

Solución de problemas de SLP Smart Transport en switches Catalyst 9000

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo resolver problemas de licencia inteligente mediante políticas (SLP) utilizando Smart Transport en switches Catalyst 9000.

Prerequisites

Requirements

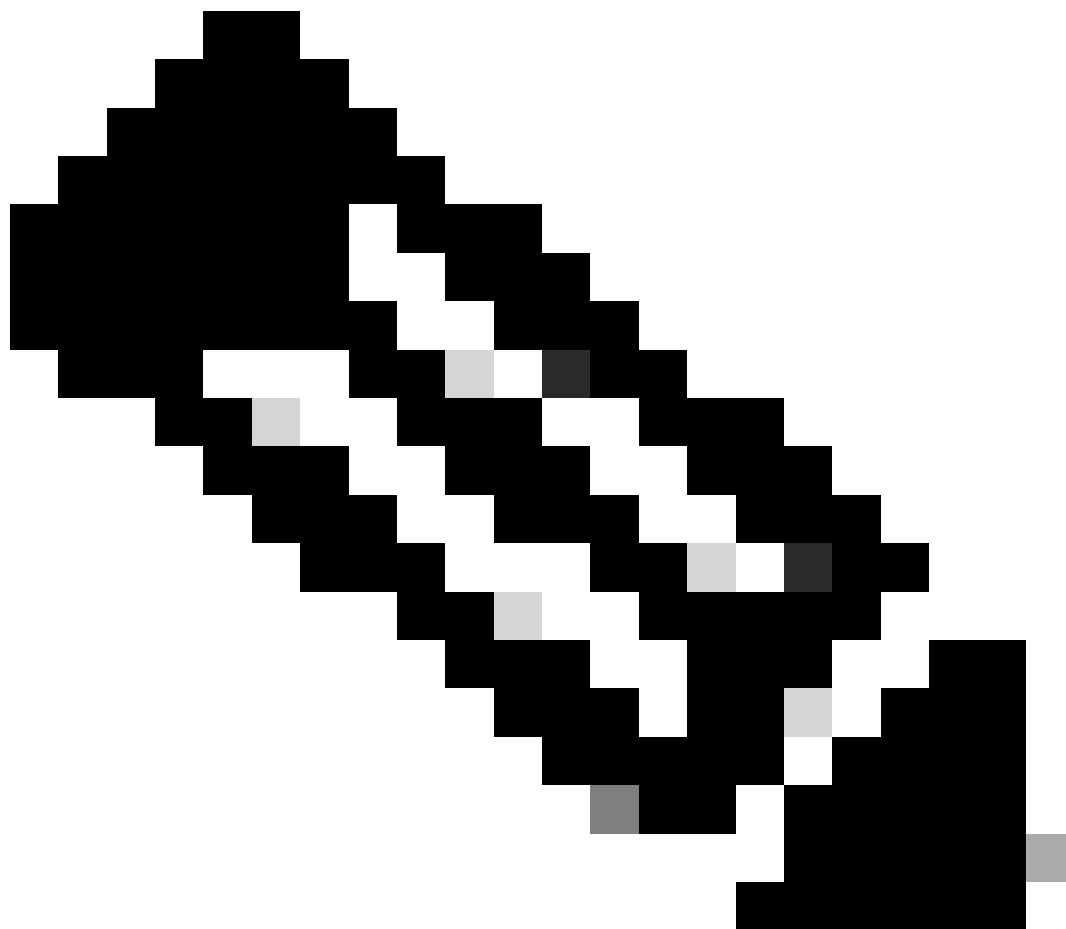
Cisco recomienda que conozca y esté familiarizado con este tema:

- Licencias inteligentes mediante políticas en dispositivos Cisco IOS® XE.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Catalyst 9200
- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS XE 17.9.1 y versiones posteriores



Nota: Consulte la guía de configuración correspondiente para conocer los comandos que se utilizan para activar estas funciones en otras plataformas de Cisco.

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

Smart Licensing Using Policy es una versión mejorada de Smart Licensing, diseñada con el objetivo principal de proporcionar una solución de licencias que garantice que las operaciones de la red no se interrumpen. En lugar de causar interrupciones, establece una relación de conformidad para justificar el hardware y las licencias de software que adquiera y utilice.

Para que los informes de licencias inteligentes funcionen correctamente, el switch Catalyst 9000 se conecta con Cisco Smart Software Manager (CSSM) para informar del uso de licencias. CSSM

sirve como plataforma centralizada para gestionar todas las licencias de software de Cisco y revisar el uso, lo que ayuda a planificar las necesidades de licencias futuras.

Existen múltiples topologías a través de las cuales un switch Catalyst 9000 puede conectarse a CSSM, pero este documento se centra en la topología específica en la que el switch está conectado directamente a CSSM. Esto significa que el switch debe ser capaz de alcanzar y establecer una conexión con CSSM, que se aloja en Internet.

En esta topología de conexión directa, hay dos opciones de transporte: Smart Transport y Call Home, siendo Smart Transport el método recomendado. Además, Smart Transport admite el uso de un proxy HTTPS y permite la selección de un VRF específico para gestionar la comunicación de licencias inteligentes con CSSM.

Al utilizar Smart Transport, el switch Catalyst 9000 intercambia información de uso de licencias con CSSM en formato JavaScript Object Notation (JSON) dentro de un mensaje HTTPS. Esta información, conocida como el Informe RUM, es enviada por el switch, y la respuesta de CSSM se denomina ACK.

La frecuencia mínima de informes para esta topología se limita a un día. Esto significa que la instancia del producto no enviará más de un informe RUM al día, lo que evita que se genere y transmita un número excesivo de informes para determinadas licencias. Esto ayuda a resolver los problemas relacionados con la memoria y las ralentizaciones del sistema causadas por una sobreproducción de informes RUM.

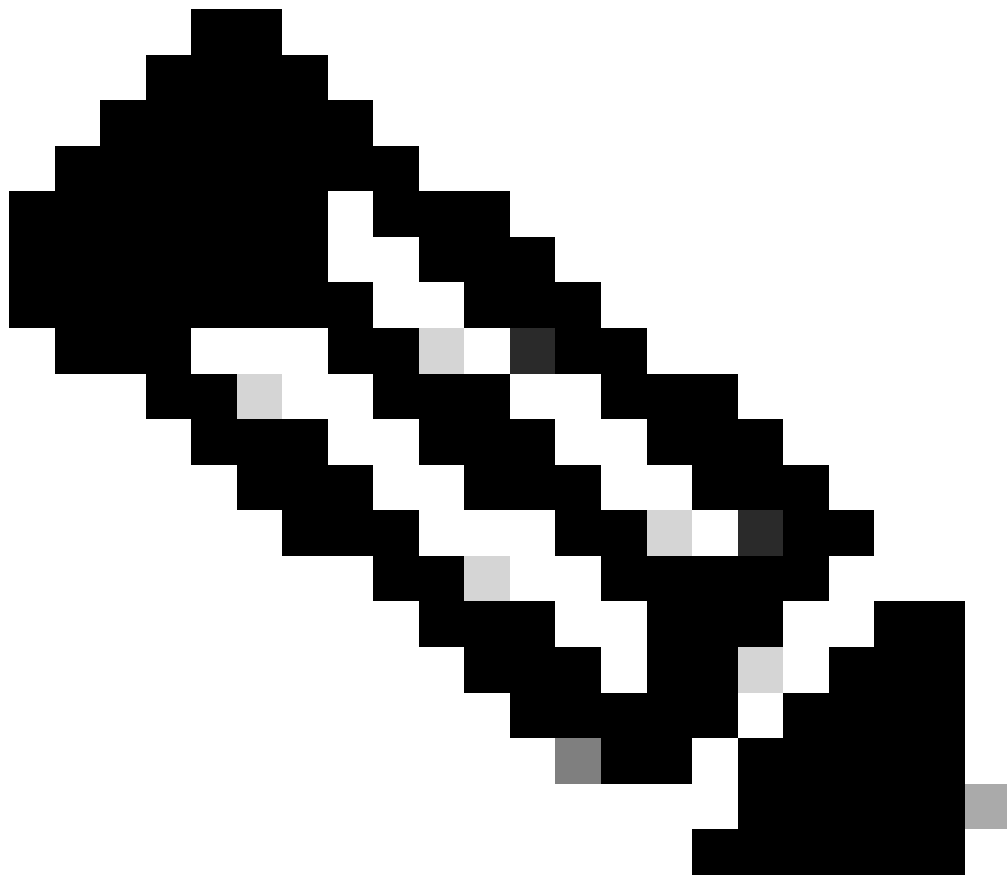
Si es necesario, puede invalidar esta restricción de limitación mediante el `license smart sync` comando en el modo EXEC privilegiado

Configurar

Siga estos pasos para configurar SLP con Smart Transport:

1. Configure Smart como tipo de transporte y utilice la URL predeterminada.

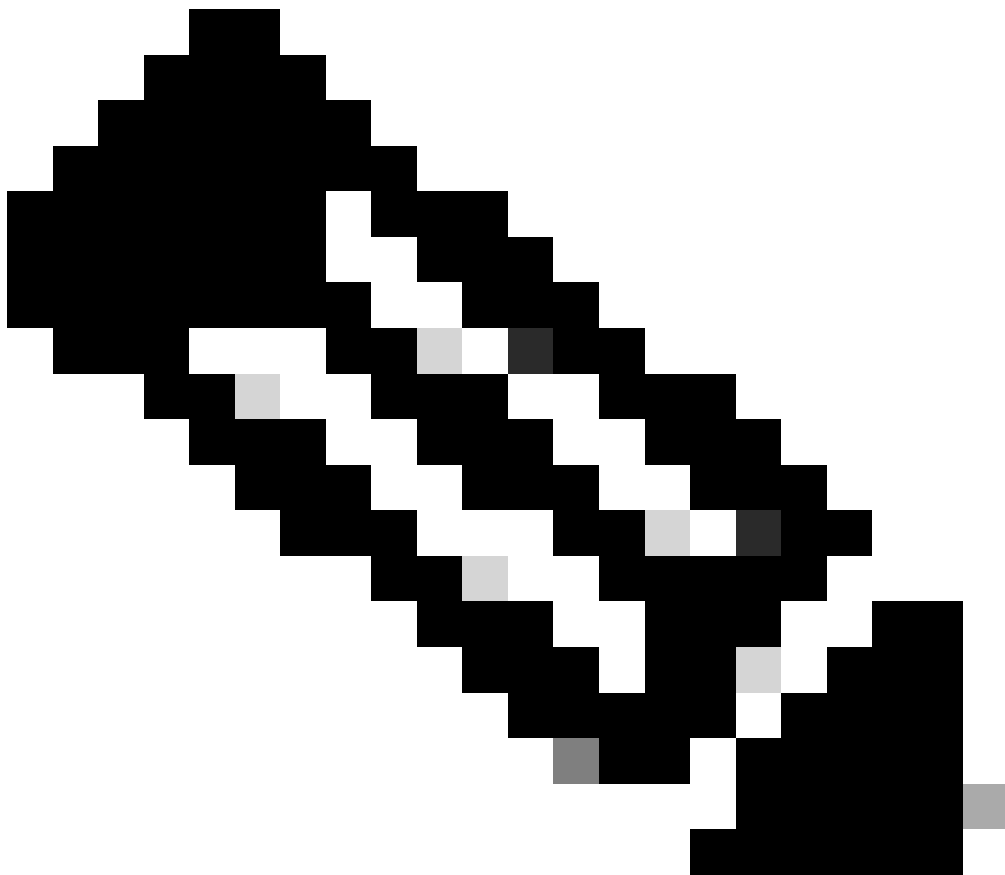
```
Switch#configure terminal
Switch(config)#license smart transport smart
Switch(config)#license smart url default
```



Nota: Si se utiliza un VRF para Smart Transport, license smart vrf debe configurarse.

-
2. Configure el servidor DNS y la interfaz de origen para la resolución DNS y las conexiones de cliente HTTP.

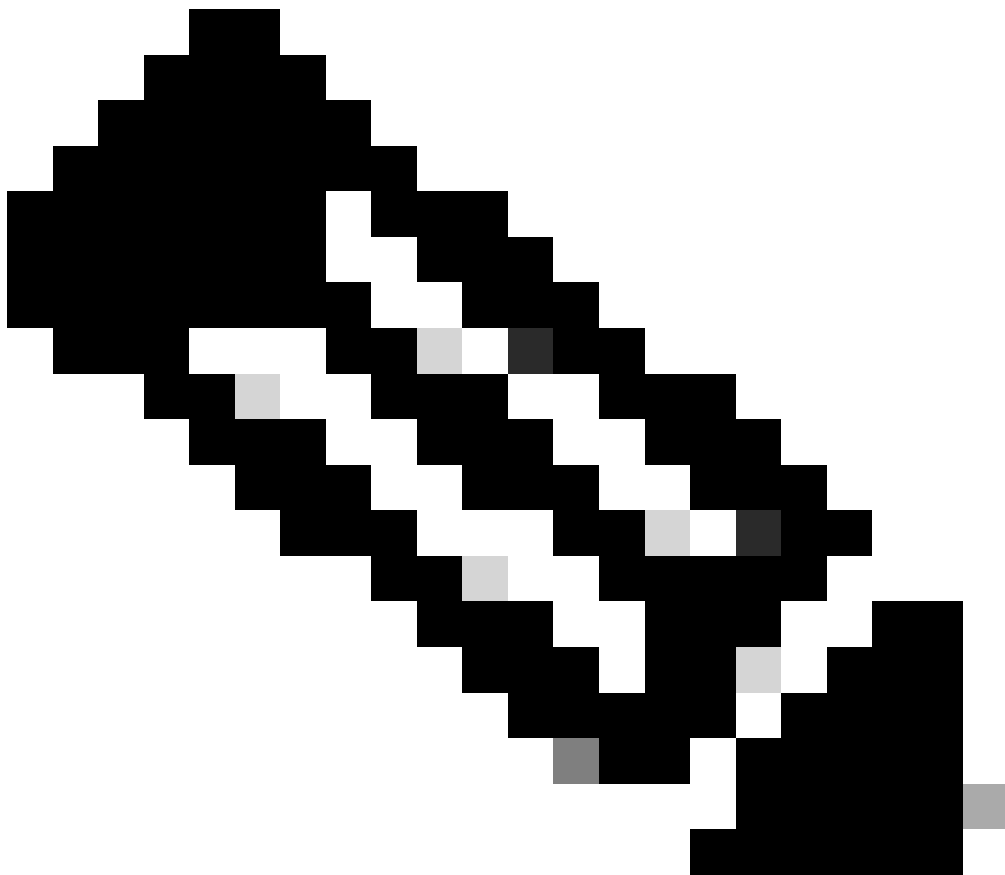
```
Switch(config)#ip domain lookup
Switch(config)#ip name-server 10.31.104.74
Switch(config)#ip domain name cisco.com
Switch(config)#ip domain lookup source-interface Vlan10
```



Nota: Si se utiliza un VRF para Smart Transport, se debe utilizar la variante VRF de estos comandos.

3. Si es necesario, configure un proxy HTTPS.

```
Switch(config)#license smart proxy address 192.168.217.105
Switch(config)#license smart proxy port 80
```



Nota: El servidor proxy se puede configurar mediante su dirección IP o nombre de host.

-
4. Genere un token en la cuenta virtual. Para completar este paso, siga el proceso descrito en [este documento](#).
 5. Instale el código de confianza en el switch.

```
Switch#license smart trust idtoken NGFkODgzMGUtZmNkMS00NTRjLWI5MjUtYjI0YWYzZjU1ZGQzLTE3NDYyNjU5%OA  
[OK]
```

Cuando se establece la confianza con CSSM, se muestra un syslog similar a este.

```
*Jan 24 23:19:05.144: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was successfu
```

Además, `show license status` muestra la hora de la instalación del código de confianza.

```
<#root>
```

```
Switch#show license status | i Trust
```

```
Trust Code Installed: Jan 24 23:19:05 2025 UTC
```

```
<--- Trust code was installed
```

Finalmente, el Registro de eventos de cuenta virtual muestra que se agregó el switch.

The screenshot shows the Cisco Software Central interface for Smart Software Licensing. The top navigation bar includes links for Alerts, Inventory, Convert to Smart Licensing, Reports, Preferences, On-Prem Accounts, Activity, and Commercial Consumption. Below this, there's a section for Virtual Account with a dropdown menu and alert counts: 65 Major, 440 Minor, and 54 Informational. The main content area has tabs for General, Licenses, Product Instances, and Event Log. The Event Log tab is active, displaying a table of events. The table has columns for Message, Time, and User. Two events are listed: one about a product instance connecting and being added to a virtual account, and another about a new token being generated.

Message	Time	User
The product instance "UDI_PID:C9300X-12Y; UDI_SN:..." connected and was added to the Virtual Account "..."	2025-Feb-21 17:12:46	System
A new Token "MzgwMDAwMTIiOGVhOC00OWExLTgzZmEiMzVhNTZkMDAyNTJhLTE3NDI3NDgy%0ANDkyMTF8U1N4MFV0R..."	2025-Feb-21 16:44:09	

Registro de eventos de cuenta virtual que muestra el dispositivo.

Troubleshoot

Si el establecimiento de confianza con CSSM falla, se muestra un syslog que indica el motivo del fallo.

```
*Jan 24 15:17:46.341: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart Software Ma
```

Entre las posibles razones de un fallo de comunicación se incluyen:

- No se puede resolver el nombre de host/dominio del servidor: La dirección URL de Smart Transport o el nombre de host del servidor proxy no se resolvieron mediante DNS. Valide las configuraciones de resolución de nombres y la disponibilidad del servidor DNS.

- Tiempo de espera de conexión agotado: Se intentó la conexión, pero no hubo respuesta. Valide que la conexión HTTPS con CSSM se está estableciendo mediante capturas de paquetes y compruebe si un dispositivo, como un servidor proxy o un firewall, está bloqueando la conectividad. Si utiliza un servidor proxy, asegúrese de que está utilizando el puerto correcto.

Siga estos pasos y comandos de validación para resolver problemas de SLP con Smart Transport:

1. Valide los registros de eventos de Smart Licensing.

```
<#root>
```

```
Switch#
```

```
show license eventlog 1
```

```
**** Event Log ****
```

```
2025-01-24 13:58:23.900 UTC SAEVT_INIT_START version="5.5.29_rel/114"
2025-01-24 13:58:23.922 UTC SAEVT_INIT_CRYPT0 success="False" error="Crypto Initialization has not
2025-01-24 13:58:23.922 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmRegister"
2025-01-24 13:58:27.620 UTC SAEVT_READY
2025-01-24 13:58:27.621 UTC SAEVT_ENABLED
2025-01-24 13:58:27.665 UTC SAEVT_EXPORT_FLAG exportAllowed="False"
2025-01-24 13:58:27.732 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_SYSDAT
2025-01-24 13:58:27.742 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_SYSDAT
2025-01-24 13:58:27.742 UTC SAEVT_TAG_AUTHORIZED count="1" entitlementTag="regid.2017-05.com.cisco
2025-01-24 13:58:27.744 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_SYSDAT
2025-01-24 13:58:27.744 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_LICENS
2025-01-24 13:58:27.763 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_SYSDAT
2025-01-24 13:58:27.767 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_SYSDAT
2025-01-24 13:58:27.767 UTC SAEVT_TAG_AUTHORIZED count="1" entitlementTag="regid.2017-05.com.cisco
2025-01-24 13:58:27.767 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_SYSDAT
2025-01-24 13:58:27.768 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_LICENS
2025-01-24 13:58:30.425 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmInitialize"
2025-01-24 13:58:30.431 UTC SAEVT_HA_CHASSIS_ROLE udi="PID:C9300-48UN,SN:<SN>"
2025-01-24 13:58:30.431 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmRegister"
2025-01-24 13:58:37.975 UTC SAEVT_HA_ROLE udi="PID:C9300-48UN,SN:<SN>" haRole="Active"
2025-01-24 13:58:38.048 UTC SAEVT_HA_CHASSIS_ROLE udi="PID:C9300-48UN,SN:<SN>" haRole="Active"
2025-01-24 13:58:38.048 UTC SAEVT_HA_ROLE udi="PID:C9300-48UN,SN:<SN>" haRole="Active"
2025-01-24 13:58:38.062 UTC SAEVT_INIT_CONFIG_READ_BEGIN
2025-01-24 13:58:40.884 UTC SAEVT_HOSTNAME_CHANGE
2025-01-24 13:58:41.734 UTC SAEVT_HA_EVENT eventType="SmartAgentSetNVPairs"
2025-01-24 13:58:42.408 UTC SAEVT_INIT_CONFIG_READ_DONE
2025-01-24 13:58:42.531 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_OIR_AD
2025-01-24 13:58:42.531 UTC SAEVT_HA_CONFIG
2025-01-24 13:58:42.531 UTC SAEVT_HA_UDI udi="PID:C9300-48UN,SN:<SN>" haRole="Active"
2025-01-24 13:58:42.732 UTC SAEVT_LICENSE_USAGE count="0" type="destroy" entitlementTag="regid.201
2025-01-24 13:58:42.744 UTC SAEVT_LICENSE_USAGE count="0" type="destroy" entitlementTag="regid.201
2025-01-24 13:58:43.140 UTC SAEVT_INIT_SYSTEM_INIT
2025-01-24 13:58:44.143 UTC SAEVT_INIT_CRYPT0 success="False" error="Crypto Initialization has not
2025-01-24 13:59:14.143 UTC SAEVT_INIT_CRYPT0 success="True"
2025-01-24 13:59:14.144 UTC SAEVT_COMM_RESTORED
2025-01-24 13:59:14.176 UTC SAEVT_INIT_COMPLETE
2025-01-24 14:00:14.145 UTC SAEVT_PRIVACY_CHANGED enabled="True"
2025-01-24 14:00:27.432 UTC
```

```
SAEVT_UTILITY_REPORT_START
```

2025-01-24 15:17:46.341 UTC

```
SAEVT_COMM_FAIL error="Connection timed out". <--- Connection timed out
2025-01-24 15:35:22.627 UTC SAEVT_COMM_RESTORED <--- Communication with CSSM restored
```

2. Valide la conectividad con CSSM enviando un ping e intentando una conexión telnet. Esto verifica que se esté produciendo la resolución de nombres y que no haya ningún bloque administrativo entre el switch y el CSSM.

<#root>

Switch#

```
show ip interface brief | exclude unassigned
```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan10	10.31.121.118				
YES	DHCP	up		up	

Switch#

```
ping smartreceiver.cisco.com source Vlan10
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to X.X.X.X, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5)

, round-trip min/avg/max = 364/365/368 ms

Switch#

```
telnet smartreceiver.cisco.com 443 /ipv4 /source-interface vlan10
```

Trying X.X.X.X, 80 ...

Open

[Connection to X.X.X.X closed by foreign host]

Alternativamente, si se está utilizando un servidor proxy, puede probar los mismos comandos utilizando la dirección IP y el puerto del servidor proxy.

<#root>

Switch#

```
ping 192.168.217.105
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.217.105, timeout is 2 seconds:  
!!!!
```

```
Success rate is 100 percent (5/5)
```

```
, round-trip min/avg/max = 364/365/368 ms
```

```
Switch#
```

```
telnet 192.168.217.105 80 /ipv4 /source-interface vlan10
```

```
Trying 192.168.217.105, 80 ...
```

```
Open
```

```
[Connection to 192.168.217.105 closed by foreign host]
```

3. Validar que se están enviando informes RUM y si hay una respuesta.

```
<#root>
```

```
Switch#
```

```
show license history message
```

```
Message History (oldest to newest):
```

```
=====
```

```
Trust Establishment:
```

```
REQUEST: Jan 24 23:18:59 2025 UTC <--- RUM report was sent
```

```
{"request":{"header":{"request_type":"ID_TOKEN_TRUST","sudi":{"udi_pid":"C9300-48UN",
```

```
RESPONSE: Jan 24 23:19:05 2025 UTC <--- Response from CSSM was received
```

```
{"signature":{"type":null,"value":null,"piid":null,"cert_sn":null},"response":{"header":{"vers
```

```
Usage Reporting:
```

```
No past history
```

```
Result Polling:
```

```
No past history
```

```
Authorization Request:
```

```
No past history
```

```
Authorization Return:
```

```
No past history
```

```
Trust Sync:
```

```
No past history
```

```
Import Message History (oldest to newest):
```

```
=====
```

```
Import POLICY:
```

```
No past Import history
```

Import AUTH:
No past Import history

Import TRUST CODE:
Received on Jan 24 23:19:05 2025 UTC
<TRUST_CODE>

Import RUM ACK:
No past Import history

Import CONVERSION ACK:
No past Import history

Import ACCOUNT INFO:
Last policy received on Jan 24 23:19:05 2025 UTC
<ACCOUNT_INFO>

Switch#

show license tech support | sec Trust

Trust Establishment:
Attempts: Total=1,

Success=1

, Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response: OK on Jan 24 23:19:05 2025 UTC <--- Trust establishment succeeded

Failure Reason:

Last Success Time: Jan 24 23:19:05 2025 UTC

Last Failure Time:

Trust Acknowledgement:

Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response:

Failure Reason:

Last Success Time:

Last Failure Time:

Trust Sync:

Attempts: Total=1,

Success=1,

Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response: OK on Jan 24 23:19:50 2025 UTC

Failure Reason:

Last Success Time: Jan 24 23:19:50 2025 UTC

Last Failure Time:

Trusted Store Interface: True

Local Device: P:C9300-48UN,S:

, state[2], Trust Data INSTALLED TrustId:612

Overall Trust: INSTALLED (2) <--- Trust code installed

Si se envía una solicitud pero no hay respuesta del CSSM, el `show license history message` comando muestra que no hay datos JSON para la respuesta dada y se pueden obtener más detalles sobre la falla.

<#root>

Switch#

show license history message

! <--- Output omitted for brevity --->

Trust Establishment:

REQUEST: Feb 21 16:54:49 2025 UTC

`{"request":{"header":{"request_type":"ID_TOKEN_TRUST"},"sudi":{"udi_pid":"C9300X-12Y"}}`,

RESPONSE: Feb 21 16:54:49 2025 UTC

<--- The line is empty, which means there was no response from CSSM

REQUEST: Feb 21 16:55:19 2025 UTC

`{"request":{"header":{"request_type":"ID_TOKEN_TRUST"},"sudi":{"udi_pid":"C9300X-12Y"}}`,

! <--- Output omitted for brevity --->

Switch#

show license tech support | sec Trust

Trust Establishment:

Attempts: Total=2, Success=0,

Fail=2

Ongoing Failure: Overall=2 Communication=2

Last Response: NO REPLY on Feb 21 16:55:39 2025 UTC

<--- Failure reason was NO REPLY

Failure Reason: <none>

Last Success Time: <none>
Last Failure Time: Feb 21 16:55:39 2025 UTC
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: P:C9300-48UN,S:<SN>, state[1],

NOT INSTALLED

TrustId:605

<--- Trust point exists but it is not installed yet

Overall Trust: No ID

4. Active el switch para enviar un informe RUM para sincronizar con CSSM.

<#root>

Switch#

show clock

*23:38:54.683 UTC Fri Jan 24 2025

Switch#

show license tech support | i Utility

Utility:

Start Utility Measurements: Jan 24 23:35:55 2025 UTC (4 minutes, 38 seconds remaining)

Send Utility RUM reports: Feb 23 23:20:56 2025 UTC (29 days, 23 hours, 49 minutes, 39 seconds remaining)

Process Utility RUM reports: Jan 25 23:30:58 2025 UTC (23 hours, 59 minutes, 41 seconds remaining)

Switch#

show license history message | i REQUEST

REQUEST: Jan 24 23:18:59 2025 UTC

REQUEST: Jan 24 23:20:50 2025 UTC

REQUEST: Jan 24 23:25:55 2025 UTC

REQUEST: Jan 24 23:19:41 2025 UTC

Switch#

```
license smart sync all <--- Trigger synchronization
```

```
Switch#
```

```
show license history message | i REQUEST
```

```
REQUEST: Jan 24 23:18:59 2025 UTC
```

```
REQUEST: Jan 24 23:20:50 2025 UTC
```

```
REQUEST: Jan 24 23:25:55 2025 UTC
```

```
REQUEST: Jan 24 23:19:41 2025 UTC
```

```
REQUEST: Jan 24 23:39:05 2025 UTC
```

```
<--- New RUM report was sent
```

```
Switch#
```

```
show license tech support | sec Trust
```

```
Trust Establishment:
```

```
Attempts: Total=1, Success=1, Fail=0 Ongoing Failure: Overall=0 Communication=0
```

```
Last Response: OK on Jan 24 23:19:05 2025 UTC
```

```
Failure Reason:
```

```
Last Success Time: Jan 24 23:19:05 2025 UTC
```

```
Last Failure Time:
```

```
Trust Acknowledgement:
```

```
Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
```

```
Last Response:
```

```
Failure Reason:
```

```
Last Success Time:
```

```
Last Failure Time:
```

```
Trust Sync:
```

```
Attempts:
```

```
Total=2, Success=2
```

```
, Fail=0 Ongoing Failure: Overall=0 Communication=0
```

```
Last Response: OK on Jan 24 23:39:14 2025 UTC <--- Successful response from CSSM
```

```
Failure Reason:
```

```
Last Success Time: Jan 24 23:39:14 2025 UTC
```

```
Last Failure Time:
```

```
Trusted Store Interface: True
```

```
Local Device: P:C9300-48UN,S:<SN>, state[2], Trust Data INSTALLED TrustId:612
```

```
Overall Trust: INSTALLED (2)
```

5. Para validar que el switch está estableciendo la conexión HTTPS con el CSSM, puede tomar una captura de paquetes. Este es un ejemplo de captura de paquetes de una conexión exitosa usando un servidor proxy.

```
<#root>
```

```
Switch#
```

```
sh ip cef 10.31.104.78
```

```
0.0.0.0/0
```

```
nexthop 10.31.121.65 Vlan10
```

```
Switch#
```

```
sh ip arp 10.31.121.65
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	10.31.121.65	0			

```
2c31.24b1.6bc6
```

```
ARPA Vlan10
```

```
Switch#
```

```
show mac address-table address 2c31.24b1.6bc6
```

Mac Address Table

Vlan	Mac Address	Type	Ports
10	2c31.24b1.6bc6	DYNAMIC	

```
Fi1/0/48
```

```
Total Mac Addresses for this criterion: 1
```

```
Switch#
```

```
monitor capture CSSM interface Fi1/0/48 both match any
```

```
Switch#
```

```
monitor capture CSSM start
```

```
Started capture point : CSSM
```

```
Switch#
```

```
show clock
```

```
*
```

```
15:41:10.058 UTC
```

```
Fri Jan 24 2025
```

```
Switch#
```

```
license smart sync all
```

```
Switch#sh license hist mess | i REQUEST  
REQUEST: Jan 24 15:35:17 2025 UTC
```

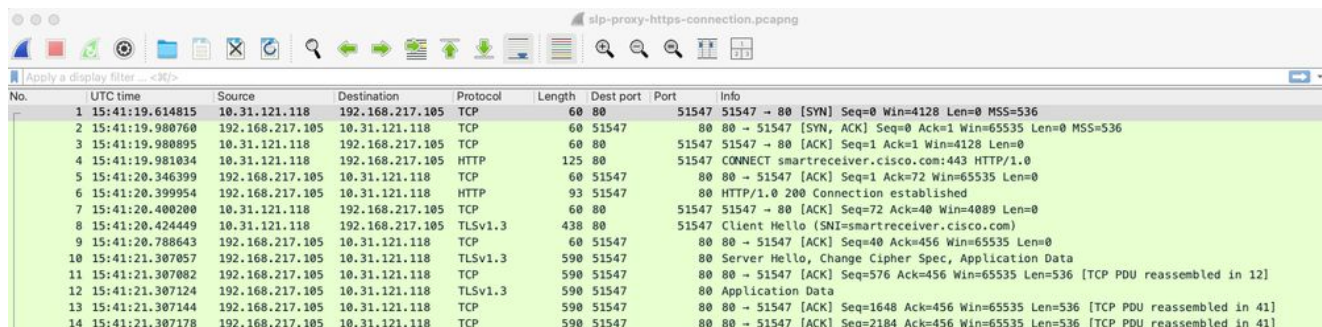
```
REQUEST: Jan 24 15:41:58 2025 UTC
```

```
Switch#
```

```
monitor capture CSSM stop
```

```
Switch#
```

```
monitor capture CSSM export location flash:slp-proxy-https-connection.pcap
Export Started Successfully
```



No.	UTC time	Source	Destination	Protocol	Length	Dest port	Port	Info
1	15:41:19.614815	10.31.121.118	192.168.217.105	TCP	60	80	51547	51547 → 80 [SYN] Seq=0 Win=4128 Len=0 MSS=536
2	15:41:19.980760	192.168.217.105	10.31.121.118	TCP	60	51547	80	80 → 51547 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=536
3	15:41:19.980895	10.31.121.118	192.168.217.105	TCP	60	80	51547	51547 → 80 [ACK] Seq=1 Ack=1 Win=4128 Len=0
4	15:41:19.981034	10.31.121.118	192.168.217.105	HTTP	125	80	51547	CONNECT smartreceiver.cisco.com:443 HTTP/1.0
5	15:41:20.346399	192.168.217.105	10.31.121.118	TCP	60	51547	80	80 → 51547 [ACK] Seq=1 Ack=72 Win=65535 Len=0
6	15:41:20.399954	192.168.217.105	10.31.121.118	HTTP	93	51547	80	HTTP/1.0 200 Connection established
7	15:41:20.400200	10.31.121.118	192.168.217.105	TCP	60	80	51547	51547 → 80 [ACK] Seq=72 Ack=40 Win=4089 Len=0
8	15:41:20.424449	10.31.121.118	192.168.217.105	TLSv1.3	438	80	51547	Client Hello (SNI=smartreceiver.cisco.com)
9	15:41:20.788643	192.168.217.105	10.31.121.118	TCP	60	51547	80	80 → 51547 [ACK] Seq=40 Ack=456 Win=65535 Len=0
10	15:41:21.307857	192.168.217.105	10.31.121.118	TLSv1.3	590	51547	80	Server Hello, Change Cipher Spec, Application Data
11	15:41:21.307882	192.168.217.105	10.31.121.118	TCP	590	51547	80	80 → 51547 [ACK] Seq=576 Ack=456 Win=65535 Len=536 [TCP PDU reassembled in 12]
12	15:41:21.307124	192.168.217.105	10.31.121.118	TLSv1.3	590	51547	80	Application Data
13	15:41:21.307144	192.168.217.105	10.31.121.118	TCP	590	51547	80	80 → 51547 [ACK] Seq=1648 Ack=456 Win=65535 Len=536 [TCP PDU reassembled in 41]
14	15:41:21.307178	192.168.217.105	10.31.121.118	TCP	590	51547	80	80 → 51547 [ACK] Seq=2184 Ack=456 Win=65535 Len=536 [TCP PDU reassembled in 41]

Captura de paquetes de una conexión HTTPS satisfactoria con CSSM mediante un servidor proxy.

6. Si la captura de paquetes muestra que la conexión HTTPS está intentando establecerse pero falla, podría deberse a una falla de intercambio de señales TLS o SSL. Estas depuraciones se pueden utilizar para investigaciones posteriores.

```
debug ip http client all
debug ssl openssl states
debug ssl openssl errors
debug crypto pki messages
debug crypto pki transactions
```

7. Si en algún momento es necesario quitar el código de confianza instalado del switch, se puede realizar un restablecimiento de fábrica de Smart Licensing. Este proceso requiere una recarga. Después del restablecimiento de fábrica, se puede instalar un nuevo código de confianza. El uso de este comando elimina toda la información de licencias, incluida la directiva.

```
<#root>
```

```
Switch#
```

```
license smart factory reset
```

```
%Warning: reload required after "license smart factory reset" command
```

```
Switch#
```

```
show license status | include Trust
```

```
Trust Code Installed:
```

```
<--- Installed trust code now shows none
```

```
Switch#
```

```
reload
```

Información Relacionada

- [Licencias inteligentes mediante políticas para los switches Catalyst de Cisco serie 9000](#)
- [Comprensión de Smart Licensing para Catalyst Switching](#)
- [Cisco Live: Introducción a las licencias inteligentes mediante políticas](#)
- [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).