteligentes tradicionales en un par de aspectos:

- El WLC ahora se comunica con el CSSM a través del dominio smartreceiver.cisco.com, en lugar del tools.cisco.com.

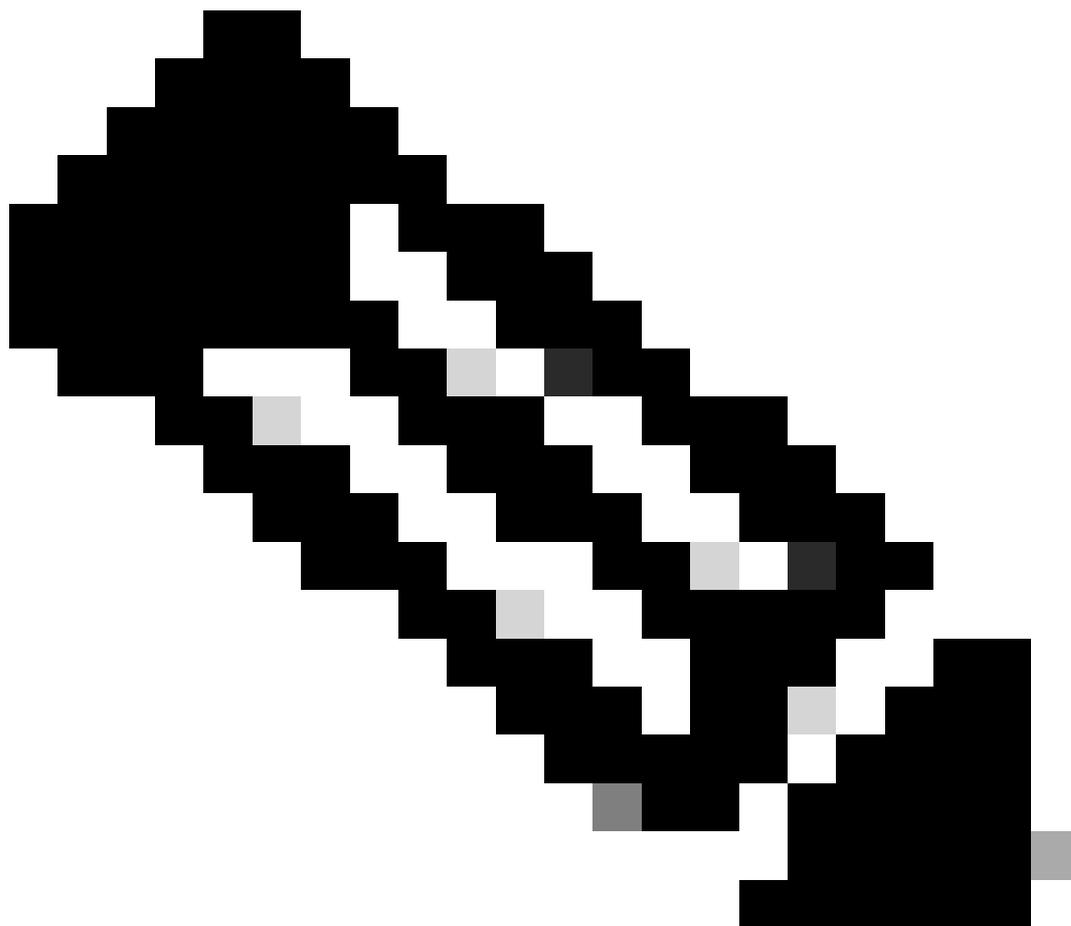
- En lugar de registrarse, el WLC ahora establece la confianza con el CSSM o SSM en las instalaciones.
 - Los comandos CLI se han alterado ligeramente.
 - La reserva de licencias inteligentes (SLR) ya no existe. En su lugar, puede informar periódicamente de su uso manualmente.
 - El modo de evaluación ya no existe. El WLC continúa funcionando a plena capacidad incluso sin licencia. El sistema se basa en el honor y se supone que debe informar sobre el uso de su licencia periódicamente (automática o manualmente en el caso de redes con espacios de ventilación).
-



Nota: Advertencia: Si utiliza un controlador inalámbrico Cisco Catalyst 9800-CL, asegúrese de estar familiarizado con el requisito obligatorio ACK que comienza con Cisco IOS® XE Cupertino 17.7.1. Consulte RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller.

* Un nuevo controlador 9800 debe cumplir con ciertos procedimientos para que se complete el flujo de trabajo de licencias inteligentes.

1. Cree un token desde el portal CSSM e impórtelo para establecer una ID de confianza necesaria para obtener la autorización para los informes de uso de licencias en el futuro. Este valor de ID de confianza es la clave para que CSSM valide el informe enviado desde el controlador 9800. Este token de confianza se actualizaría periódicamente y se intercambiaría como parte de los informes de uso de Rum con CSSM.



Nota: A partir de Cisco IOS XE Cupertino 17.7.1, se requiere un código de confianza. El código de confianza se establece por número de serie, por lo que la configuración de SSO de 9800 HA tendría 2 códigos de confianza instalados.

Código de confianza

Una clave pública vinculada a UDI, que la instancia del producto utiliza para:

- Firma un informe RUM. Esto evita la manipulación y garantiza la autenticidad de los datos.
- Habilite la comunicación segura con CSSM.

A partir de Cisco IOS XE Cupertino 17.7.1, se obtiene automáticamente un código de confianza en las topologías en las que la instancia del producto inicia el envío de datos a CSLU y en las topologías en las que la instancia del producto se encuentra en una red con brechas de aire.

- Se puede obtener un código de confianza de CSSM, mediante un token de ID.

Aquí se genera un token de ID en la interfaz de usuario web de CSSM para obtener un código de confianza e instalarlo en la instancia del producto. Debe sobrescribir el código de confianza instalado de fábrica si lo hay. Si una instancia de producto está conectada directamente a CSSM, utilice este método para permitir que la instancia de producto se comunique con CSSM de forma segura. Este método de obtención de un código de confianza es aplicable a todas las opciones de conexión directa a CSSM. Para obtener más información, consulte [Conectado directamente a CSSM](#).

Desde Cisco IOS XE Cupertino 17.9.1, se obtiene automáticamente un código de confianza en las topologías en las que la CSLU inicia la recuperación de datos de la instancia del producto.

Si hay un código de confianza instalado de fábrica, se sobrescribe automáticamente. Un código de confianza obtenido de esta manera se puede utilizar para una comunicación segura con CSSM.

* Asegúrese de que la configuración del 9800 para las licencias inteligentes está intacta. 9800 utiliza Smart como transporte para comunicarse con CSSM.

Inteligente con CSSM

```
Device(config)#license smart transport smart Device(config)#license smart url https://smartreceiver.cisco.com/licservice/license
```

Uso inteligente del proxy

```
license smart proxy { address address_hostname| port port_num } Device(config)#license smart url default Device(config)#license smart proxy address
```

```
Device(config)#license smart proxy port
```

SSM en las instalaciones

```
Device(config)#license smart transport cslu Device(config)#license smart url cslu https://SSM-Onprem-FQDN-address>/cslu/v1/pi/ssmsfloodingslup2304-1
```

Asegúrese de que la búsqueda de dominio y el servidor de nombres sean accesibles a través de la interfaz de origen.

Device(config)#ip domain name

Device(config)#ip name server

Device(config)#ip domain lookup

El comando show license all devuelve el tipo de transporte y los detalles de URL configurados en 9800: Asegúrese de que la configuración es absoluta.

Transporte inteligente

Type: Smart URL: <https://smartreceiver.cisco.com/licservice/license> Proxy: Not Configured VRF:

SSM en las instalaciones

Transport: Type: cslu Cslu address: <https://SSM-Onprem-FQDN-address>/cslu/v1/pi/ssmsfloodingslup2304-1>

* si hay algún proxy entre 9800 y CSSM, asegúrese de permitir la dirección IP indicada en el proxy para una comunicación perfecta.

Probar conexión con Smart Receiver

Utilice el comando curl:

- curl <https://smartreceiver.cisco.com/licservice/license>
- Respuesta esperada: ¡Este es el Smart Receiver!

Probar conexión al servidor SSM en las instalaciones

Utilice el comando curl:

- curl -v -k <https://SSM-Onprem-FQDN-address>/cslu/v1/pi/ssmsfloodingslup2304-1>
- Respuesta esperada: ¡Este es el Smart Receiver!

Buscar dirección IP del receptor

Utilice este comando nslookup:

- nslookup smartreceiver.cisco.com

Respuesta esperada:

- Servidor: 171.70.168.183 ← Este es el servidor DNS

- Servidor: dns-sj.cisco.com ← Opcionalmente, se puede mostrar
- Dirección: 10.10.10.10#53
- Nombre: smartreceiver.cisco.com
- Dirección: 146.112.59.81
- Nombre: smartreceiver.cisco.com
- Dirección: 2a04:e4c7:ffe::f

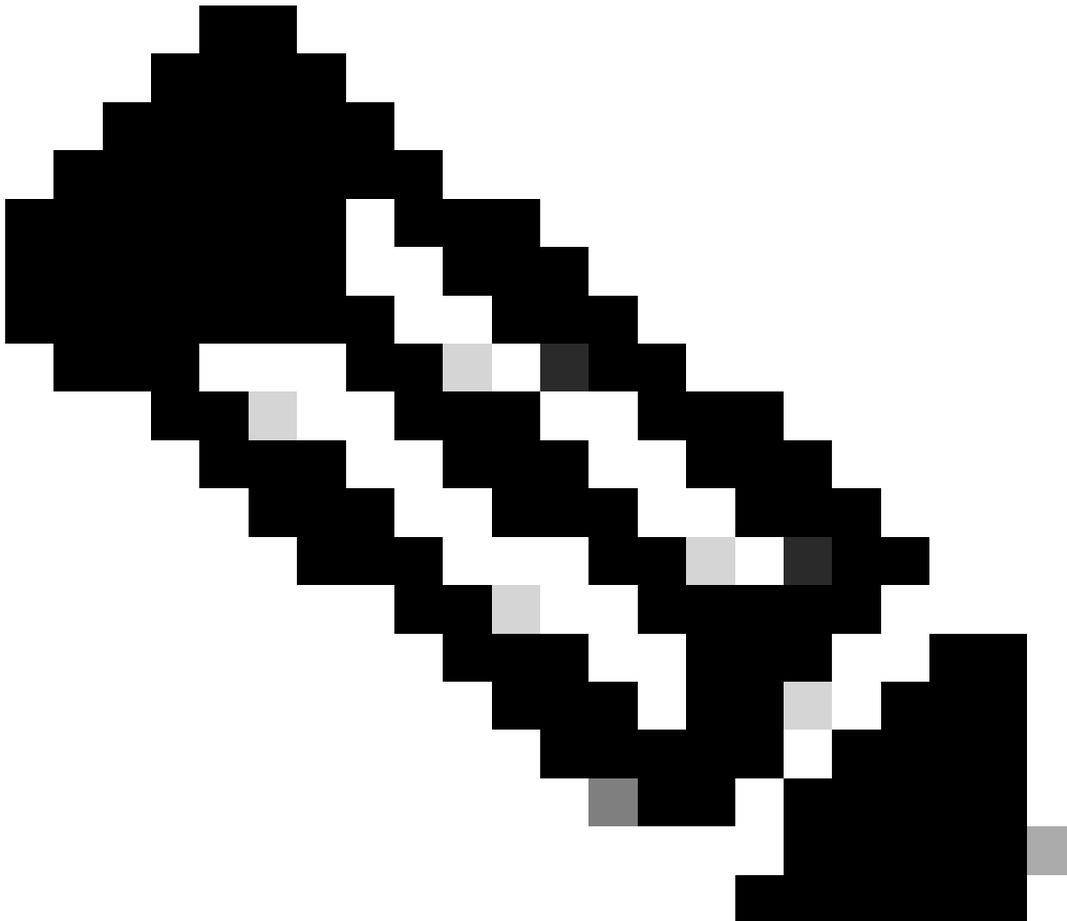
¿Cómo resuelve el sistema la dirección IP?

Utilice el comando dig:

- dig smartreceiver.cisco.com + short

Resultado esperado

- 146.112.59.81



Nota: El componente Smart Receiver de CSSM ha sustituido al antiguo tools.cisco.com y

a un único punto de contacto para la elaboración de informes, el registro y la facturación de los clientes de MSLA.

ip http client source-interface <source-interface>

Este comando marca explícitamente la trayectoria de origen al CSSM.

ip http client secure-trustpoint SLA-TrustPoint

Asegúrese de que secure-trustpoint esté seleccionado como SLA-TrustPoint, ya que está firmado por la CA raíz de licencias. Tanto SSM en las instalaciones como CSSM son de confianza gracias al certificado de CA raíz de licencias.

Certificado de CA:

Estado: Disponible

Número de serie del certificado (hex): 01

Uso del certificado: Firma

Emisor:

cn=CA raíz de licencias de Cisco

o=Cisco

Asunto:

cn=CA raíz de licencias de Cisco

o=Cisco

Fecha de validez:

fecha de inicio: 19:48:47 UTC 30 de mayo de 2013

fecha de finalización: 19:48:47 UTC 30 de mayo de 2038

Puntos de confianza asociados: SLA-TrustPoint de Trustpool

Almacenamiento: nvram:CiscoLicensi#1CA.cer

License smart sync all es el comando para iniciar un nuevo informe Rum desde el controlador 9800 y el formato XML. Cuando este comando se ejecuta en el controlador donde el código de confianza no está instalado en la versión 17.9.x, primero genera una solicitud para el código de confianza en lugar del informe de uso de Rum.

Código de confianza procesado desde CSSM no válido

Importar CÓDIGO DE CONFIANZA:

Recibido el 17 de septiembre de 2024 17:35:26 UTC

```
<smartLicenseTrust><trustCode><udi>P:C9800-L-F-K9,S:FCL2630000P</udi><status><success>>false</success><message>Ya se ha procesado para este dispositivo una solicitud de confianza correspondiente a un id de confianza superior.</message><code>OLD_TRUST_ID</code><correlationID>>null-null</correlationID></status></trustCode><signature>MEQCIAg71/hlcWxUiiof8VstpmPhRH8jptPZPrvaSpsuwVgLAiAQ3IUVMuS8bOHwySOB/j/3RmG4uSDq/EbUp+vfrYD9nQ==</signature></smartLicenseTrust>
```

CSSM espera que el controlador envíe el id de código de confianza incremental como un propósito de seguridad y la implicación de un código de confianza no válido detendría a CSSM para procesar las solicitudes RUM de licencias del controlador. Esto finalmente resultaría en un problema de administración de licencias en el panel de licencias CSSM.

Código de confianza válido procesado desde CSSM

Importar CÓDIGO DE CONFIANZA:

```
<smartLicenseTrust><trustCode><udi>P:C9800-L-F-K9,S:XXXXXXXXXX</udi><customerInfo><smartAccount>Cuenta inteligente interna de demostración de Cisco</smartAccount><virtualAccount>0Demo-HK-PartnerA</virtualAccount></customerInfo><piid>0eb1d627-bbed-46a8-9a4b-fc5b48a7c36b</piid id><dateStamp>2024-09-10T07:21:30</dateStamp></subCA><trustId>110</trustId><status><success>>true</success><correlationID>>null</correlationID></status></trustCode><signature>MEUCIGMPyt6VEmv/DMziybLDnsHRZAxfl1r1vI3BBNtrdpBtAiEAojAqDYkGn206meTHt8+dqra0LAcIHEZKxmqeurKOU0g=</signature></smartLicenseTrust>
```

Frecuencia de comunicación

El intervalo de informe que puede configurar en CLI o GUI no tiene ningún efecto.

El WLC 9800 se comunica con el CSSM o con el administrador de software inteligente en las instalaciones cada 8 horas, sin importar el intervalo de informes que se configure a través de la interfaz web o la CLI. Esto significa que los puntos de acceso recién incorporados pueden aparecer en el CSSM hasta 8 horas después de haberse incorporado inicialmente.

Puede averiguar la próxima vez que se calculen y notifiquen las licencias con el comando `show license air entity summary`. Este comando no es parte de la salida típica de `show tech` o `show license all`:

comando `show license air entities summary`:

```
Last license report time.....: 10:00:07.753 UTC Mon Sep 16 2024 Upcoming license report time.....: 18:00:07.808 UTC
Mon Sep 16 2024 No. of APs active at last report.....: 3 No. of APs newly added with last report.....: 1 No. of APs deleted with last
report.....: 0
```

El código de confianza posterior se ha instalado correctamente en el controlador 9800. La siguiente fase consiste en generar el informe de uso de la actividad de la licencia a través de Rum (Unidad de medida de recursos) en formato XML. El comando License smart sync all/local iniciaría o generaría o abriría una nueva medición de Rum basada en el AP administrado en el controlador. Básicamente, el componente 9800 Smart Agent envía una llamada API al módulo de licencias para recopilar un nuevo informe de Rum con información sobre licencias.

comando show license rum id all:

This command would list CLOSED, ACK and OPEN state of Rum report on the controller. 1719005447 OPEN N air-network-advantage
1719005448 OPEN N air-dna-advantage

comando show license rum id 1719005447 detail:

Puede obtener detalles de la licencia notificada en ID de Rum. Este comando extrae software_identifier_tag, que es el elemento clave coincidente en la base de datos CSSM para validar un tipo de licencia de una instancia de producto.

regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896

Detalles del informe de uso de licencias inteligentes:

=====

ID del informe: 1719005447

Nombre de métrica: DERECHO

Nombre de la función: air-network-advantage

Valor de métrica: regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896

UDI: PID:C9800-L-F-K9,SN:FCL2630000P

ID del informe anterior: 1719005445, ID del siguiente informe: 0

Estado: ABIERTO, Motivo del cambio de estado: Ninguno

Motivo del cierre: Ninguno

Hora de inicio: 10 de septiembre 10:00:08 UTC de 2024, Hora de finalización: 16 de septiembre 16:15:08 UTC de 2024

Estado de almacenamiento: EXISTIR

ID de la transacción: 0

Mensaje de transacción: <none>

* Ahora, se genera el informe Rum. En el estado OPEN, se debe enviar al CSSM correctamente

para recibir el ACK del CSSM.

A) Verify which licenses are activated/in use - show version - show license summary - show license usage <<< it would also indicate which licenses are Perpetual vs Subscription C) Verify if enforced/export controlled license is authorized: - show license authorization D) Verify what messages were sent to/received from SSM On-Prem/CSSM - show license history message E) Check for errors - show license eventlog F) Collect detailed information/counters: - show license tech support G) Collect license tech support file - show tech-support license

Errores informados en el resultado de show license eventlog y/o show log

"Fallo de comunicaciones con Cisco Smart License Utility (CSLU): No se ha facilitado información detallada"

Este error se puede observar cuando no se estableció la comunicación HTTPS con On-Prem.
Motivos potenciales:

- Se utiliza un VRF específico para la comunicación con OnPrem. La interfaz de origen del cliente HTTP debe configurarse manualmente
- La comprobación de revocación NO está inhabilitada en la configuración SLA-Trustpoint
- Otro punto de confianza se establece como el valor predeterminado para la señalización criptográfica (por ejemplo: en el gateway SIP)

"Error 502 del servidor HTTP: Puerta de enlace incorrecta"

Este error está siendo investigado actualmente por el equipo de desarrollo local. En la mayoría de los casos no se observa ningún impacto en el servicio.

Normalmente, 10 segundos después, SAVE_COMM_RESTORED.

Ejemplo:

```
9 de julio 13:15:29.902: %SMART_LIC-3-COMM_FAILED: Fallo de comunicaciones con la utilidad
Cisco Smart License Utility (CSLU): Error 502 del servidor HTTP: Gateway incorrecto
9 jul 13:15:39.881: %SMART_LIC-5-COMM_RESTORED: Comunicaciones con Cisco Smart
License Utility (CSLU) restauradas
```

"Error 404 del servidor HTTP: Not found"

Este error se observa en el dispositivo Cisco IOS XE cuando se intentó instalar el código de confianza mientras la URL de transporte señalaba a la CSLU (On-Prem).

El comando "license smart trust idtoken <token> [all|local]" SÓLO se utiliza cuando el dispositivo se comunica directamente con CSSM.

NOTE: En función de la plataforma, este mensaje también puede significar que la opción "Validar dispositivo" está activada en el panel de configuración de CSLU del espacio de trabajo de administración local. Compruebe si el dispositivo que está intentando registrar se encuentra en la

ficha "SSL con la política" del servidor local. Si los dispositivos no se encuentran en esa ficha, deberá desactivar este botón. A continuación, intente que el dispositivo se sincronice de nuevo con el servidor en las instalaciones. Para ver una imagen de esta configuración, consulte el final de este artículo.

SAVE_INIT_CRYPTO success="Falso" error="La inicialización de criptografía no se ha completado"

Este error se puede observar poco después de que se inicie el sistema. Después de aproximadamente 30 segundos, la inicialización de criptografía se completa, en tal caso no hay impacto en el servicio.

Ejemplo:

```
2012-06-25 10:09:23.378 UTC SAVE_INIT_SYSTEM_INIT
2012-06-25 10:09:24.383 UTC SAVE_INIT_CRYPTO success="Falso" error="La inicialización
criptográfica no se ha completado"
2012-06-25 10:09:54.383 UTC SAVE_INIT_CRYPTO success="Verdadero"
```

Si la inicialización criptográfica no se completa durante varios minutos/horas, verifique si la configuración NTP está presente y/o si los relojes están sincronizados. Guardar la configuración en ejecución ayuda a reiniciar la inicialización criptográfica.

Se recomienda investigar más con el TAC de Cisco si el problema continúa.

SAVE_UTILITY_RUM_FAIL error="[HOST_NOT_FOUND] No se ha encontrado el host del dispositivo"

Lo más probable es que la configuración "Validar dispositivo" esté establecida en el panel de configuración de CSLU en el espacio de trabajo de administración local.

Esta configuración ayuda a garantizar que se reciben los informes de RUM de instancias de productos conocidas.

SAVE_COMM_FAIL error="No se puede resolver el nombre de host/nombre de dominio del servidor"

Este error indica un problema de conectividad que puede originarse con la resolución DNS. Debe asegurarse de que el dispositivo puede resolver la URL de destino. Por lo general, el comando `ip host <url> <ipassociated>` está mal configurado. Compruebe este punto.

Lo más probable es que encuentre un fallo de comunicación.

Estadísticas de comunicación:

=====

Nivel de comunicación permitido: INDIRECTO

Estado general: <empty>

Establecimiento de confianza:

Intentos: Total=30, Satisfactorio=0, Fallo=30 Fallo continuo: Global=30 Comunicación=30

<<<<<<<<<

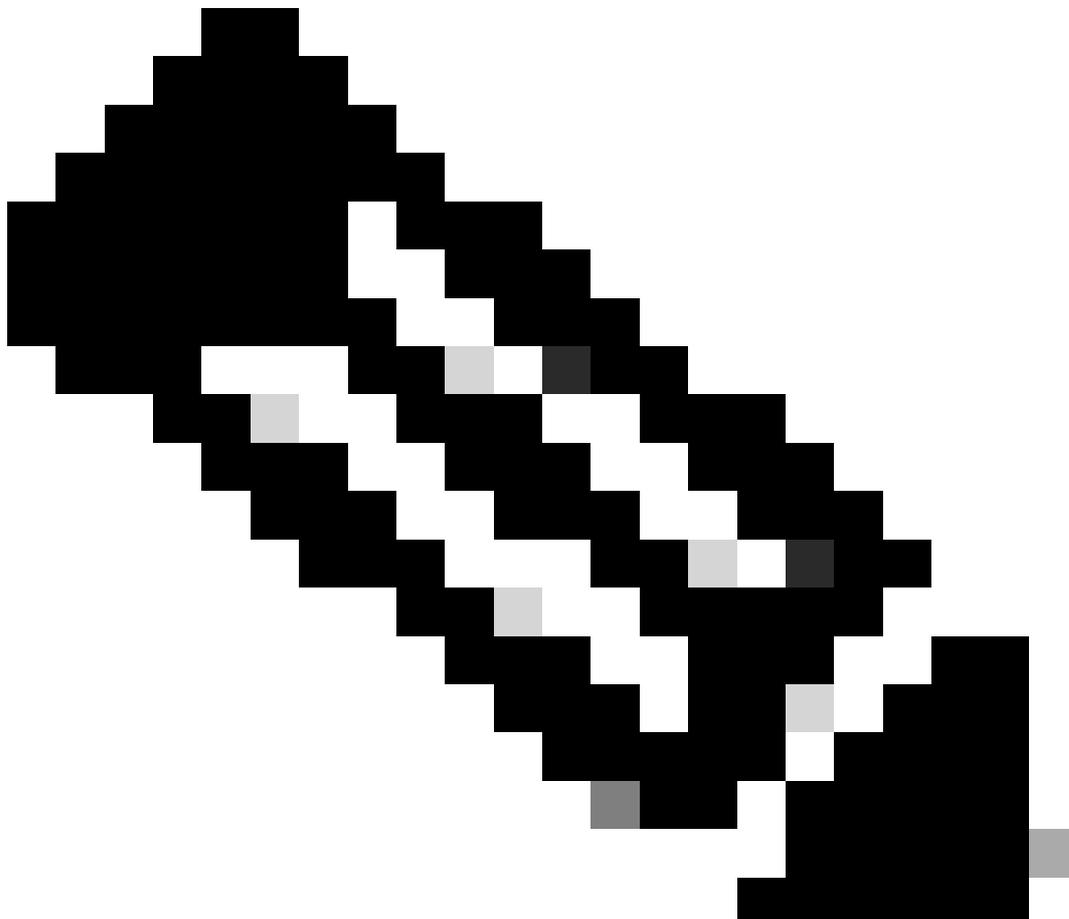
Última respuesta: SIN RESPUESTA el 12 de febrero 10:52:56 2023 GMT <<<<<<<<

Motivo de falla: <none>

Hora del último éxito: <none>

Hora del último fallo: 12 de febrero 10:52:56 2023 GMT

El nivel de comunicación permitido como INDIRECTO significa que el código de confianza requerido no está instalado correctamente en el controlador 9800.



Nota: Nota: CSSM es la fuente de veracidad de todos los datos de licencias.

* Si se mitiga el problema de comunicación básico entre 9800 y CSSM realizando la prueba, habilite la depuración en ciertos módulos involucrados para las comunicaciones de licencias inteligentes. La habilitación de la depuración en 9800 provocaría un pico en la CPU durante cierto

intervalo de tiempo y, por lo tanto, debe realizar estas acciones fuera del horario comercial.

Depurar

* Hay 4 módulos implicados en la comunicación de licencias inteligentes desde 9800 a CSSM o SSM en las instalaciones

1. Módulo criptográfico

PKI:

Crypto PKI Msg debugging is on Crypto PKI Trans debugging is on Crypto PKI callbacks debugging is on Crypto PKI Validation Path debugging is on

2. Módulo Http

Servidor HTTP:

HTTP Server transaction debugging is on HTTP Server tokens debugging is on HTTP Server EZSetup debugging is on HTTP Server URL debugging is on HTTP Server Authentication debugging is on HTTP Server Side Includes debugging is on HTTP Application Inout debugging is on HTTP Application Detail debugging is on HTTP Server Error debugging is on HTTP SSL Error debugging is on HTTP CTC trace debug debugging is on HTTP CTC error debug debugging is on HTTP SESSION debugging is on HTTP TPS Trace debugging is on HTTP TPS Error debugging is on HTTP WSMAN debugging is on

3. Módulo Openssl

ssl openssl:

TLS state debugging is on TLS msg debugging is on TLS errors debugging is on

4. El módulo de licencias inteligentes se denomina agente inteligente, incluido el gateway de transporte

Licencia:

License IPC communication debugging is on License Events debugging is on License warnings and errors debugging is on

Registros del sistema:

comprobación de identidad del servidor y validación de SAN en el certificado. Validación Trustpoint de la biblioteca SSL crypto.

16 sep 16:29:12.236: Verificación de identidad del servidor con host: 10.106.43.37

16 sep 16:29:12.236: La identidad del servidor para verificar es la dirección IP 10.106.43.37 len 12

16 sep 16:29:12.329: CRYPTO_PKI: (A645F) Compruebe si hay certificados idénticos

16 sep 16:29:12.329: CRYPTO_PKI(Búsqueda de certificados) issuer="cn=Cisco Licensing Root CA,o=Cisco" serial number= 0F 42 40

16 sep 16:29:12.329: CRYPTO_PKI: (A645F) Los puntos de confianza adecuados son: SLA-TrustPoint,Trustpool6,Trustpool6,

16 sep 16:29:12.329: CRYPTO_PKI: (A645F) Intentando validar el certificado mediante la política SLA-TrustPoint

16 sep 16:29:12.329: CRYPTO_PKI: (A645F) Uso de SLA-TrustPoint para validar el certificado

16 sep 16:29:12.345: SSL_connect:negociación SSL finalizada correctamente

16 sep 16:29:12.345: SSL_connect:negociación SSL finalizada correctamente

Una vez enviado el informe de uso a CSSM, debe ver la actualización correcta en el comando show license history message:

Las solicitudes tendrían componentes como UDI_SERIAL_NUMBER, hostname, software_tag_identifier que indican qué modo de licencia consume el controlador 9800 y request_type como "LICENSE_USAGE"

Existen varios tipos de licencia:

1. ID_TOKEN_TRUST

2. TRUST_SYNC

3. USO_LICENCIA

Informes de uso:

PETICIÓN: 16 de septiembre 16:30:16 UTC de 2024

```
"{"sender_info":{"connect_info":{"name":"C_agent","version":"5.8.6_rel/15","production":true,"addL-F-K9","udi_serial_number":"FCL2630000P"},"product_instance_identifier":"tag_identifier","software_number":"regid.2019-06.com.cisco.C9800_L_F_K9,1.0_9529f872-1b08-4cac-9279-71c391233fc2"},"device_list":[{"sudi":{"udi_pid":"C9800-L-F-K9","udi_serial_number":"FCL2630000 P"},"software_tag_identifier":"regid.2019-06.com.cisco.C9800_L_F_K9,1.0_9529f872-1b08-4cac-9279-71c391233fc2"},"product_instance_identifier":"","product_version":"17.12.02","hostname":"renjith-eap-test","role":"Active","request_type":"ID_TOKEN_TRUST","request_line_id":1,"smart_license":
```

Informes de uso:

PETICIÓN: 16 de septiembre 16:30:16 UTC de 2024

```
"{"sender_info":{"connect_info":{"name":"C_agent","version":"5.8.6_rel/15","production":true,"addL-F-K9","udi_serial_number":"FCL2630000P"},"product_instance_identifier":"
```

```
tag_identifier,\"software_number\": \"regid.2019-06.com.cisco.C9800_L_F_K9,1.0_9529f872-1b08-4cac-9279-71c391233fc2\"},\"device_list\": [{\"sudi\": {\"udi_pid\": \"C9800-L-F-K9\", \"udi_serial_number\": \"FCL2630000 P\"}, \"software_tag_identifier\": \"regid.2019-06.com.cisco.C9800_L_F_K9,1.0_9529f872-1b08-4cac-9279-71c391233fc2\"}, \"product_instance_identfier\": \"\", \"product_version\": \"17.12.02\", \"hostname\": \"renjith-eap-test\", \"role\": \"Active\", \"request_type\": \"TRUST_SYNC\", \"request_line_id\": 1, \"smart_license\":
```

Informes de uso:

PETICIÓN: 16 de septiembre 16:30:16 UTC de 2024

```
{\"sender_info\": {\"connect_info\": {\"name\": \"C_agent\", \"version\": \"5.8.6_rel/15\", \"production\": true, \"additional_info\": {\"amp\": 1726504216022, \"nonce\": \"77709655117429624\", \"sudi\": {\"udi_pid\": \"C9800-L-F-K9\", \"udi_serial_number\": \"FCL2630000P\"}, \"product_instance_identfier\": \"\", \"software_tag_identifier\": \"regid.2019-06.com.cisco.C9800_L_F_K9,1.0_9529f872-1b08-4cac-9279-71c391233fc2\"}, \"device_list\": [{\"sudi\": {\"udi_pid\": \"C9800-L-F-K9\", \"udi_serial_number\": \"FCL2630000P\"}, \"software_tag_identifier\": \"regid.2019-06.com.cisco.C9800_L_F_K9,1.0_9529f872-1b08-4cac-9279-71c391233fc2\"}, \"product_instance_identfier\": \"\", \"product_version\": \"17.12.02\", \"hostname\": \"renjith-eap-test\", \"role\": \"Active\", \"request_type\": \"LICENSE_USAGE\", \"request_line_id\": 1, \"smart_license\":
```

* Es importante comprender la respuesta de CSSM o SSM en las instalaciones:

Paquete de respuesta de error:

RESPUESTA: 16 de septiembre 16:30:16 UTC de 2024

```
{  
  \"estado\": \"ERROR\",  
  \"message_code\": \"ERROR al consumir licencias\",  
  \"mensaje\": \"\",  
  \"nonce\": \"77709655117429624\"  
}
```

El error indica que ya ha habido una entrada para el controlador en el servidor de licencias en las instalaciones de CSSM o SSM que está negando la adición de un nuevo registro en la base de datos. Se debe eliminar el registro activo o obsoleto de CSSM o SSM en las instalaciones y volver a enviar el informe Rum.

ID de sondeo de respuesta válida:

RESPUESTA: 16 de septiembre 16:29:14 UTC de 2024

```
{
```

```
"sender_info": {  
  "connect_info": {  
    "nombre": "CSLU_V1",  
    "versión": "v1",  
    "producción": verdadero,  
    "additional_info": "",  
    "capacidades": [  
      "UTILIDAD",  
      "DLC",  
      "AppHA",  
      "VARIOS NIVELES",  
      "EXPORT_2",  
      "OK_TRY_AGAIN",  
      "POLICY_USAGE",  
      "CSLU_V1",  
      "CSLU_V2",  
      "TELEMETRÍA"  
    ]  
  },  
  "timestamp": 1726504153302,  
  "nonce": "10743401694998030696",  
  "sudi": {  
    "udi_pid": "C980-L-F-K9",  
    "udi_serial_number": "FCL2630000P"  
  },  
  "product_instance_identifier": "",  
  "software_tag_identifier": "regid.2019-06.com.cisco.C9800_L_F_K9,1.0_9529f872-1b08-4cac-
```

9279-71c391233fc2"

```
},  
"estado": "COMPLETO",  
"license_data": [  
  {  
    "estado": "OK_POLL",  
    "id_línea_solicitud": 1,  
    "sudi": {  
      "udi_pid": "C980-L-F-K9",  
      "udi_serial_number": "FCL2630000P"  
    },  
    "poll_id": 5583279046281676962,  
    "poll_interval": 86739,  
    "smart_license": ""  
  }  
]  
}
```

* Cómo validar poll_id se almacena en la base de datos local 9800 y con qué frecuencia sondea para obtener una ACK para el informe Rum enviado.

Comando de prueba para validar la necesidad de activarse a través del servicio interno.

```
conf t service internal exit test license smart conversion list-poll-info Poll Request Information: PollID | Type | Delta | Poll Time  
5583279046281676962 | TRUST_SYNC | 86673 | Sep 17 17:33:05 2024 UTC
```

* Como se puede entender en la explicación de que las solicitudes iniciales enviadas por el controlador 9800 siempre serían token de código de confianza y sin él, el controlador 9800 nunca generaría un nuevo informe de uso de Rum y, por lo tanto, el cambio de uso de la licencia no se puede enviar en CSSM.

* Un ejemplo solicita poll_id para License_usage.

```
test license smart conversion list-poll-info Poll Request Information: PollID | Type | Delta | Poll Time 5583279046281677674 |
```

* si ya hay un ACK procesado en la base de datos CSSM o SSM On-Prem, puede forzar al agente inteligente en el controlador 9800 a sondear y obtener ACK lo antes posible sin esperar el tiempo mencionado

en el ciclo poll_id.

test license smart conversion sched_poll 5583279046281676962 ? <0-4294967295> delta Time in Seconds

Información Relacionada

- [Configuración de licencias offline \(Air Gapped\) en el WLC 9800](#)
- [Soporte técnico y descargas de Cisco](#)
- [Configuración de Catalyst 9800 WLC Smart Licensing mediante la política con DNA Center](#)

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).