

Dépannage de SLP Smart Transport sur les commutateurs Catalyst 9000

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment dépanner Smart Licensing Using Policy (SLP) en utilisant Smart Transport sur les commutateurs Catalyst 9000.

Conditions préalables

Exigences

Cisco vous recommande de connaître et de vous familiariser avec ce sujet :

- Licence Smart utilisant la politique sur les périphériques Cisco IOS® XE.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Catalyst 9200
- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS XE 17.9.1 et versions ultérieures



Remarque : Consultez le guide de configuration approprié pour connaître les commandes utilisées afin d'activer ces fonctionnalités sur d'autres plateformes Cisco.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Smart Licensing Using Policy est une version améliorée de Smart Licensing, conçue dans le but principal de fournir une solution de gestion des licences qui garantit la continuité des opérations de votre réseau. Plutôt que d'être perturbatrice, elle établit une relation de conformité pour tenir compte des licences matérielles et logicielles que vous achetez et utilisez.

Pour que les rapports Smart Licensing fonctionnent correctement, le commutateur Catalyst 9000 se connecte à Cisco Smart Software Manager (CSSM) pour signaler l'utilisation des licences. CSSM sert de plate-forme centralisée pour gérer toutes les licences logicielles Cisco et examiner

leur utilisation, ce qui permet de planifier les besoins futurs en matière de licences.

Il existe plusieurs topologies par lesquelles un commutateur Catalyst 9000 peut se connecter à CSSM, mais ce document se concentre sur la topologie spécifique dans laquelle le commutateur est directement connecté à CSSM. Cela signifie que le commutateur doit être capable d'atteindre et d'établir une connexion avec CSSM, qui est hébergé sur Internet.

Dans cette topologie de connexion directe, il existe deux options de transport : Smart Transport et Call Home, Smart Transport étant la méthode recommandée. En outre, Smart Transport prend en charge l'utilisation d'un proxy HTTPS et permet de sélectionner un VRF spécifique pour gérer la communication de licence intelligente avec CSSM.

Lors de l'utilisation de Smart Transport, le commutateur Catalyst 9000 échange des informations d'utilisation de licence avec CSSM au format JSON (JavaScript Object Notation) dans un message HTTPS. Ces informations, connues sous le nom de rapport RUM, sont envoyées par le commutateur, et la réponse du CSSM est appelée un ACK.

La fréquence minimale des rapports pour cette topologie est limitée à une journée. Cela signifie que l'instance de produit n'envoie pas plus d'un rapport RUM par jour, ce qui empêche la génération et la transmission d'un nombre excessif de rapports pour certaines licences. Cela permet de résoudre les problèmes liés à la mémoire et les ralentissements du système provoqués par une surproduction de rapports RUM.

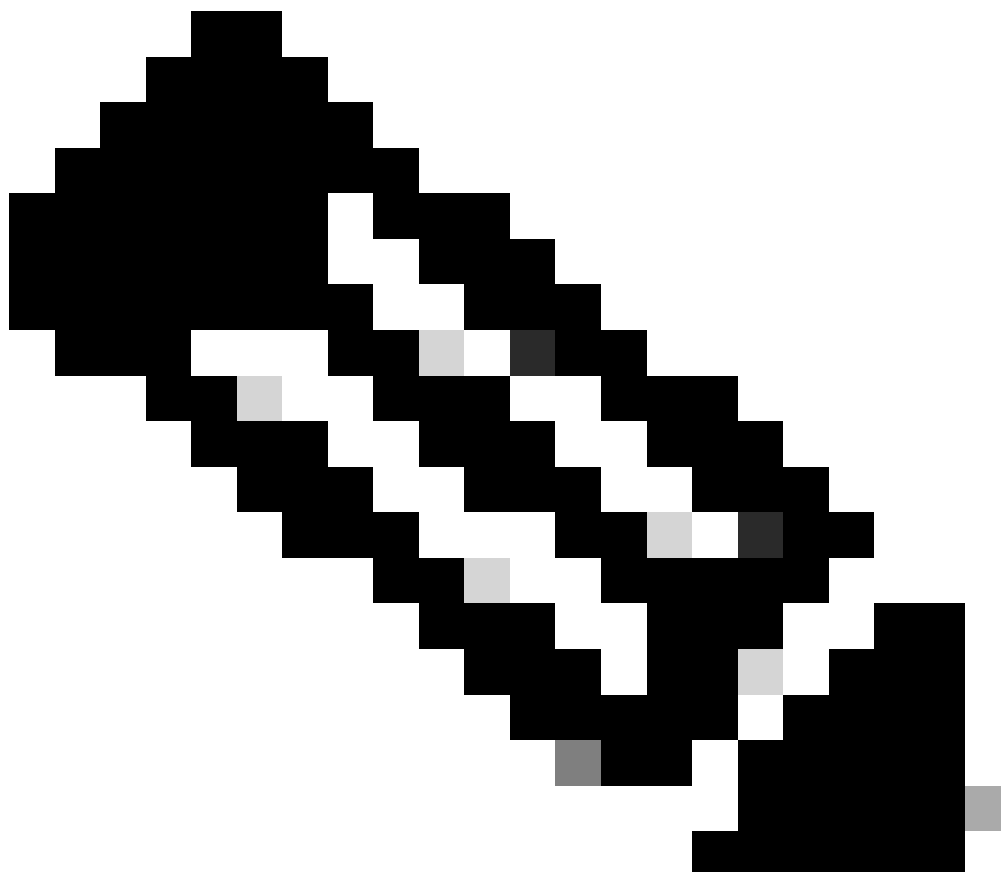
Si nécessaire, vous pouvez remplacer cette restriction de limitation à l'aide de la commande du mode `license smart sync` d'exécution privilégié

Configurer

Procédez comme suit pour configurer SLP avec Smart Transport :

1. Configurez Smart comme type de transport et utilisez l'URL par défaut.

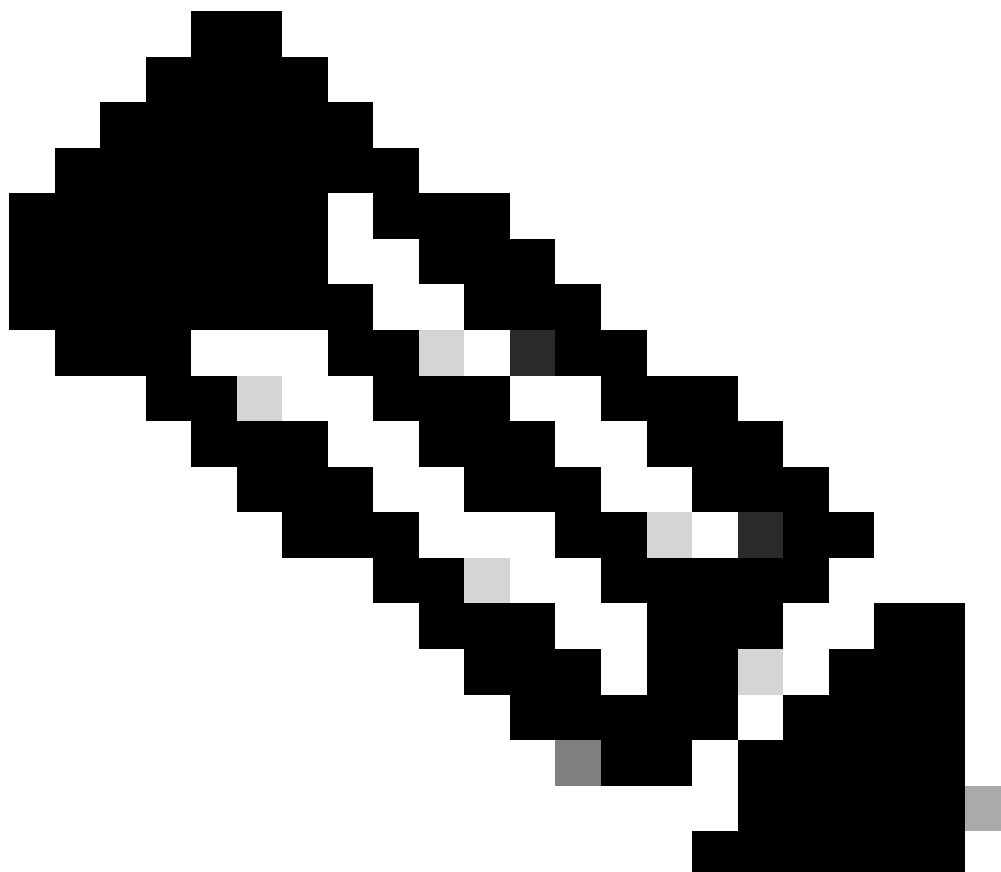
```
Switch#configure terminal
Switch(config)#license smart transport smart
Switch(config)#license smart url default
```



Remarque : Si un VRF est utilisé pour Smart Transport, il est license smart vrf nécessaire de le configurer.

-
2. Configurez le serveur DNS et l'interface source pour la résolution DNS et les connexions client HTTP.

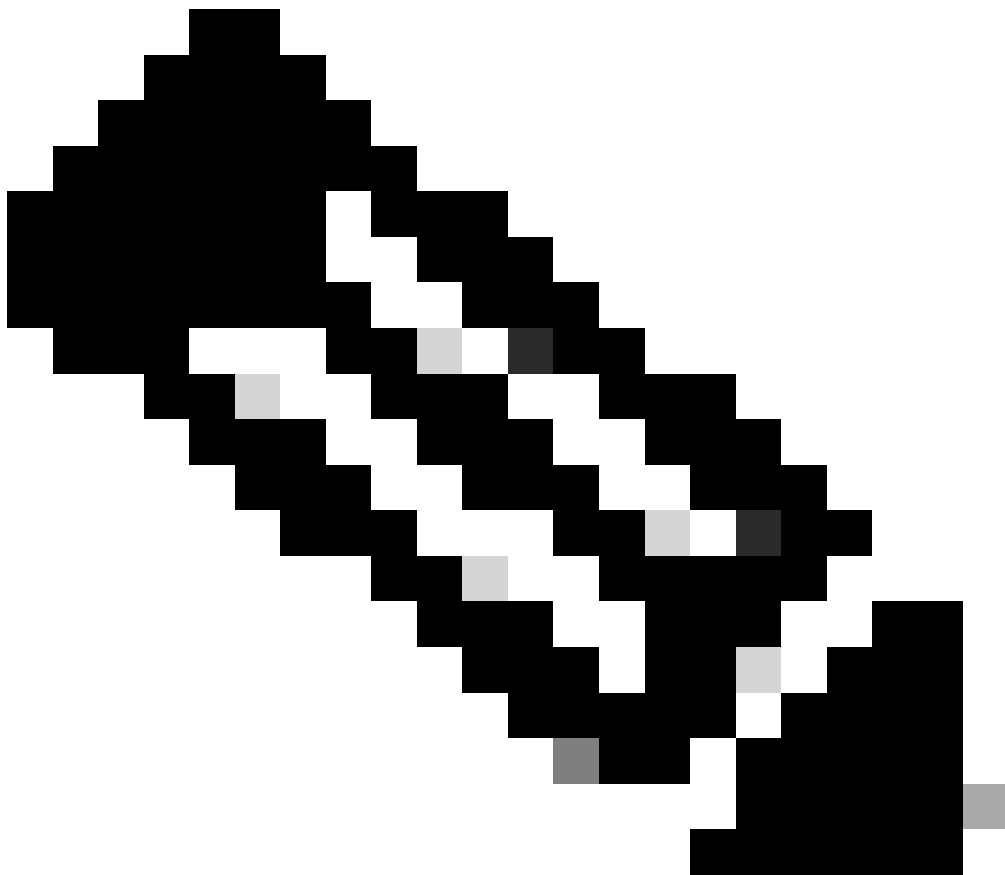
```
Switch(config)#ip domain lookup
Switch(config)#ip name-server 10.31.104.74
Switch(config)#ip domain name cisco.com
Switch(config)#ip domain lookup source-interface Vlan10
```



Remarque : Si un VRF est utilisé pour Smart Transport, la variante VRF de ces commandes doit être utilisée.

3. Si nécessaire, configurez un proxy HTTPS.

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



Remarque : Le serveur proxy peut être configuré à l'aide de son adresse IP ou de son nom d'hôte.

-
4. Générez un jeton dans le compte virtuel. Pour effectuer cette étape, suivez le processus décrit dans [ce document](#).
 5. Installez le code de confiance sur le commutateur.

```
Switch#license smart trust idtoken NGFkODgzMGUtZmNkMS00NTRjLWI5MjUtYjI0YWYzZjU1ZGQzLTE3NDYnNjU5%OA
```

```
[OK]
```

Une fois l'établissement de la confiance avec CSSM réussi, un syslog similaire à celui-ci est affiché.

*Jan 24 23:19:05.144: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was successfully installed.

En outre, indiquez l'heure d'installation du code d'approbation.

<#root>

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

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

<--- Trust code was installed

Enfin, le journal des événements du compte virtuel indique que le commutateur a été ajouté.

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 64 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 from 2025-Feb-21 17:12:46 where a product instance connected, and another from 2025-Feb-21 16:44:09 where a new token was added.

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	...

Journal des événements du compte virtuel montrant le périphérique.

Dépannage

Si l'établissement de la confiance avec CSSM échoue, un syslog indiquant la raison de l'échec s'affiche.

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

Les raisons possibles d'un échec de communication sont les suivantes :

- Impossible de résoudre le nom d'hôte/de domaine du serveur : L'URL Smart Transport ou le nom d'hôte du serveur proxy n'a pas été résolu par DNS. Validez les configurations de résolution de noms et l'accessibilité du serveur DNS.

- Délai de connexion dépassé : La connexion a été tentée, mais il n'y a pas eu de réponse. Vérifiez que la connexion HTTPS avec CSSM est établie à l'aide de captures de paquets et vérifiez si un périphérique, tel qu'un serveur proxy ou un pare-feu, bloque la connectivité. Si vous utilisez un serveur proxy, assurez-vous que le port correct est utilisé.

Suivez ces étapes et les commandes de validation pour dépanner SLP avec Smart Transport :

1. Validez les journaux d'événements 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_re1/114"
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. Validez la connectivité avec CSSM en envoyant une requête ping et en essayant une connexion Telnet. Cela permet de vérifier que le nom est résolu et qu'il n'y a pas de bloc administratif entre le commutateur et le 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]

Si vous utilisez un serveur proxy, vous pouvez également essayer les mêmes commandes en utilisant l'adresse IP et le port du serveur 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. Vérifiez que les rapports RUM sont envoyés et qu'il y a une réponse.

```
<#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 une requête est envoyée mais qu'il n'y a pas de réponse de CSSM, la `show license history` commande n'affiche aucune donnée JSON pour la réponse donnée et plus de détails sur l'échec peuvent être obtenus.

<#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. Déclenchez le commutateur pour envoyer un rapport RUM à synchroniser avec 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. Pour vérifier que le commutateur établit la connexion HTTPS avec le CSSM, vous pouvez effectuer une capture de paquets. Voici un exemple de capture de paquets d'une connexion réussie à l'aide d'un serveur 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
```

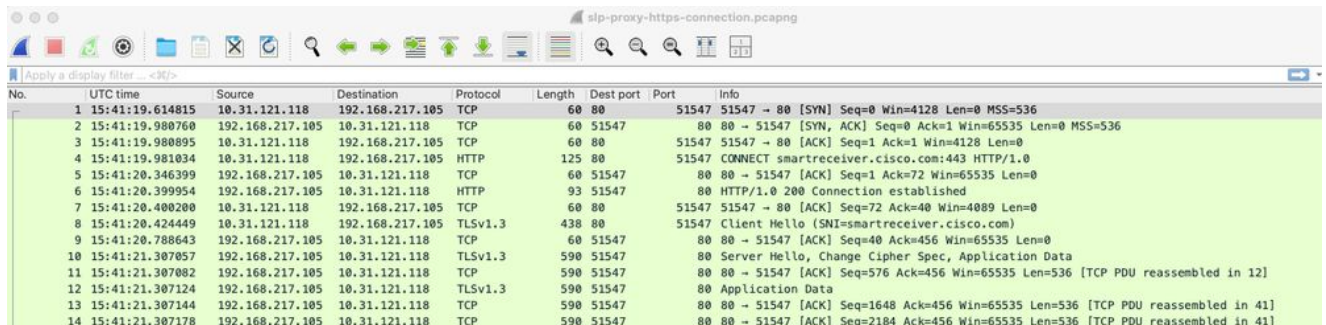
```
REQUEST: Jan 24 15:41:58 2025 UTC
```

```
Switch#
```

```
monitor capture CSSM stop
```

```
Switch#
```

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

A screenshot of the Wireshark network protocol analyzer interface. The title bar shows the file name 'slp-proxy-https-connection.pcapng'. The main display area shows a list of 14 captured packets. The first packet is a SYN packet from 10.31.121.118 to 192.168.217.105 on port 80. Subsequent packets show the TCP connection being established and the start of an HTTP/1.0 connection. The 'Info' pane on the right shows details for the selected packet, including the 'CONNECT smartreceiver.cisco.com:443 HTTP/1.0' message.

No.	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]

Capture de paquets d'une connexion HTTPS réussie avec CSSM à l'aide d'un serveur proxy.

- Si la capture de paquets indique que la connexion HTTPS tente d'être établie mais échoue, cela peut être dû à un échec de connexion TLS ou SSL. Ces débogages peuvent être utilisés pour des recherches plus approfondies.

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

- Si, à un moment donné, le code d'approbation installé doit être supprimé du commutateur, une réinitialisation de la fabrique de licences Smart peut être effectuée. Ce processus nécessite un rechargement. Après la réinitialisation d'usine, un nouveau code d'approbation peut être installé. Cette commande supprime toutes les informations de licence, y compris la stratégie.

```
<#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
```

Informations connexes

- [Licences intelligentes utilisant la politique pour les commutateurs de la gamme Cisco Catalyst 9000](#)
- [Comprendre les licences Smart pour la commutation Catalyst](#)
- [Cisco Live : Introduction à la politique d'utilisation des licences Smart](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.