

Catalyst 9000交換機上的SLP智慧傳輸故障排除

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文說明如何使用Catalyst 9000交換器上的智慧傳輸，對使用原則(SLP)的智慧授權進行疑難排解。

必要條件

需求

思科建議您瞭解並熟悉以下主題：

- 在Cisco IOS® XE裝置上使用策略的智慧許可。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Catalyst 9200
- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS XE 17.9.1及更高版本



附註：請參閱適當的組態設定指南來瞭解使用的命令，以便在其他思科平台上啟用這些功能。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

使用策略的智慧許可是智慧許可的增強版本，其設計的主要目標是提供許可解決方案，確保您的網路運營保持無中斷。它不是破壞性的，而是建立了合規性關係，以說明您購買和使用的硬體和軟體許可證。

為使智慧許可報告正常工作，Catalyst 9000交換機與思科智慧軟體管理器(CSSM)連線以報告許可證使用情況。CSSM是管理所有思科軟體許可證和稽核使用情況的集中平台，可幫助規劃未來的許可需求。

Catalyst 9000交換器可透過多個拓撲連線到CSSM，但本檔案重點介紹交換器直接連線到CSSM的

特定拓撲。這表示交換器必須能夠與託管在Internet上的CSSM連線並建立連線。

在此直接連線拓撲中，有兩種傳輸選項：Smart Transport和Call Home，推薦使用Smart Transport。此外，智慧傳輸支援使用HTTPS代理並允許選擇特定VRF來處理與CSSM的智慧許可通訊。

使用智慧傳輸時，Catalyst 9000交換機在HTTPS消息中與CSSM交換許可證使用資訊，該資訊採用JavaScript對象表示法(JSON)格式。此資訊稱為RUM報告，由交換機傳送，來自CSSM的響應稱為ACK。

此拓撲的最小報告頻率被限制為一天。這意味著產品例項每天最多只能傳送一個RUM報告，從而防止生成和傳輸特定許可證的過多報告。這有助於解決記憶體相關問題和由RUM報告超量生成導致的系統減速。

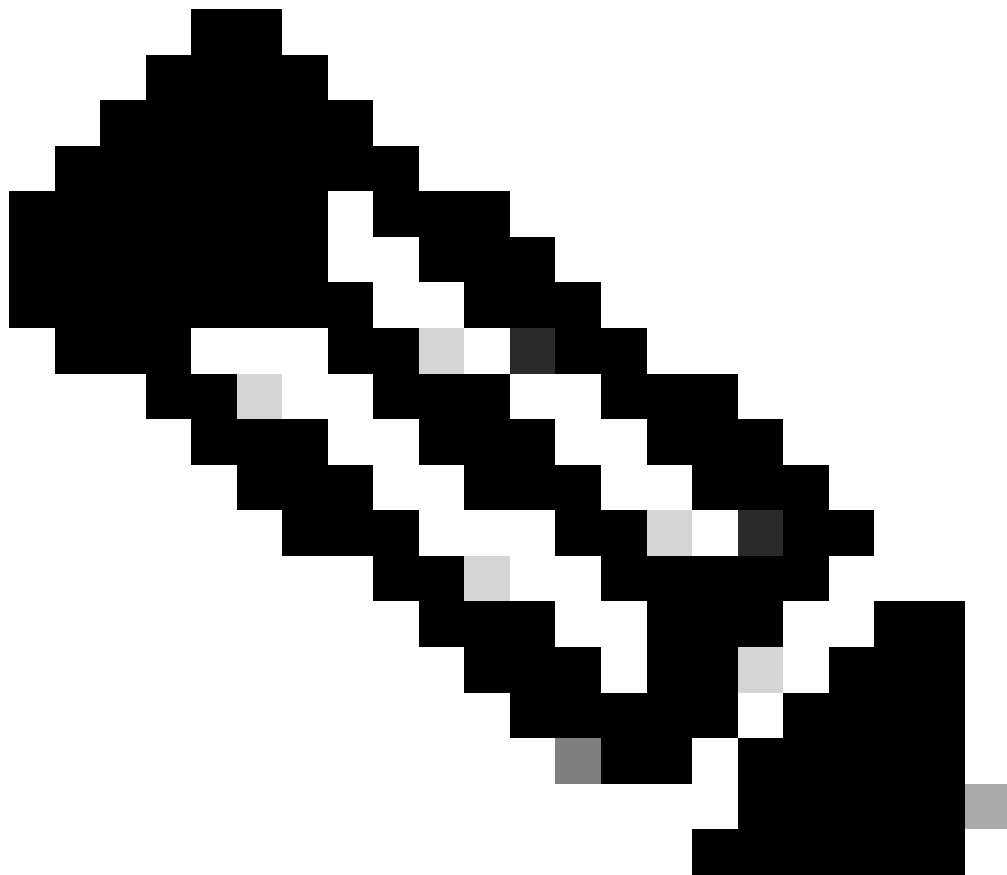
如果需要，您可以在特權EXEC模式下使用`license smart sync`命令來覆蓋此限制限制

設定

請按照以下步驟使用智慧傳輸配置SLP:

1. 將智慧配置為傳輸型別，並使用預設URL。

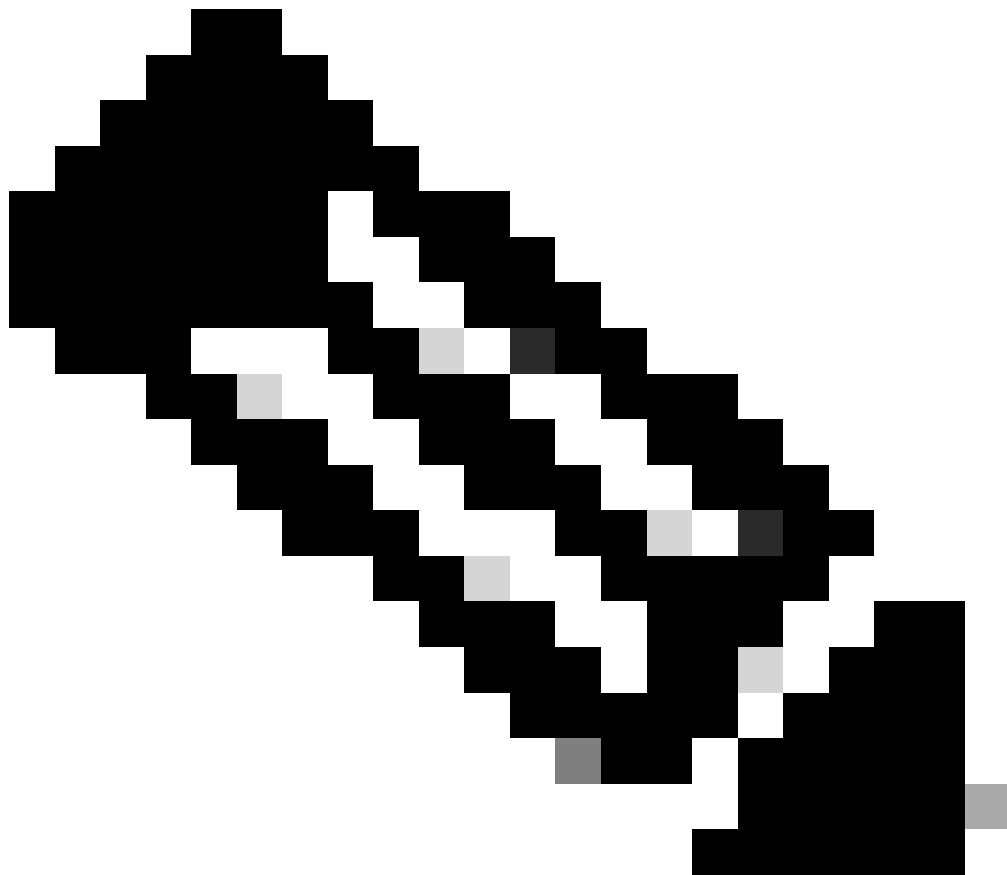
```
Switch#configure terminal
Switch(config)#license smart transport smart
Switch(config)#license smart url default
```



附註：如果將VRF用於智慧傳輸license smart vrf，則需要配置。

2. 為DNS解析和HTTP客戶端連線配置DNS伺服器和源介面。

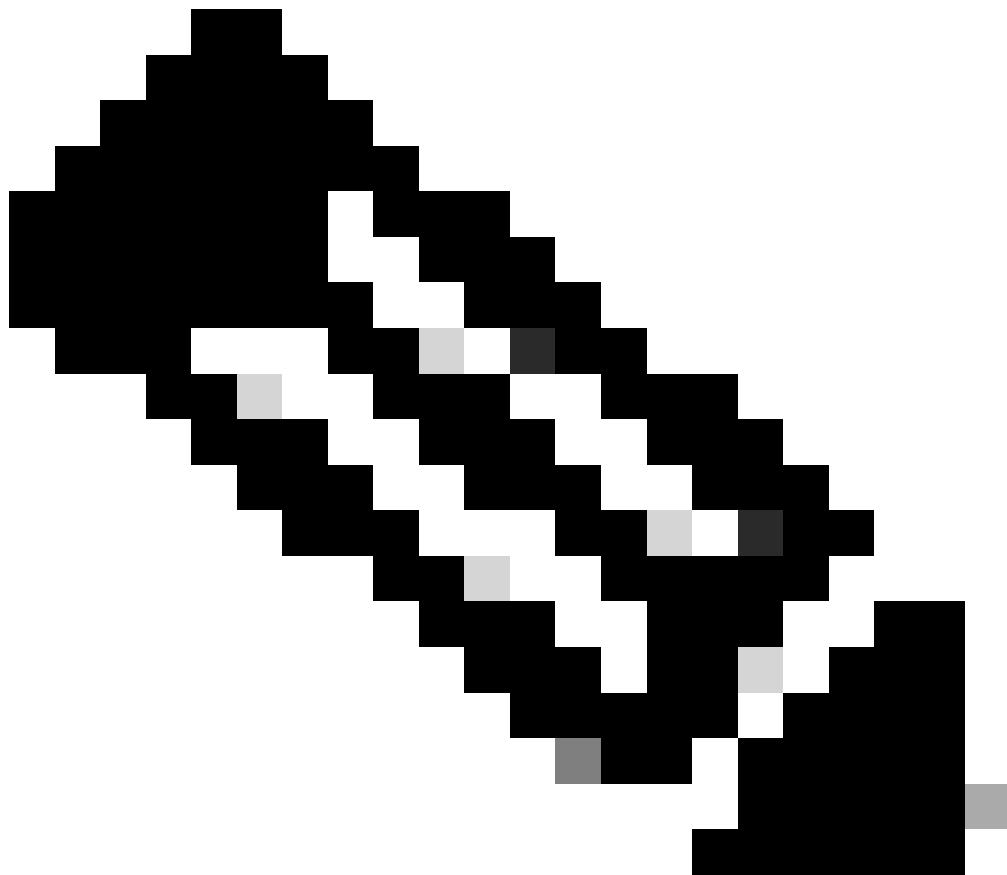
```
Switch(config)#ip domain lookup
Switch(config)#ip name-server 10.31.104.74
Switch(config)#ip domain name cisco.com
Switch(config)#ip domain lookup source-interface Vlan10
```



附註：如果將VRF用於智慧傳輸，則需要使用這些命令的VRF變體。

3. 如果需要，請配置HTTPS代理。

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



附註：可以使用代理伺服器的IP地址或主機名配置代理伺服器。

-
4. 在虛擬帳戶中生成令牌。要完成此步驟，請按照本文檔中概述的[流程操作](#)。
 5. 在交換機上安裝信任代碼。

```
Switch#license smart trust idtoken NGFkODgzMGUtZmNkMS00NTRjLWI5MjUtYjI0YWYzZjU1ZGQzLTE3NDAYNjU5%OA  
[OK]
```

使用CSSM成功建立信任後，將顯示一個與此類似的系統日誌。

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

此外show license status，還顯示信任代碼安裝時間。

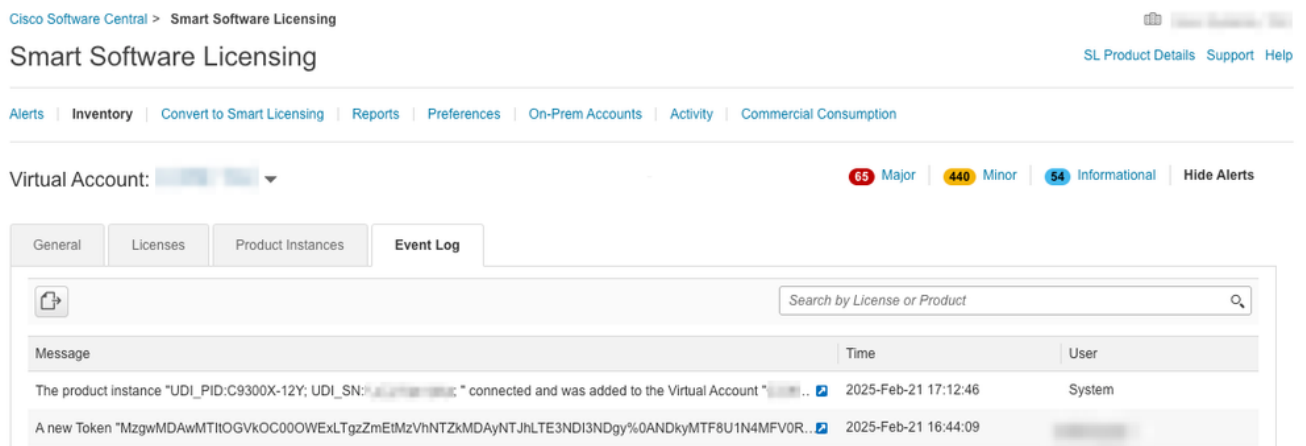
```
<#root>
```

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

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

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

最後，虛擬帳戶事件日誌顯示交換機已新增。



顯示裝置的虛擬帳戶事件日誌。

疑難排解

如果使用CSSM建立信任失敗，將顯示一個系統日誌，指示失敗的原因。

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

通訊失敗的可能原因包括：

- 無法解析伺服器主機名/域名：DNS未解析智慧傳輸URL或代理伺服器主機名。驗證DNS伺服器的名稱解析配置和可達性。
- 連線超時：已嘗試連線，但沒有響應。使用封包擷取驗證正在建立與CSSM的HTTPS連線，並檢查裝置（例如代理伺服器或防火牆）是否封鎖連線。如果使用代理伺服器，請確保使用正確的埠。

按照以下步驟和驗證命令對使用智慧傳輸的SLP進行故障排除：

1. 驗證智慧許可事件日誌。

<#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. 通過傳送ping並嘗試telnet連線來驗證與CSSM的連線。這可驗證名稱解析是否正在進行，以及交換機和CSSM之間是否不存在管理塊。

```
<#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]
```

或者，如果使用的是代理伺服器，則可以使用代理伺服器的IP地址和埠嘗試相同的命令。

```
<#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. 驗證正在傳送RUM報告以及是否存在響應。

<#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

如果傳送了請求但沒有CSSM的響應，則命令未顯示給定響應的JSON數據。show license history message，並且可以獲得有關故障的更多詳細資訊。

<#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. 觸發交換機以傳送RUM報告以與CSSM同步。

<#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. 要驗證交換機是否正在與CSSM建立HTTPS連線，您可以捕獲資料包。以下是使用代理伺服器成功連線的封包擷取範例。

<#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	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	15:41:21.307057	192.168.217.105	10.31.121.118	TLSv1.3	590	51547	80	Server Hello, Change Cipher Spec, Application Data
11	15:41:21.307082	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]

使用代理伺服器成功與CSSM建立HTTPS連線的資料包捕獲。

- 如果資料包捕獲顯示HTTPS連線嘗試建立但失敗，則可能是因為TLS或SSL握手失敗。這些debug可用於進一步調查。

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

- 如果任一時刻需要從交換機刪除已安裝的信任代碼，則可以執行智慧許可工廠重置。此過程需要重新載入。出廠重置後，可以安裝新的信任代碼。使用此命令可刪除所有許可資訊，包括策略。

```
<#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

相關資訊

- [Cisco Catalyst 9000系列交換機的智慧許可使用策略](#)
- [瞭解Catalyst交換的智慧授權](#)
- [Cisco Live:使用策略的智慧許可簡介](#)
- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。