

Configurar & Solucionar problemas de licencia inteligente de Catalyst 9800 con SLUP

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Licencias tradicionales frente a SLUP](#)

[Configuración](#)

[CSSM de conexión directa](#)

[Conectado a CSLU](#)

[Iniciada por instancia de producto](#)

[iniciado por CSLU](#)

[Conectado a SSM en las instalaciones](#)

[Configuración de Smart Transport a través de un Proxy HTTPS](#)

[Frecuencia de comunicación](#)

[Restablecimiento de fábrica de licencias](#)

[En caso de RMA o sustitución de hardware](#)

[Actualización desde el registro de licencias específicas \(SLR\)](#)

[Resolución de problemas](#)

[Acceso a Internet, comprobaciones de puertos y ping](#)

[Syslog](#)

[Capturas de paquetes](#)

[Comandos show](#)

[Depuraciones/btrace](#)

[Problemas comunes](#)

[El WLC no tiene acceso a Internet o el firewall bloquea/altera el tráfico](#)

[Alerta de CA desconocida en capturas de paquetes](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar y resolver problemas de licencia inteligente usando la política (SLUP) en el controlador de LAN inalámbrica (WLC) Catalyst 9800 .

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

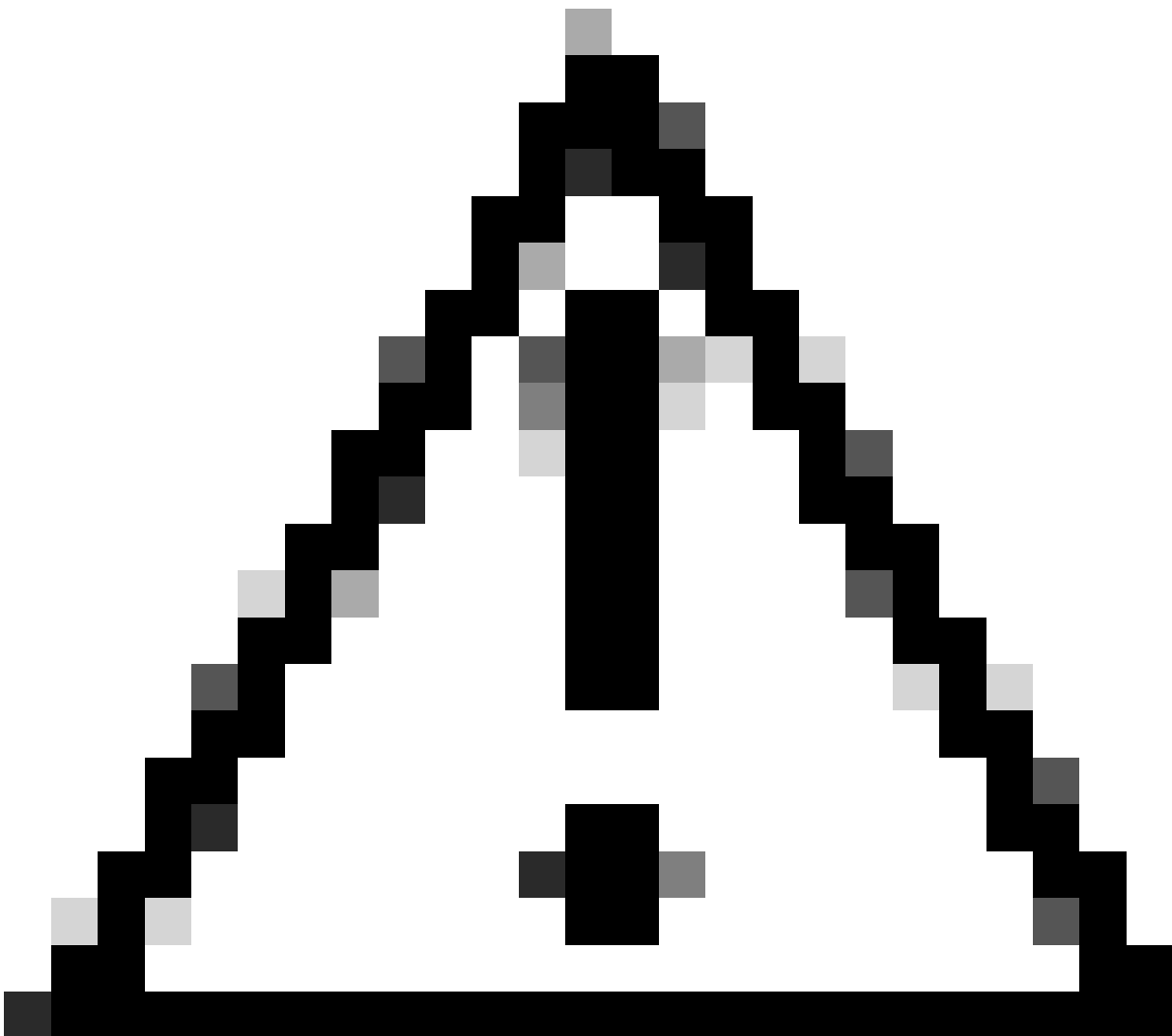
- Licencias inteligentes mediante políticas (SLUP)
- Controlador de LAN inalámbrica (WLC) Catalyst 9800

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



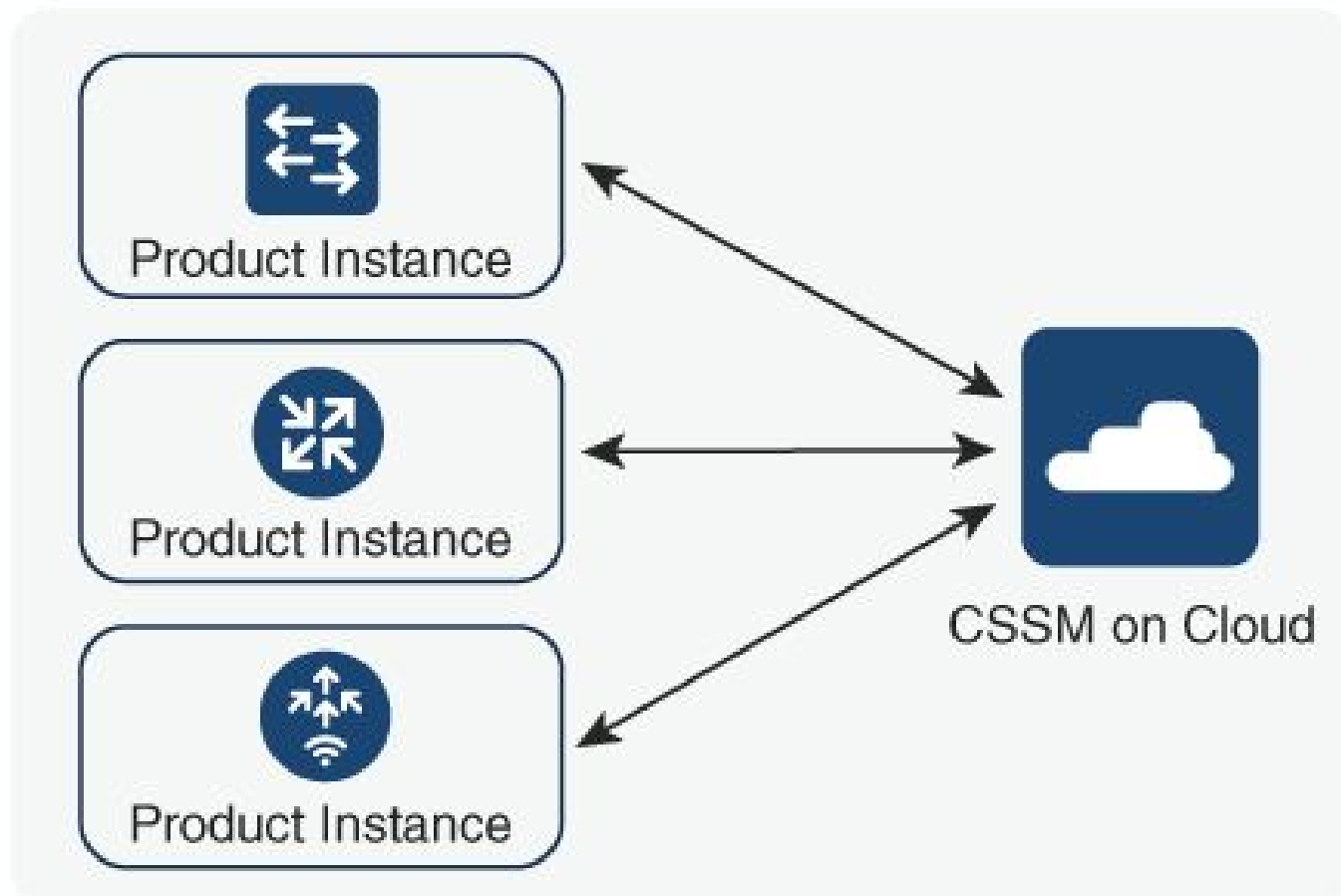
Precaución: Las notas de este artículo contienen sugerencias o referencias útiles al

material no cubierto en el documento. Se recomienda que lea cada nota.

1. Conexión directa a la nube de [Cisco Smart Software Manager](#) (nube CSSM)
2. Conectado a CSSM mediante [CSLU](#) (Cisco Smart License Utility Manager)
3. 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, CSLU y licencia inteligente SSM en las instalaciones con problemas de política en el Catalyst 9800.

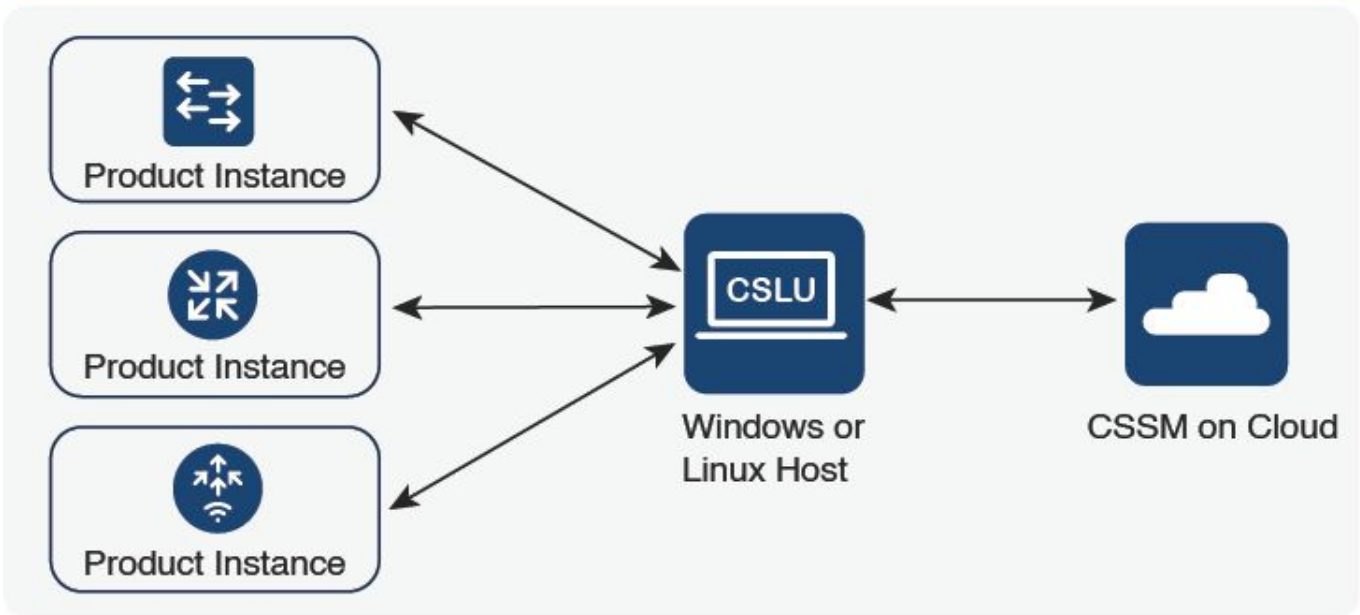
Directly Connected to CSSM



356794

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

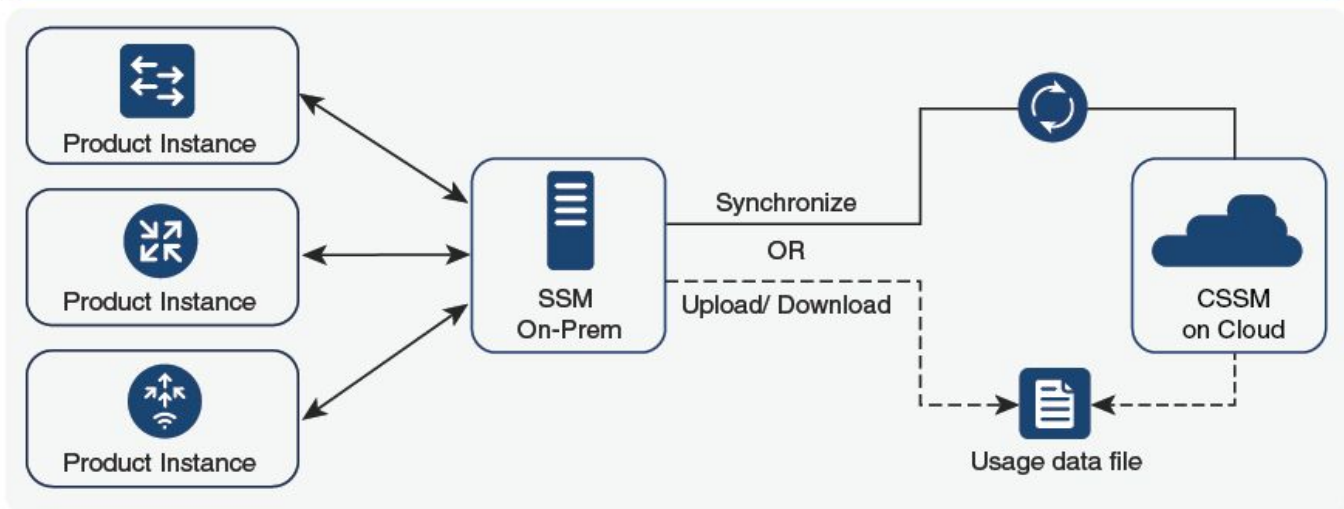
Connected to CSSM Through CSLU



356791


Opción 2. Conexión mediante CSLU

SSM On-Prem Deployment



357508

Opción 3. Conexión mediante On-prem Smart Software Manager (SSM in situ)

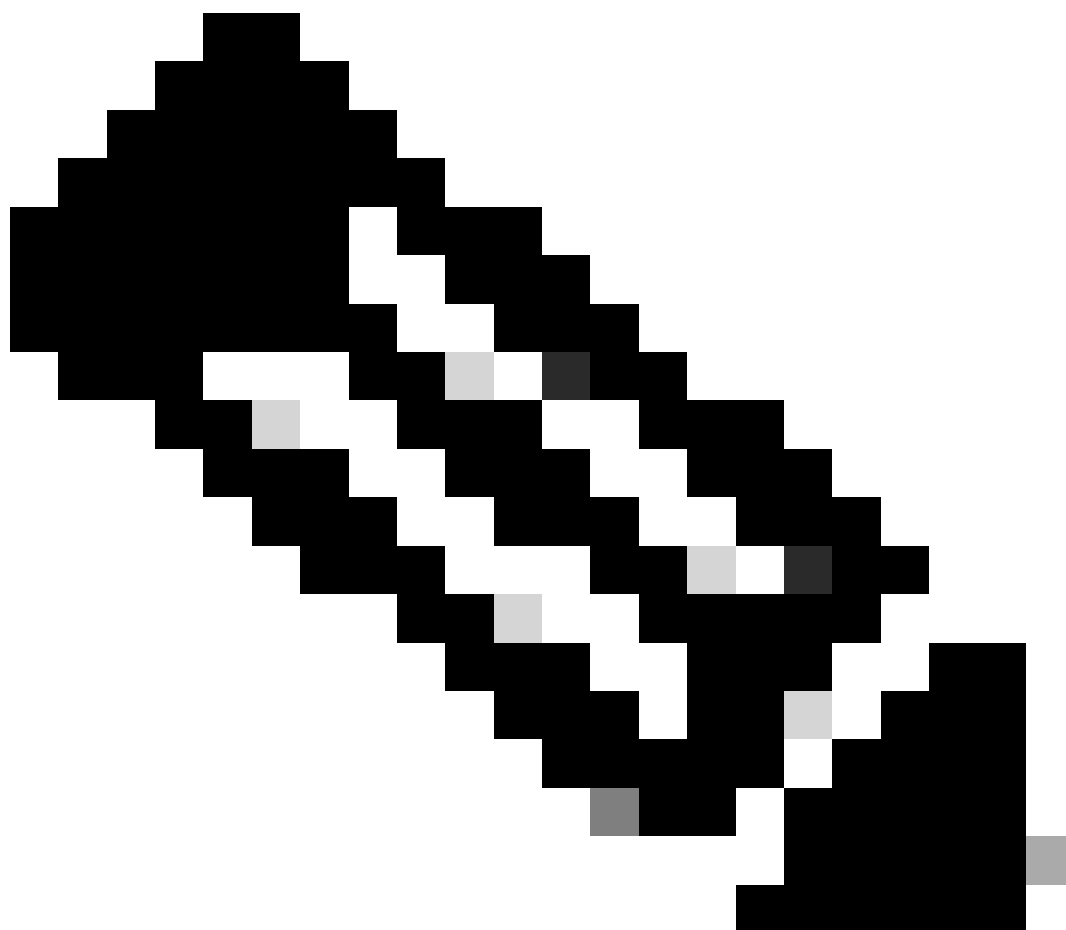
 Nota: Todos los comandos mencionados en este artículo son aplicables solamente a los WLC que ejecutan la versión 17.3.2 o posterior.

Licencias tradicionales frente a SLUP

La función Smart Licensing Using Policy se ha introducido en Catalyst 9800 con la versión de código 17.3.2. La versión 17.3.2 inicial pierde el menú de configuración SLUP en la interfaz de

usuario web del WLC, que se introdujo 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 dominio 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.
- Ya no existe la Reserva de Licencias Inteligentes (SLR). En su lugar, puede informar periódicamente de su uso manualmente.
- Ya no hay modo de evaluación. 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 conexión).




Advertencia: Si utiliza un controlador inalámbrico Catalyst 9800-CL de Cisco, asegúrese de estar familiarizado con el requisito ACK obligatorio que comienza con Cisco IOS® XE Cupertino 17.7.1. Consulte [Requisito de notificación y reconocimiento RUM para el](#)

Configuración


CSSM de conexión directa

Una vez que se ha creado el token en el CSSM, para establecer la confianza, se deben ejecutar estos comandos:

 Nota: Token Max. El recuento del número de usos debe ser al menos 2 en un caso de WLC en HA SSO.

```
configure terminal
ip http client source-interface <interface>
ip http client secure-trustpoint <TP>
license smart transport smart
license smart url default
exit
write memory
terminal monitor
license smart trust idtoken <token> all force
```

- El comando `ip http client source-interface` especifica la interfaz L3 de la que se originarán los paquetes relacionados con la licencia
- El comando `ip http client secure-trustpoint` especifica qué punto de confianza/certificado se utiliza para la comunicación CSSM. El nombre del punto de confianza se puede encontrar usando el comando `show crypto pki trustpoints`. Se recomienda utilizar un certificado autofirmado `TP-self-signed-xxxxxxxxx` o un certificado instalado por el fabricante (también conocido como MIC, disponible solamente en 9800-40, 9800-80 y 9800-L), generalmente llamado `CISCO_IDEVID_SUDI`.
- El comando de monitor de terminal hace que el WLC imprima los registros en la consola y ayude a confirmar que la confianza se ha establecido con éxito. Se puede inhabilitar usando el `terminal no monitor`.
- La palabra clave `all` del último comando indica a todos los WLC en el clúster de HA SSO que establezcan la confianza con el CSSM.
- La palabra clave `force` le dice al WLC que invalide cualquiera de las confianzas previamente establecidas e intente una nueva.

 Nota: Si no se establece la confianza, el 9800 lo intenta de nuevo 1 minuto después de que se ejecute el comando y, a continuación, no lo vuelve a intentar durante algún tiempo. Ingrese nuevamente el comando `token` para forzar un nuevo establecimiento de confianza.

Conectado a CSLU

Cisco Smart License Utility Manager (CSLU) es una aplicación basada en Windows (también disponible en Linux) que permite a los clientes administrar licencias y sus instancias de productos asociadas desde sus instalaciones en lugar de tener que conectar directamente sus instancias de productos habilitadas para Smart Licensed a Cisco Smart Software Manager (CSSM).

Esta sección solo cubre la configuración inalámbrica del 9800. Hay otros pasos que se deben realizar para configurar las licencias con la CSLU (como instalar la CSLU, configurar el software de la CSLU, etc.), que se tratan en las [Guías de configuración](#) .Si desea implementar un método de comunicación iniciado por la instancia del producto o iniciado por la CSLU, o completar la secuencia de tareas correspondiente.

Iniciada por instancia de producto

1. Garantizar la disponibilidad de la red desde el controlador a la CSLU
2. Asegúrese de que el tipo de transporte esté configurado en cslu:

```
(config)#license smart transport cslu
(config)#exit
#copy running-config startup-config
```

3. Si desea que el controlador detecte la CSLU, debe realizar la acción. Si desea que la CSLU se detecte mediante DNS, no es necesario realizar ninguna acción. Si desea descubrirlo mediante una URL, introduzca estos comandos:

```
(config)#license smart url cslu http://<cslu_ip>:8182/cslu/v1/pi
(config)#exit
#copy running-config startup-config
```

iniciado por CSLU

Cuando configura la comunicación iniciada por la CSLU, la única acción necesaria es verificar y asegurar la disponibilidad de la red a la CSLU desde el controlador.

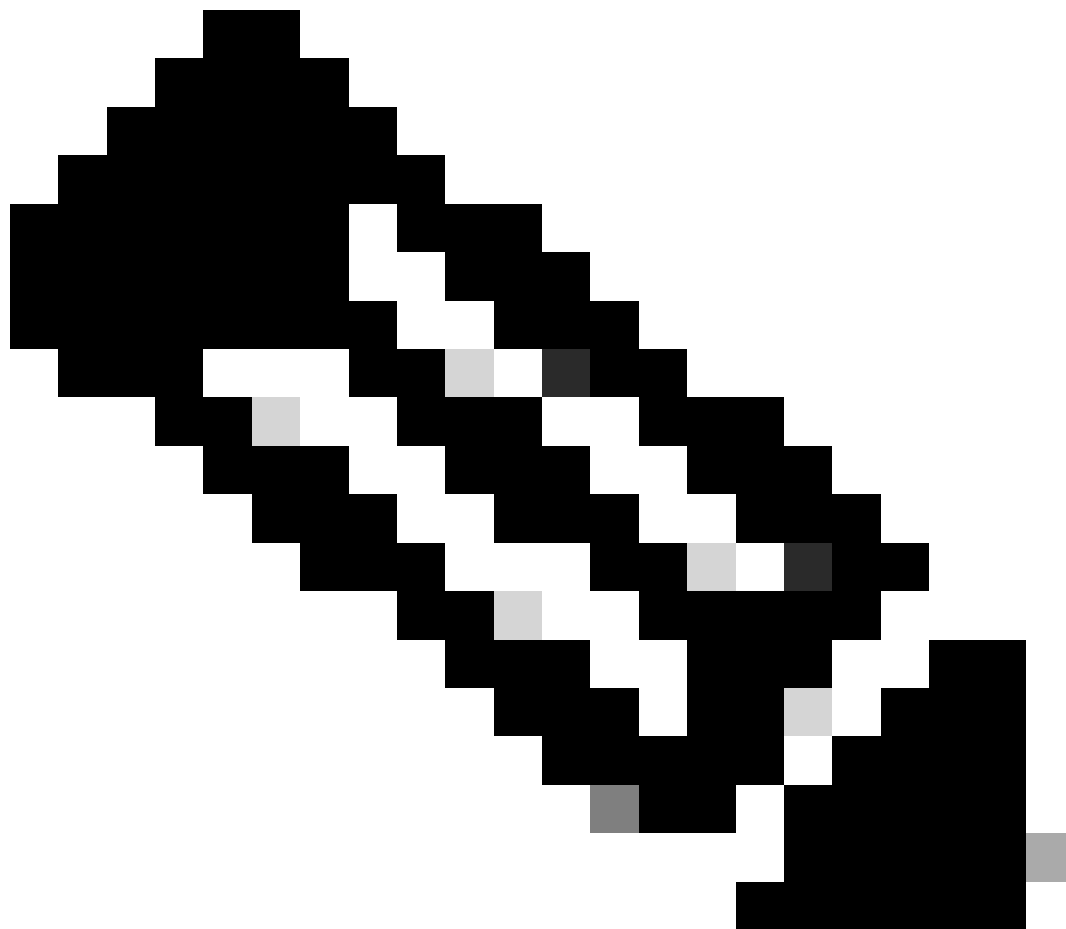
Conectado a SSM en las instalaciones

La configuración con SSM en las instalaciones es bastante similar a la conexión directa. Las instalaciones deben ejecutar la versión 8-202102 o posterior. Para las versiones SLUP (17.3.2 y posteriores), se recomienda utilizar la URL CSLU y el tipo de transporte. La URL se puede obtener de la interfaz de usuario web en las instalaciones en la sección **Licencias inteligentes > Inventario > <Cuenta virtual> > General**.

```
configure terminal
ip http client source-interface <interface>
```

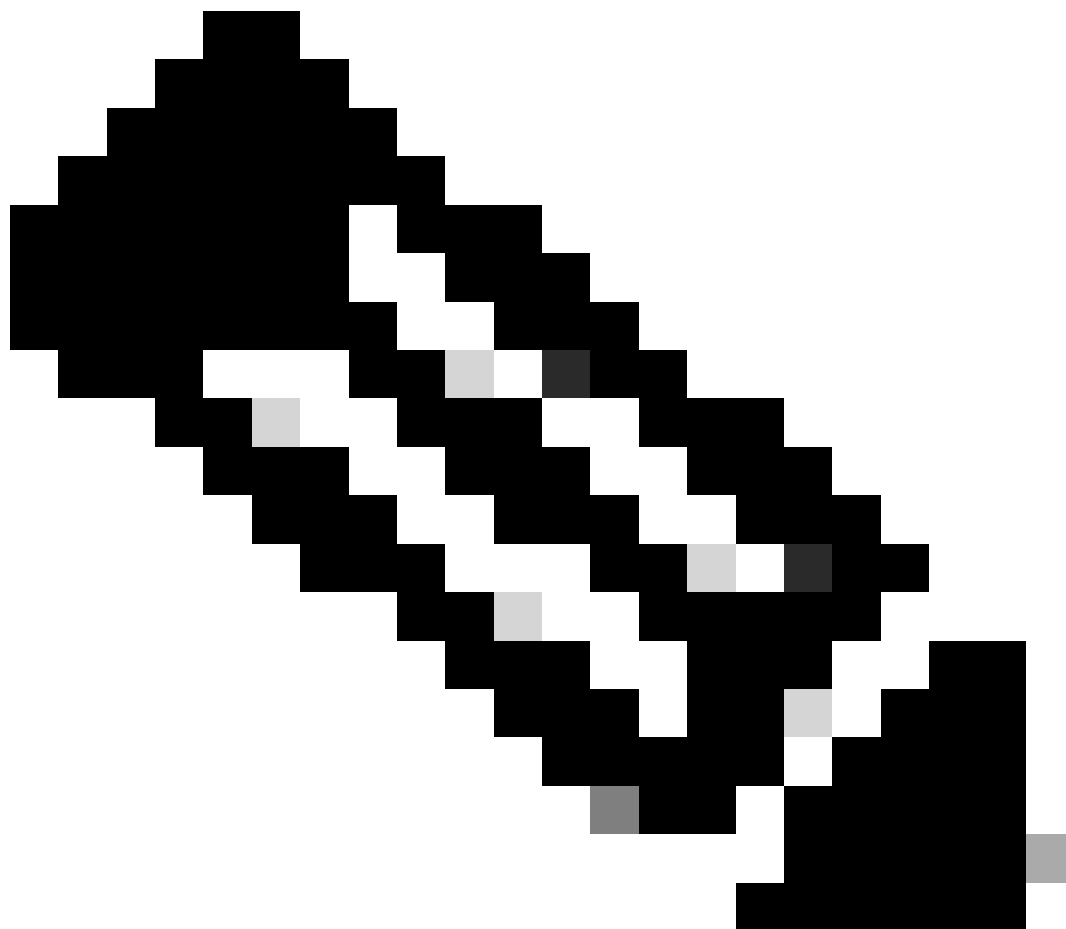
```
ip http client secure-trustpoint <TP>
license smart transport cs1u
license smart url https://<on-prem-ssm-domain>/SmartTransport
crypto pki trustpoint SLA-TrustPoint
  revocation-check none
exit
write memory
terminal monitor
```

El SSM en las instalaciones no requiere el uso de un token de confianza.



Nota: Si está recibiendo el mensaje, %PKI-3-CRL_FETCH_FAIL: Error en la recuperación de CRL para trustpoint SLA-TrustPoint, es porque no ha configurado revocation-check none bajo SLA-TrustPoint. Este es el punto de confianza que se utiliza para Smart Licensing. En el caso de In situ, el certificado del servidor de licencias suele ser un certificado autofirmado para el que no es posible la verificación de CRL, de ahí el requisito de configurar comprobaciones de no revocación.

Configuración de Smart Transport a través de un Proxy HTTPS



Nota: Los proxies autenticados todavía no se soportan a partir de la versión de código 17.9.2. Si utiliza proxies autenticados en su infraestructura, considere la posibilidad de utilizar [Cisco Smart License Utility Manager \(CSLU\)](#), que admite este tipo de servidores.

Para utilizar un servidor proxy para comunicarse con CSSM al utilizar el modo de transporte inteligente, siga estos pasos:

```
configure terminal
  ip http client source-interface <interface>
  ip http client secure-trustpoint <TP>
  license smart transport smart
  license smart url default
  license smart proxy address <proxy ip/fqdn>
  license smart proxy port <proxy port>
exit
write memory
```

```
terminal monitor
license smart trust idtoken <token> all force
```

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`:

```
<#root>
```

WLC#

```
show license air entities summary
```

```
Last license report time.....: 07:38:15.237 UTC Fri Aug 27 2021
Upcoming license report time.....: 15:38:15.972 UTC Fri Aug 27 2021
No. of APs active at last report.....: 3
No. of APs newly added with last report.....: 0
No. of APs deleted with last report.....: 0
```

Restablecimiento de fábrica de licencias

Catalyst 9800 WLC puede tener toda su configuración de licencias y confiar en el restablecimiento de fábrica y aún así mantener todas las demás configuraciones. Esto requiere una recarga del WLC:

```
WLC-1#license smart factory reset
%Warning: reload required after "license smart factory reset" command
```

En caso de RMA o sustitución de hardware

Si el 9800 WLC necesita ser reemplazado, el nuevo dispositivo tiene que registrarse con CSSM/On-prem Smart Software Manager y se percibe como un nuevo dispositivo. Para liberar el recuento de licencias del dispositivo anterior, es necesario realizar una eliminación manual en

Instancias de productos:

The screenshot shows the Cisco Software Central interface for Smart Software Licensing. The breadcrumb trail is "Cisco Software Central > Smart Software Licensing". The page title is "Smart Software Licensing". There are navigation links for "Feedback", "Support", and "Help". A menu bar includes "Alerts", "Inventory", "Convert to Smart Licensing", "Reports", "Preferences", "On-Prem Accounts", and "Activity". The virtual account is "Wireless TAC". There is a notification for "3 Major" alerts and a "Hide Alerts" button. The "Product Instances" tab is active, showing a table with columns: Name, Product Type, Last Contact, Alerts, and Actions. A search bar contains "9V4ZPZN8DW". The table has one entry: "UDI_PID:C9800-CL-K9; UDI_SN:9V4ZPZN8DW;" with Product Type "C9800CL" and Last Contact "2021-May-21 21:37:46". An "Actions" dropdown menu is open, showing "Transfer..." and "Remove..." options.

Actualización desde el registro de licencias específicas (SLR)

Las versiones anteriores del WLC, anteriores a la 17.3.2, utilizaban un método de licencia fuera de línea especial llamado Registro de licencia específico (SLR). Este método de licencia ha quedado obsoleto en las versiones que utilizan SLUP (17.3.2 y versiones posteriores).

Si actualiza un controlador 9800 que estaba usando SLR a una versión posterior a 17.3.2 o 17.4.1, se recomienda que pase a la generación de informes SLUP sin conexión en lugar de confiar en los comandos SLR. Guarde el archivo RUM de uso de licencia y regístrelo en el portal de licencias inteligentes. Dado que el SLR ya no existe en las versiones más recientes, se informa del recuento de licencias correcto y se libera cualquier licencia no utilizada. Las licencias ya no se bloquean, pero se informa del número exacto de usos.

Resolución de problemas

Acceso a Internet, comprobaciones de puertos y ping

En lugar del `tools.cisco.com` que utilizaban las licencias inteligentes tradicionales, el nuevo SLUP utiliza el dominio `smartreceiver.cisco.com` para establecer la confianza. En el momento de escribir este artículo, este dominio se resuelve en varias direcciones IP diferentes. No todas estas direcciones son a las que se puede hacer ping. Los ping no deben ser utilizados como una prueba de alcance de Internet del WLC. No poder hacer ping a estos servidores no significa que no estén funcionando correctamente.

En lugar de pings, se debe utilizar telnet sobre el puerto 443 como prueba de alcance. Telnet se puede comprobar en el dominio `smartreceiver.cisco.com` o directamente en las direcciones IP del servidor. Si el tráfico no está siendo bloqueado, el puerto debe aparecer como abierto en la salida:

```
WLC-1#telnet smartreceiver.cisco.com 443
Trying smartreceiver.cisco.com (192.330.220.90, 443)... Open <-----
[Connection to 192.330.220.90 closed by foreign host]
```

Syslog

Si se habilita el comando terminal monitor mientras se configura el token, el WLC imprime los registros relevantes en la CLI. Estos mensajes también se pueden obtener si ejecuta el comando show logging. Los registros de una confianza establecida correctamente tienen el siguiente aspecto:

```
WLC-1#license smart trust idtoken <token> all force
Aug 22 12:13:08.425: %CRYPTO_ENGINE-5-KEY_DELETED: A key named SLA-KeyPair has been removed from key st
Aug 22 12:13:08.952: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named SLA-KeyPair has been generated or impor
Aug 22 12:13:08.975: %PKI-6-CONFIGAUTOSAVE: Running configuration saved to NVRAM
Aug 22 12:13:11.879: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was successfully in
```

Registros de un WLC sin un servidor DNS definido o con un servidor DNS que no funciona:

```
Aug 23 09:19:43.486: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart Software Man
```

Registros de un WLC con un servidor DNS en funcionamiento, pero sin acceso a Internet:

```
Aug 23 09:23:30.701: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart Software Man
```

Capturas de paquetes

A pesar de que la comunicación entre el WLC y el CSSM/SSM en las instalaciones está cifrada y pasa sobre HTTPS, la realización de capturas de paquetes puede revelar qué causa que la confianza no se establezca. La manera más fácil de recolectar capturas de paquetes es a través de la interfaz Web del WLC.

Vaya a Troubleshooting > Packet Capture. Cree un nuevo punto de captura:

Troubleshooting > Packet Capture

+ Add × Delete

Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
0 items per page							
No items to display							

Asegúrese de que la casilla de verificación Monitor Control Plane esté habilitada. Aumente el tamaño del búfer hasta un máximo de 100 MB. Agregue la interfaz que debe capturarse. El tráfico de licencias inteligentes se origina en la interfaz de administración inalámbrica de forma predeterminada o en la interfaz definida con el comando `ip http client source-interface`:

Configuration details for the packet capture:

- Capture Name*: license
- Filter*: any
- Monitor Control Plane:
- Buffer Size (MB)*: 100
- Limit by*: Duration, 3600 secs ≈ 1.00 hour
- Available (3): GigabitEthernet1, GigabitEthernet2, Vlan1
- Selected (1): Vlan39

Inicie las capturas y ejecute el comando `license smart trust idtoken <token> all force`:

Troubleshooting > Packet Capture


+ Add × Delete

Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
<input checked="" type="checkbox"/> license	Vlan39	Yes	0%	any	3600 secs	Inactive	<input checked="" type="button" value="Start"/>

1 - 1 of 1 items

Las capturas de paquetes de un establecimiento de confianza deben contener estos pasos:

1. Establecimiento de la sesión TCP utilizando la secuencia SYN, SYN-ACK y ACK
2. Establecimiento de sesión TLS con intercambio de certificados de servidor y de cliente. El establecimiento termina con el paquete New Session Ticket.
3. Intercambio de paquetes cifrados (tramas de datos de aplicaciones) donde el WLC informa del uso de licencias
4. Terminación de la sesión TCP mediante FIN-PSH-ACK, FIN-ACK y secuencia ACK

 Nota: Las capturas de paquetes contienen muchas más tramas, incluidas múltiples tramas de actualización de ventana TCP y de datos de aplicación

Dado que la nube de CSSM utiliza 3 direcciones IP públicas diferentes, para filtrar todas las capturas de paquetes entre el WLC y el CSSM, utilice estos filtros de Wireshark:

```
ip.addr==172.163.15.144 or ip.addr==192.168.220.90 or ip.addr==172.163.15.144
```

Si utiliza un SSM en las instalaciones, filtre por la dirección IP del SSM:

```
ip.addr==<on-prem-ssm-ip>
```

Ejemplo: Capturas de paquetes de un establecimiento de confianza exitoso con CSSM conectado directamente con todas las capturas de paquetes significativas filtradas:

No.	Arrival Time	Source	Destination	Protocol	Info
559	Aug 23, 2021 11:31:13.35...	192.168.10.150	192.133.220.90	TCP	22425 → 443 [SYN] Seq=0 Win=4128 Len=0 MSS=536
576	Aug 23, 2021 11:31:13.46...	192.133.220.90	192.168.10.150	TCP	443 → 22425 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1390
578	Aug 23, 2021 11:31:13.46...	192.168.10.150	192.133.220.90	TCP	22425 → 443 [ACK] Seq=1 Ack=1 Win=4128 Len=0
580	Aug 23, 2021 11:31:13.46...	192.168.10.150	192.133.220.90	TLSv1.2	Client Hello
608	Aug 23, 2021 11:31:13.58...	192.133.220.90	192.168.10.150	TLSv1.2	Server Hello
612	Aug 23, 2021 11:31:13.58...	192.168.10.150	192.133.220.90	TCP	[TCP Window Update] 22425 → 443 [ACK] Seq=168 Ack=537 Win=4128 Len=0
614	Aug 23, 2021 11:31:13.58...	192.133.220.90	192.168.10.150	TCP	443 → 22425 [ACK] Seq=537 Ack=168 Win=31953 Len=536 [TCP segment of a reassembled PDU]
673	Aug 23, 2021 11:31:13.70...	192.133.220.90	192.168.10.150	TLSv1.2	Certificate [TCP segment of a reassembled PDU]
675	Aug 23, 2021 11:31:13.70...	192.133.220.90	192.168.10.150	TLSv1.2	Server Key Exchange [TCP segment of a reassembled PDU]
695	Aug 23, 2021 11:31:13.71...	192.133.220.90	192.168.10.150	TLSv1.2	Certificate Request, Server Hello Done
711	Aug 23, 2021 11:31:13.85...	192.168.10.150	192.133.220.90	TLSv1.2	Certificate, Client Key Exchange
718	Aug 23, 2021 11:31:14.01...	192.168.10.150	192.133.220.90	TLSv1.2	Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
737	Aug 23, 2021 11:31:14.13...	192.133.220.90	192.168.10.150	TLSv1.2	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
745	Aug 23, 2021 11:31:14.13...	192.168.10.150	192.133.220.90	TLSv1.2	Application Data
747	Aug 23, 2021 11:31:14.13...	192.168.10.150	192.133.220.90	TLSv1.2	Application Data
749	Aug 23, 2021 11:31:14.13...	192.168.10.150	192.133.220.90	TLSv1.2	Application Data, Application Data
22..	Aug 23, 2021 11:31:45.00...	192.168.10.150	192.133.220.90	TCP	22425 → 443 [FIN, PSH, ACK] Seq=4306 Ack=9738 Win=3625 Len=0
22..	Aug 23, 2021 11:31:45.11...	192.133.220.90	192.168.10.150	TCP	443 → 22425 [FIN, ACK] Seq=9738 Ack=4307 Win=31250 Len=0
22..	Aug 23, 2021 11:31:45.11...	192.168.10.150	192.133.220.90	TCP	22425 → 443 [ACK] Seq=4307 Ack=9739 Win=3625 Len=0

Comandos show

Estos comandos show contienen información útil sobre el establecimiento de confianza:

```
show license status
show license summary
show tech-support license
show license tech-support
show license air entities summary
```

```
show license history message (useful to see the history and content of messages sent to SL)
```

```
show tech wireless (actually gets show log and show run on top of the rest which can be useful)
```

El comando show license history message es uno de los comandos más útiles ya que puede mostrar los mensajes reales enviados desde el WLC y recibidos de vuelta desde el CSSM.

Un establecimiento de fideicomiso exitoso tiene impresos los mensajes "REQUEST: Aug 23 10:18:08 2021 Central" y "RESPONSE: Aug 23 10:18:10 2021 Central". Si no hay nada después de la línea de RESPUESTA, eso significa que el WLC no recibió una respuesta del CSSM.

Este es un ejemplo de un resultado del mensaje show license history para un establecimiento de confianza exitoso:

REQUEST: Aug 23 10:18:08 2021 Central

```
{"request":{"header":{"request_type":"POLL_REQ","sudi":{"udi_pid":"C9800-CL-K9","udi_serial_number":"NB"},"version":"1.3","locale":"en_US.UTF-8","signing_cert_serial_number":"3","id_cert_serial_number":"","product_instance_identfier":"","connect_info":{"name":"C_agent","version":"5.0.9_release","additional_info":"","capabilities":["UTILITY","DLC","AppHA","MULTITIER","EXPORT_2","POLICY_USAGE"]},"request_data":{"sudi":{"udi_pid":"C9800-CL-K9","udi_serial_number":"NB"},"timestamp":1629713888600,"nonce":"11702702165338740293","product_instance_identfier":"original_request_type":"LICENSE_USAGE","original_pid":"2e84a42f-c903-44c5-83b2-e62e258c780f","signature":{"type":"SHA256","key":"59152896","value":"eiJ7IuQaTCFfgUkwls76WZxa5DRI5A0gMqQd5POU6VNsH2j9dHco4T1NJ/aCmBR1MRmkfxyVSWsx41mjJL1mp0Si3ZS4FBMv1F/EBOUfowREe2oz21rQp1cAFpPn5S1aFezW/Nu6SQZfIW+IdF+2qnJeNFAIZbNpgOB5d5HIJvDmDIImvDu3bMRHhQAWr2KKzGF6jPz0hs7bGY/+F1fTLQk5LFEUaKtNH/tuxJPFH1Fh9//uhsd+NaQyfdRF1udkbFUBTFkvPxHW9/5w=="}}
```

RESPONSE: Aug 23 10:18:10 2021 Central

```
{"signature":{"type":"SHA256","value":"TXZE034fqAu12jy9V4+HoB2hDSh19au/5sgodiCVatmu671/6MyN7kZfEzREufY8SLrjTF04grGeQTcH7yEj0D+gztWXC0u8RBT7/Bo9aBs\n4x1i0E6f1PB3BP6yu7KIEUQZ8yHz1wDT+mVtJGi6TRrtYnV3KQMpCUMF5Fw0ksf3SfXreNZJuzWXzjHvtm1usCQXw7ZTBzffYsNK001kJ1r\nnvgB2PkV7JU1sA481kpIv1Pu16IiJXqk+2PC2IzCrCLG571VN3XgX1pE12SHyQ/DAw==","pid":null,"cert_sn":null},"response":{"header":{"version":"1.3","locale":"","mp":1629713890172,"nonce":null,"request_type":"POLL_REQ","sudi":{"udi_pid":"C9800-CL-K9","udi_serial_number":"9PJK8D70CNB"},"agent_actions":null,"connect_info":{"name":"SSM","version":"1.3","product_instance_identfier":["DLC","AppHA","EXPORT_2","POLICY_USAGE","UTILITY"],"additional_info":"","signing_cert_serial_number":"59152896","product_instance_identfier":"","status_code":"FAILED"},"Invalid ProductInstanceIdentifier: 2e84a42f-c903-44c5-83b2-e62e258c780f provided in the polling request 262236","retry_time_seconds":0,"response_data":"","sch_response":null}}
```

Depuraciones/btrace

Ejecute este comando unos minutos después de que se haya intentado establecer una confianza mediante un comando license smart trust idtoken all force. Los registros de IOSRP son extremadamente detallados. Agregar | include smart-agent" al comando para obtener solo registros de licencias inteligentes.

```
show logging process iosrp start last 5 minutes
show logging process iosrp start last 5 minutes | include smart-agent
```

También puede ejecutar estas depuraciones y, a continuación, volver a configurar los comandos de licencia para forzar una nueva conexión:

```
debug license events
debug license errors
```

```
debug license agent all
```

Problemas comunes

El WLC no tiene acceso a Internet o el firewall bloquea/altera el tráfico

Las capturas de paquetes incorporadas en el WLC son una manera fácil de ver si el WLC recibe algo detrás del CSSM o del SSM en las instalaciones. Si no hubo respuesta, lo más probable es que el firewall esté bloqueando algo.


El comando `show license history message` imprime una respuesta vacía 1 segundo después de que se envíe la solicitud si no se recibió ninguna respuesta de la nube CSSM o SSM en las instalaciones.

Por ejemplo, esto puede llevarle a creer que se recibió una respuesta vacía, pero en realidad no hubo respuesta alguna:

```
REQUEST: Jun 29 11:12:39 2021 CET
```

```
{"request":{"header":{"request_type":"ID_TOKEN_TRUST","sudi":{"udi_pid":"C9800-CL-K9"},"ud
```

```
RESPONSE: Jun 29 11:12:40 2021 CET
```

 Nota: Actualmente existe una solicitud de mejora con el ID de bug de Cisco [CSCvy84684](https://www.cisco.com/cisco/webbugtool/bugdetails?bug=CSCvy84684) que hace que el mensaje `show license history` imprima una respuesta vacía cuando no hay respuesta. Esto es para mejorar la salida del comando `show license history message`

Alerta de CA desconocida en capturas de paquetes

La comunicación con CSSM o SSM in situ requiere un certificado decente en el lado 9800. Puede ser autofirmado, pero no puede ser inválido o caducado. En tal caso, una captura de paquetes muestra una alerta TLS para CA desconocida enviada por CSSM cuando el certificado de cliente HTTP 9800 ha caducado.


La licencia inteligente utiliza la configuración del cliente `ip http`, que es diferente del servidor `ip http` que utiliza la interfaz web del WLC. Esto significa que estos comandos deben configurarse correctamente:

```
ip http client source-interface <interface>  
ip http client secure-trustpoint <TP>
```

El nombre del punto de confianza se puede encontrar con el comando `show crypto pki trustpoints`. Se recomienda utilizar un certificado autofirmado `TP-self-signed-xxxxxxxxx` o un certificado

instalado por el fabricante (MIC) que se suele llamar CISCO_IDEVID_SUDI y está disponible únicamente en 9800-80, 9800-40 y 9800-L.

Es importante tener en cuenta que los dispositivos que realizan la interceptación de TLS, como un firewall con la función de descifrado SSL, pueden evitar que el C9800 establezca un intercambio de señales satisfactorio con el servidor de licencias de Cisco, ya que el certificado HTTPS presentado es el certificado de firewall en lugar del certificado del servidor de licencias de Cisco.

 Nota: Asegúrese de configurar los comandos source-interface y secure-trustpoint. Se necesita un comando source-interface incluso si el WLC tiene solamente una interfaz L3.

Información Relacionada

- [Licencias inteligentes con modo Air Gap en 9800](#)
- [Soporte técnico y descargas de Cisco](#)

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).