

Fehlerbehebung bei SLP Smart Transport auf Catalyst Switches der Serie 9000

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Fehlerbehebung bei Smart Licensing mithilfe von Policy (SLP) mithilfe von Smart Transport auf Catalyst 9000-Switches beschrieben.

Voraussetzungen

Anforderungen

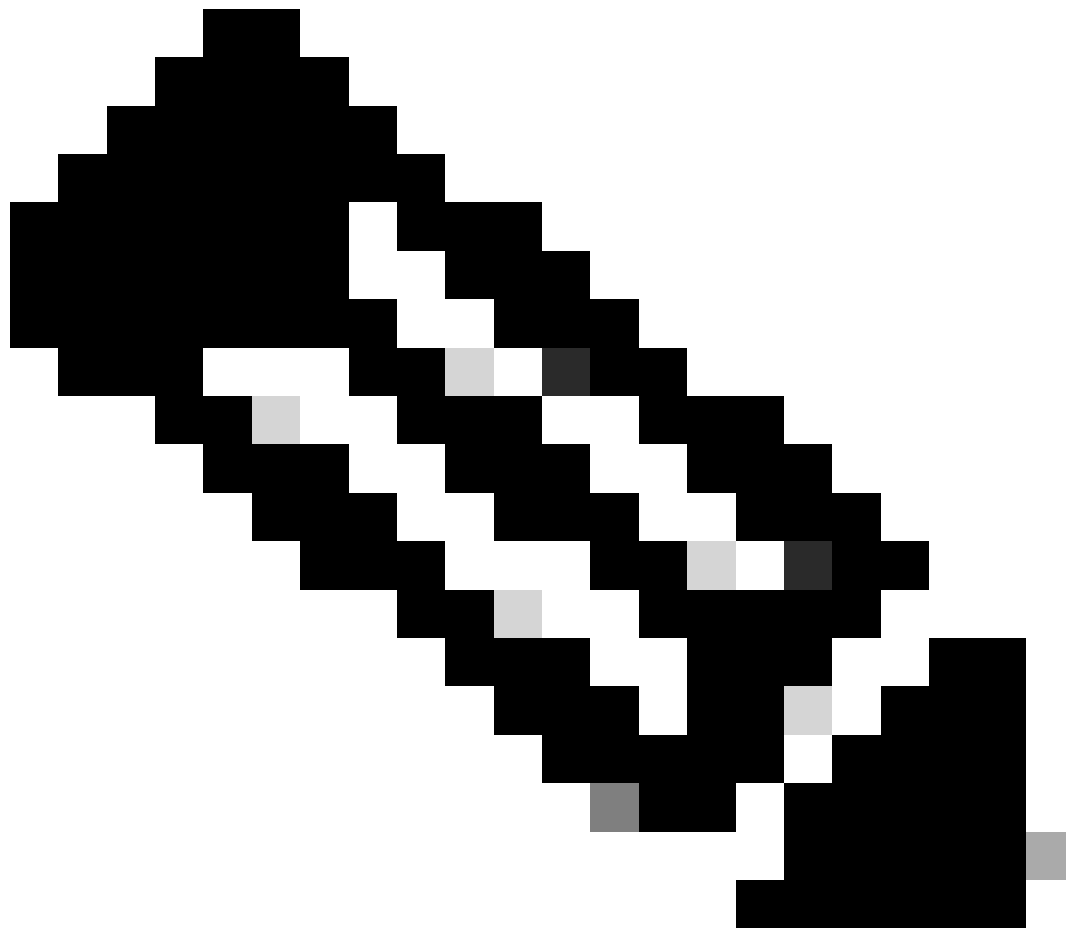
Cisco empfiehlt, dass Sie mit diesem Thema vertraut sind:

- Smart Licensing mithilfe einer Richtlinie auf Cisco IOS® XE-Geräten

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Catalyst 9200
- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS XE 17.9.1 und neuere Versionen



Anmerkung: Die Befehle, um diese Funktionen auf anderen Cisco Plattformen zu aktivieren, finden Sie im entsprechenden Konfigurationsleitfaden.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Smart Licensing Using Policy ist eine erweiterte Version von Smart Licensing, die als primäres Ziel entwickelt wurde, eine Lizenzierungslösung bereitzustellen, die sicherstellt, dass der Betrieb Ihres Netzwerks nicht unterbrochen wird. Statt Unterbrechungen zu vermeiden, stellt es eine Compliance-Beziehung her, bei der die von Ihnen erworbenen und genutzten Hardware- und Softwarelizenzen berücksichtigt werden.

Damit die Smart Licensing-Berichte ordnungsgemäß funktionieren, verbindet sich der Catalyst

9000-Switch mit Cisco Smart Software Manager (CSSM), um die Lizenznutzung zu melden. CSSM dient als zentralisierte Plattform zur Verwaltung aller Cisco Softwarelizenzen und zur Nutzungsüberprüfung, wodurch die Planung für zukünftige Lizenzanforderungen erleichtert wird.

Es gibt mehrere Topologien, über die ein Catalyst 9000-Switch eine Verbindung zu CSSM herstellen kann. In diesem Dokument wird jedoch die spezifische Topologie behandelt, in der der Switch direkt mit CSSM verbunden ist. Dies bedeutet, dass der Switch in der Lage sein muss, eine Verbindung mit dem CSSM herzustellen, der im Internet gehostet wird.

In dieser direkten Verbindungstopologie gibt es zwei Transportoptionen: Smart Transport und Call Home, wobei Smart Transport die empfohlene Methode ist. Darüber hinaus unterstützt Smart Transport die Verwendung eines HTTPS-Proxys und ermöglicht die Auswahl einer bestimmten VRF-Instanz für die Smart Licensing-Kommunikation mit CSSM.

Bei Verwendung von Smart Transport tauscht der Catalyst 9000-Switch Lizenznutzungsinformationen mit CSSM im JavaScript Object Notation (JSON)-Format innerhalb einer HTTPS-Nachricht aus. Diese Informationen, der so genannte RUM-Bericht, werden vom Switch gesendet, und die Antwort vom CSSM wird als ACK bezeichnet.

Die minimale Berichtshäufigkeit für diese Topologie wird auf einen Tag gedrosselt. Das bedeutet, dass die Produktinstanz nicht mehr als einen RUM-Bericht pro Tag sendet, sodass nicht zu viele Berichte für bestimmte Lizenzen generiert und übertragen werden. Dies hilft bei der Behebung von speicherbezogenen Problemen und Systemverlangsamungen, die durch eine Überproduktion von RUM-Berichten verursacht werden.

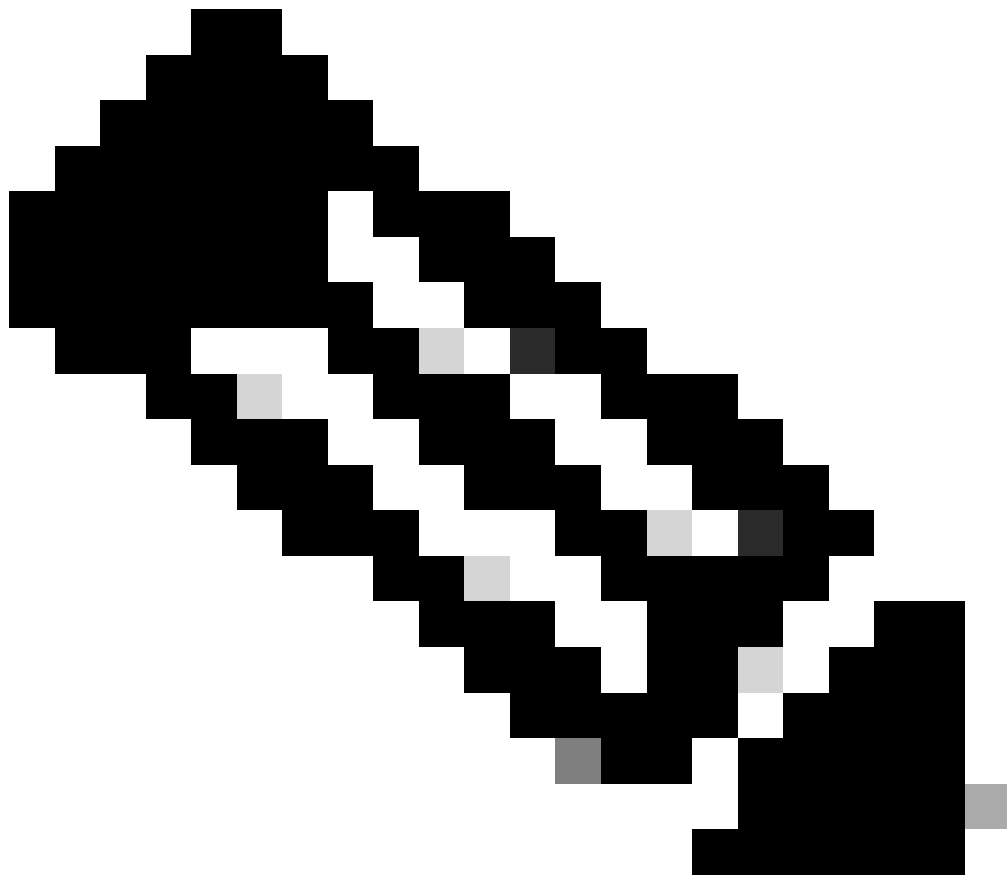
Bei Bedarf können Sie diese Einschränkung überschreiben, indem Sie den `license smart sync` Befehl im privilegierten EXEC-Modus verwenden.

Konfigurieren

Gehen Sie folgendermaßen vor, um SLP mit Smart Transport zu konfigurieren:

1. Konfigurieren Sie Smart als Transporttyp, und verwenden Sie die Standard-URL.

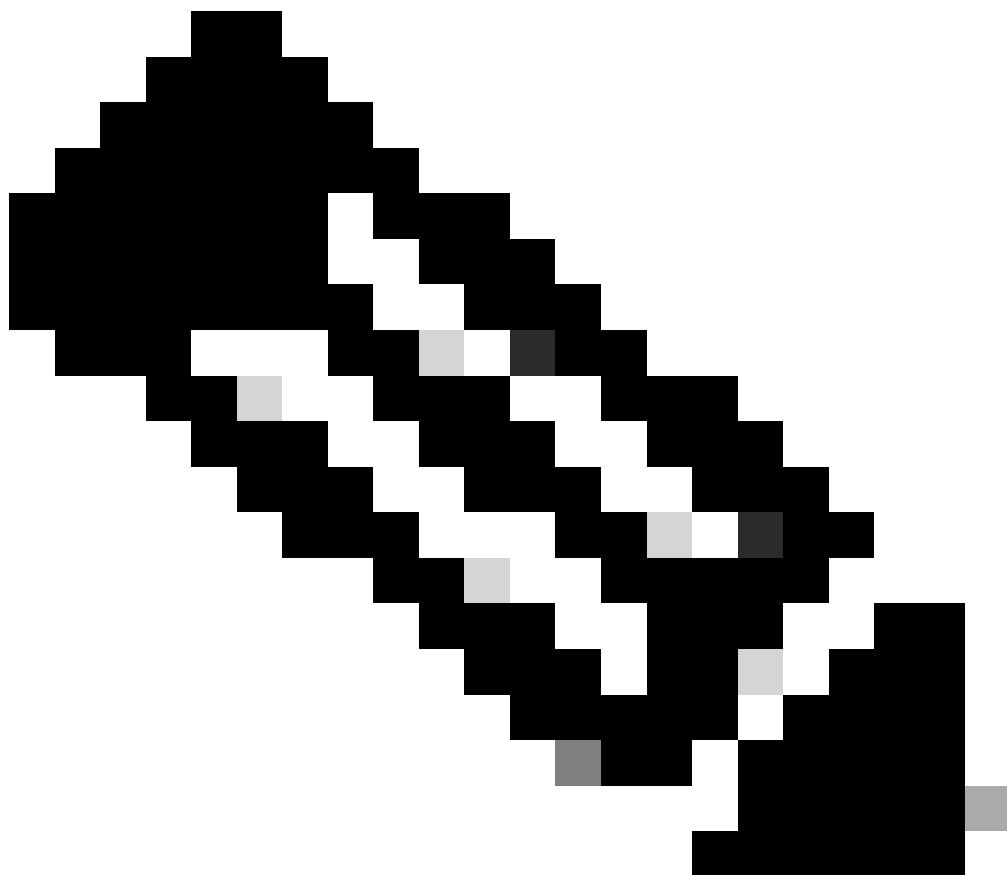
```
Switch#configure terminal
Switch(config)#license smart transport smart
Switch(config)#license smart url default
```



Anmerkung: Wenn eine VRF-Instanz für Smart Transport verwendet wird, muss `license smart vrf` konfiguriert werden.

-
2. Konfigurieren Sie den DNS-Server und die Quellschnittstelle für die DNS-Auflösung und HTTP-Clientverbindungen.

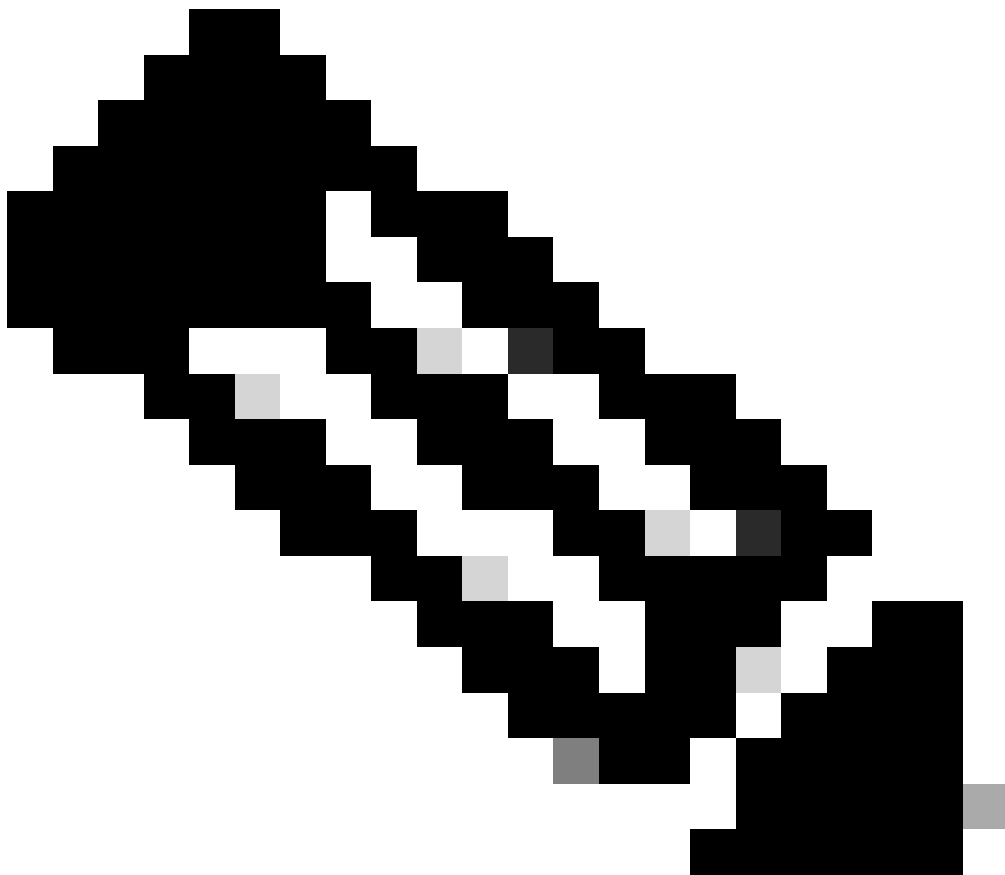
```
Switch(config)#ip domain lookup
Switch(config)#ip name-server 10.31.104.74
Switch(config)#ip domain name cisco.com
Switch(config)#ip domain lookup source-interface Vlan10
```



Anmerkung: Wenn eine VRF-Instanz für Smart Transport verwendet wird, muss die VRF-Variante dieser Befehle verwendet werden.

3. Konfigurieren Sie ggf. einen HTTPS-Proxy.

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



Anmerkung: Der Proxyserver kann mit seiner IP-Adresse oder seinem Hostnamen konfiguriert werden.

-
4. Erstellen Sie ein Token im Virtual Account. Führen Sie zum Abschließen dieses Schritts die in [diesem Dokument](#) beschriebenen Schritte aus.
 5. Installieren Sie den vertrauenswürdigen Code auf dem Switch.

```
Switch#license smart trust idtoken NGFkODgzMGUtZmNkMS00NTRjLWI5MjUtYjI0YWYzZjU1ZGQzLTE3NDAYNjU5%OA
```

```
[OK]
```

Bei erfolgreicher Einrichtung der Vertrauensstellung mit CSSM wird ein ähnliches Syslog angezeigt.

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

Darüber hinaus wird der Zeitpunkt der Installation des Trust-Codes angezeigt.

<#root>

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

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

<--- Trust code was installed

Schließlich wird im Virtual Account Event Log angezeigt, dass der Switch hinzugefügt wurde.

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, the 'Virtual Account' section is active, displaying a list of alerts with 65 Major, 440 Minor, and 64 Informational alerts. The 'Event Log' tab is selected, showing a table of events. The table has columns for Message, Time, and User. Two events are listed: one where a product instance was added to the virtual account, and another where a new token was 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 "MzgWMDAwMTIIOGVkOC00OEWEXLTgzZmEIMzVhNTZkMDAyNTJhLTE3NDI3NDgy%0ANDkyMTF8U1N4MFV0R..."	2025-Feb-21 16:44:09	...

Ereignisprotokoll für virtuelle Konten mit Gerät.

Fehlerbehebung

Wenn die Einrichtung der Vertrauensstellung mit CSSM fehlschlägt, wird ein Syslog mit der Ursache des Fehlers angezeigt.

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

Mögliche Gründe für einen Kommunikationsfehler sind:

- Der Server-Hostname/Domänenname konnte nicht aufgelöst werden: Die Smart Transport-URL oder der Hostname des Proxyservers wurde nicht durch DNS aufgelöst. Validieren Sie die Konfiguration der Namensauflösung und die Erreichbarkeit des DNS-Servers.

- Zeitüberschreitung der Verbindung: Die Verbindung wurde versucht, aber es gab keine Antwort. Überprüfen Sie, ob die HTTPS-Verbindung mit CSSM mithilfe von Paketerfassungen hergestellt wird, und prüfen Sie, ob ein Gerät wie ein Proxyserver oder eine Firewall die Verbindung blockiert. Wenn Sie einen Proxyserver verwenden, stellen Sie sicher, dass der richtige Port verwendet wird.

Befolgen Sie die folgenden Schritte und Validierungsbefehle, um eine Fehlerbehebung für SLP mit Smart Transport durchzuführen:

1. Überprüfen Sie die Smart Licensing-Ereignisprotokolle.

```
<#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. Validieren Sie die Verbindung mit CSSM, indem Sie einen Ping senden und eine Telnet-Verbindung herstellen. Dadurch wird sichergestellt, dass die Namensauflösung erfolgt und keine administrative Blockierung zwischen dem Switch und dem CSSM auftritt.

<#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]

Wenn ein Proxyserver verwendet wird, können Sie die gleichen Befehle auch unter Verwendung der IP-Adresse und des Ports des Proxyservers ausprobieren.

<#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. Überprüfen Sie, ob RUM-Berichte gesendet werden und ob eine Antwort vorliegt.

```
<#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

Wenn eine Anforderung gesendet wurde, aber keine Antwort vom CSSM vorliegt, zeigt der `show license history message` Befehl keine JSON-Daten für die angegebene Antwort an, und es können weitere Details zum Fehler abgerufen werden.

<#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. Auslösen des Switches zum Senden eines RUM-Berichts zur Synchronisierung mit 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. Um zu überprüfen, ob der Switch die HTTPS-Verbindung mit dem CSSM herstellt, können Sie eine Paketerfassung durchführen. Dies ist ein Beispiel für die Paketerfassung einer erfolgreichen Verbindung mit einem Proxyserver.

```
<#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
```

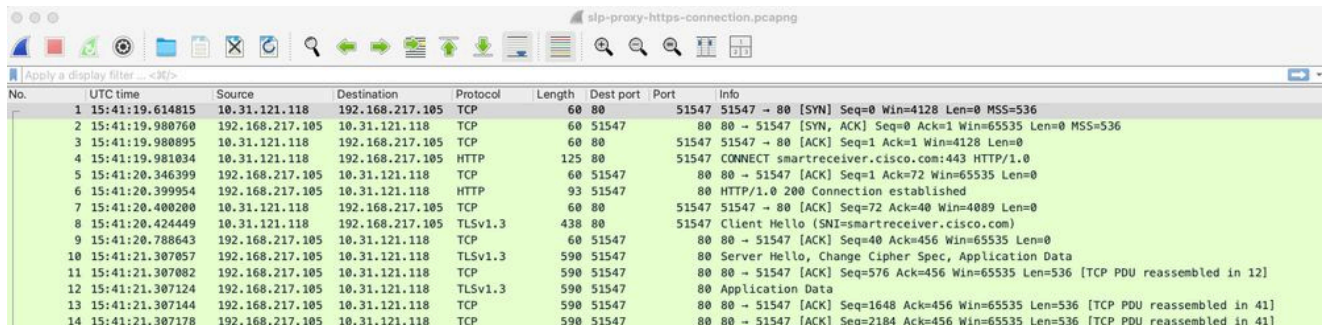
```
REQUEST: Jan 24 15:41:58 2025 UTC
```

```
Switch#
```

```
monitor capture CSSM stop
```

```
Switch#
```

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



No.	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	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	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	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	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	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]

Paketerfassung einer erfolgreichen HTTPS-Verbindung mit CSSM über einen Proxyserver.

6. Wenn die Paketerfassung zeigt, dass die HTTPS-Verbindung versucht wird, hergestellt zu werden, aber fehlschlägt, kann dies auf einen TLS- oder SSL-Handshake-Fehler zurückzuführen sein. Diese Debugs können für weitere Untersuchungen verwendet werden.

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

7. Wenn der installierte Vertrauenscode von einem Switch entfernt werden muss, kann ein Zurücksetzen auf die Werkseinstellungen von Smart Licensing durchgeführt werden. Dieser Prozess erfordert ein erneutes Laden. Nach dem Zurücksetzen auf die Werkseinstellungen kann ein neuer Vertrauenscode installiert werden. Mit diesem Befehl werden alle Lizenzinformationen entfernt, einschließlich der Richtlinie.

```
<#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

Zugehörige Informationen

- [Smart Licensing - Nutzungsrichtlinie für Cisco Catalyst Switches der Serie 9000](#)
- [Smart Licensing für Catalyst Switching verstehen](#)
- [Cisco Live: Einführung in die Smart Licensing-Nutzungsrichtlinie](#)
- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.