

配置 & 對使用SLUP的Catalyst 9800智慧許可進行故障排除

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[傳統許可與SLUP](#)

[組態](#)

[直接連線CSSM](#)

[已連線到CSLU](#)

[產品例項啟動](#)

[CSLU啟動的](#)

[已連線到內建SSM](#)

[配置透過HTTPS代理的智慧傳輸](#)

[通訊頻率](#)

[許可證工廠重置](#)

[在RMA或硬體更換的情況下](#)

[從特定授權註冊\(SLR\)升級](#)

[疑難排解](#)

[網際網路存取、連線埠檢查與Ping](#)

[系統日誌](#)

[封包擷取](#)

[顯示命令](#)

[調試/btrace](#)

[常見問題](#)

[WLC沒有網際網路存取或防火牆封鎖/變更流量](#)

[資料包捕獲中存在未知的CA警報](#)

[相關資訊](#)

簡介

本檔案介紹如何在Catalyst 9800無線LAN控制器(WLC)上使用原則(SLUP)設定智慧授權並對其進行疑難排解。

必要條件

需求

思科建議您瞭解以下主題：

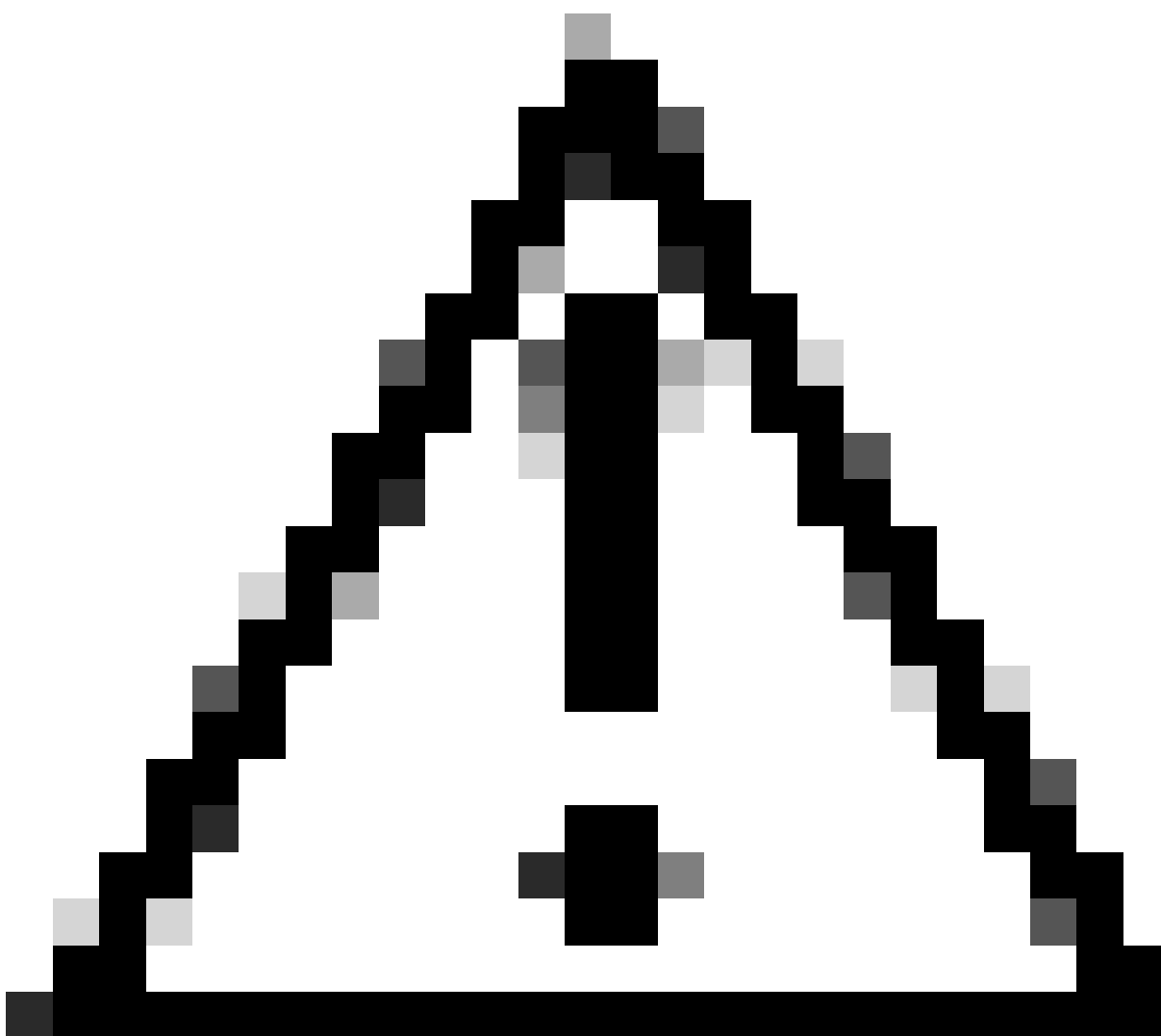
- 使用策略的智慧許可(SLUP)
- Catalyst 9800無線LAN控制器(WLC)

採用元件

本文件所述內容不限於特定軟體和硬體版本。

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

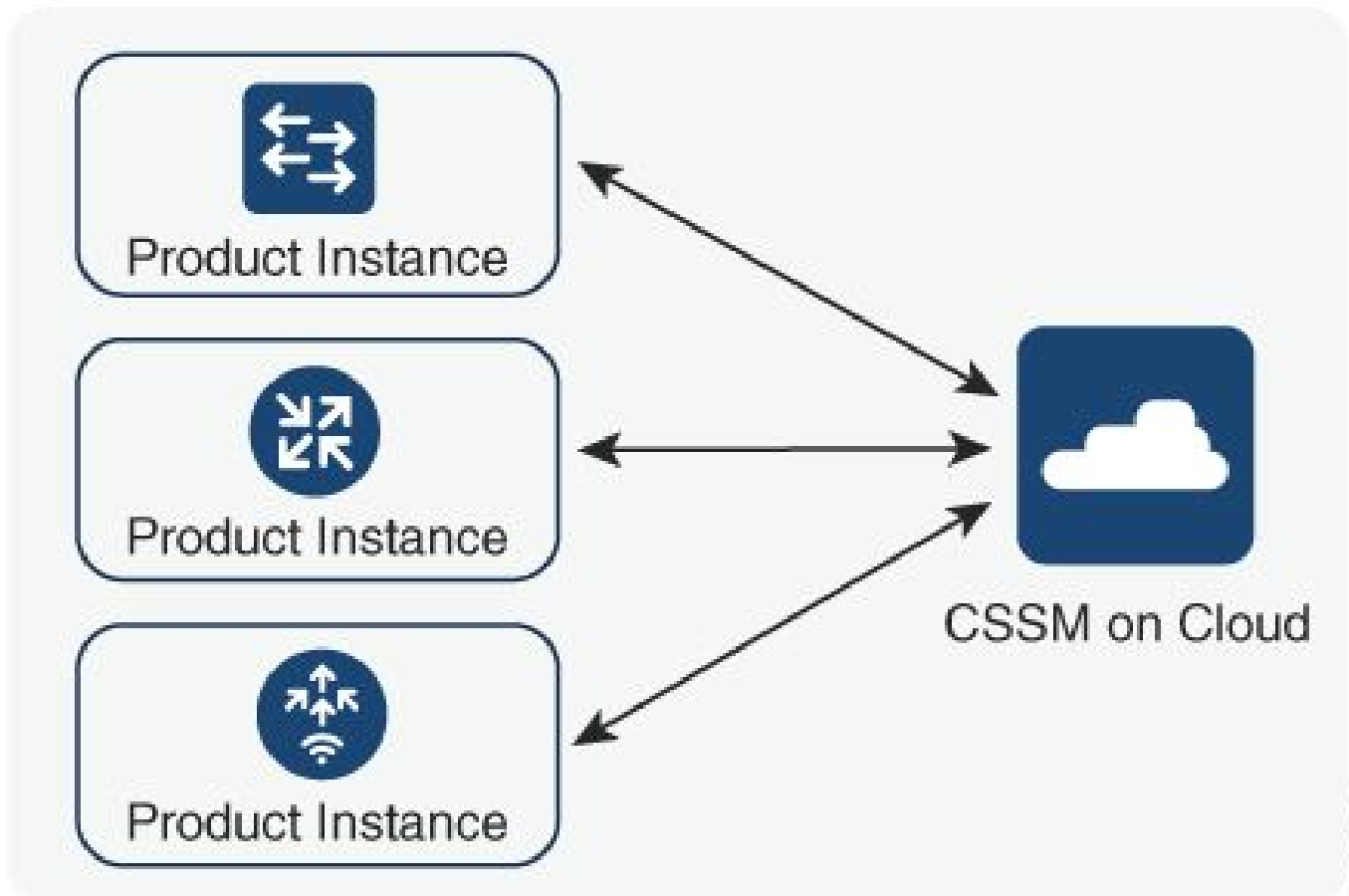


注意：本文中的備註包含有用的建議，或者對文檔未涵蓋的材料的引用。建議您閱讀每個備註。

1. 直接連線到[思科智慧軟體管理器雲](#) (CSSM雲)
2. 透過[CSLU](#) (思科智慧許可證實用程式管理器) 連線到CSSM
3. 已透過[內部智慧軟體管理器](#)連線到CSSM (內部智慧軟體管理器)

本文不包括Catalyst 9800上的所有智慧許可方案，有關詳細資訊，請參閱[使用策略進行智慧許可配置指南](#)。不過，本文確實提供了一系列有用的命令，用於解決Catalyst 9800上使用策略問題的直接連線、CSLU和內部部署SSM智慧許可問題。

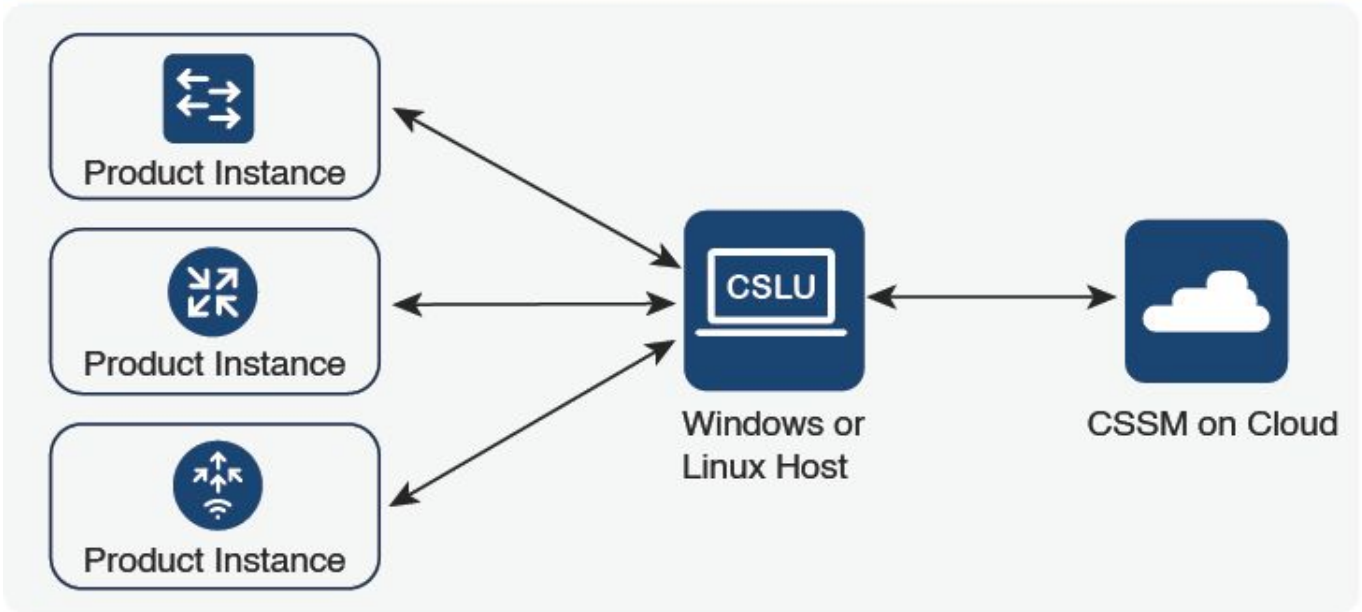
Directly Connected to CSSM



356794

選項 1.直接連線到思科智慧許可雲伺服器(CSSM)

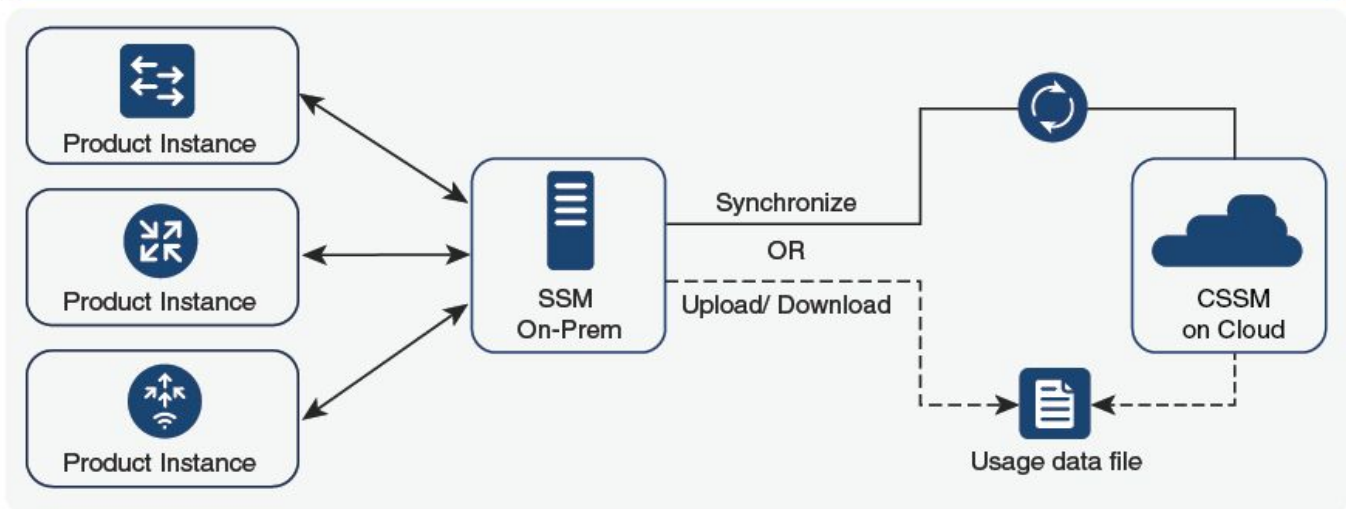
Connected to CSSM Through CSLU



356791


選項 2.透過CSLU連線

SSM On-Prem Deployment



357508

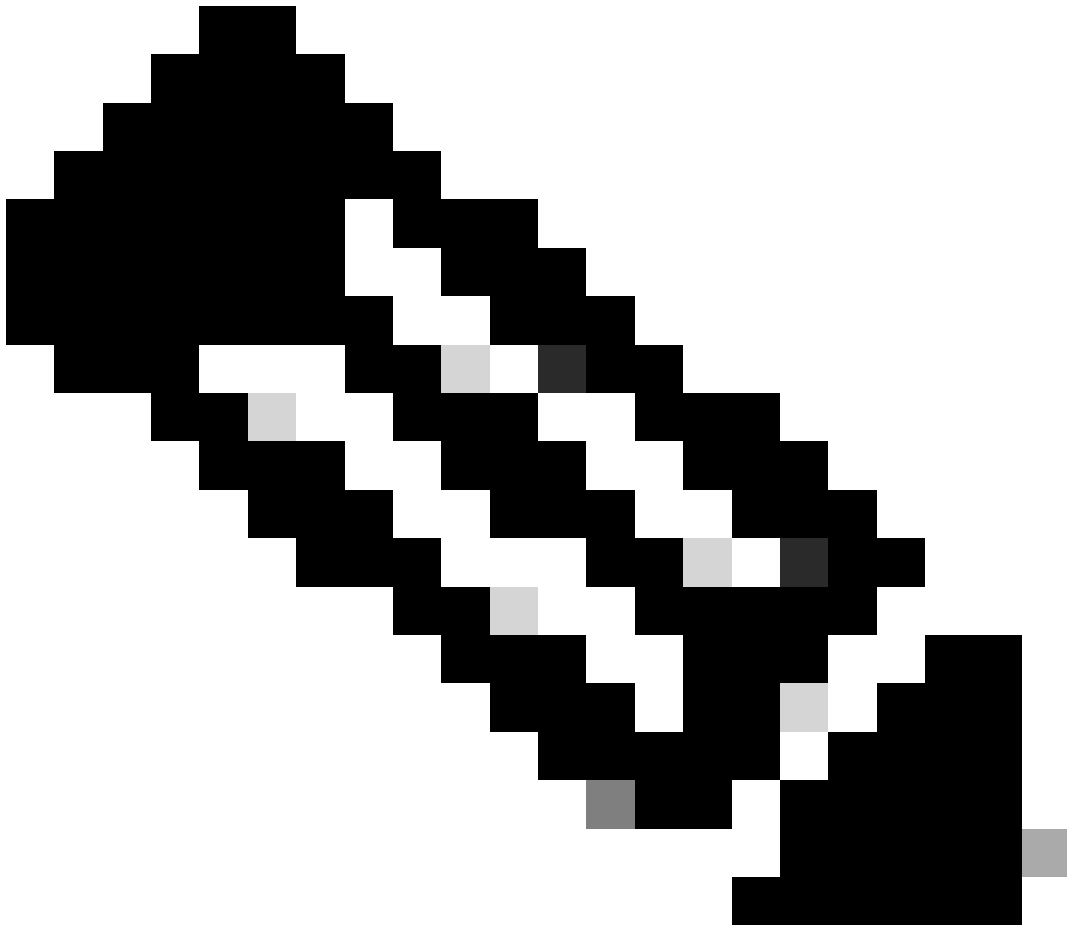
選項 3.透過內部智慧軟體管理員 (內部軟體SSM) 連線

 注意：本文中提到的所有命令僅適用於運行版本17.3.2或更高版本的WLC。

傳統許可與SLUP

Catalyst 9800已引入了使用策略的智慧許可功能，代碼版本為17.3.2。初始17.3.2版本遺漏WLC webUI中的SLUP組態功能表，該功能表是隨17.3.3版本所導入。SLUP在幾個方面不同於傳統的智慧許可：

- WLC現在透過smartreceiver.cisco.com網域(而非tools.cisco.com網域)與CSSM通訊。
 - WLC現在不進行註冊，而是與CSSM或內部版SSM建立信任。
 - CLI命令稍有更改。
 - 智慧許可預留(SLR)已不存在。相反，您可以定期手動報告使用情況。
 - 不再有評估模式。即使沒有許可證，WLC仍繼續以完全容量運行。系統基於榮譽，您應該定期（自動或手動）報告許可證使用情況，以防出現連線網路。
-




警告：如果您使用的是Cisco Catalyst 9800-CL無線控制器，請確保您熟悉以Cisco IOS® XE Cupertino 17.7.1開頭的強制ACK要求。請參閱[Cisco Catalyst 9800-CL無線控制器的RUM報告和確認要求](#)。

組態


直接連線CSSM

在CSSM上建立權杖後，為了建立信任，需要執行以下指令：

 注意：最大令牌數在HA SSO中，WLC的使用計數必須至少為2。

```
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
```

- ip http client source-interface命令指定許可相關資料包將來自的L3介面
- ip http client secure-trustpoint命令指定哪個信任點/證書用於CSSM通訊。可使用show crypto pki trustpoints命令查詢信任點名稱。建議使用自簽名證書TP-self-signed-xxxxxxxxxx證書或製造商安裝證書（也稱為MIC，僅適用於9800-40、9800-80和9800-L），通常稱為CISCO_IDEVID_SUDI。
- Terminal monitor命令使WLC將日誌列印到控制檯，並幫助確認已成功建立信任。可以使用終端無監視器停用它。
- 最後一個命令中的關鍵字all告知HA SSO集群中的所有WLC建立與CSSM的信任。
- 關鍵字force指示WLC覆蓋任何以前建立的信任並嘗試新的信任。

 注意：如果未建立信任，則9800會在執行命令1分鐘後重試，並且在一段時間內不再重試。再次輸入token命令以強制建立新的信任。

已連線到CSLU

Cisco Smart License Utility Manager (CSLU)是基於Windows的應用（在Linux上也可用），使客戶能夠從自己的場所管理許可證及其關聯的產品例項，而不必將其支援智慧許可的產品例項直接連線到Cisco Smart Software Manager (CSSM)。

本節僅介紹9800無線配置。使用CSLU配置許可（例如安裝CSLU、配置CSLU軟體等）需要執行其他步驟，[配置指南](#)中提供了這些步驟。無論您是要實施產品例項啟動的或CSLU啟動的通訊方法，還是完成相應的任務序列。

產品例項啟動

1. 確保從控制器到CSLU的網路可接通性
2. 確保傳輸型別設定為cslu：

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

3. 如果希望控制器發現CSLU，則需要執行操作。如果您希望使用DNS發現CSLU，則無需執行

任何操作。如果您要使用URL發現它，請輸入以下命令：

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

CSLU啟動的

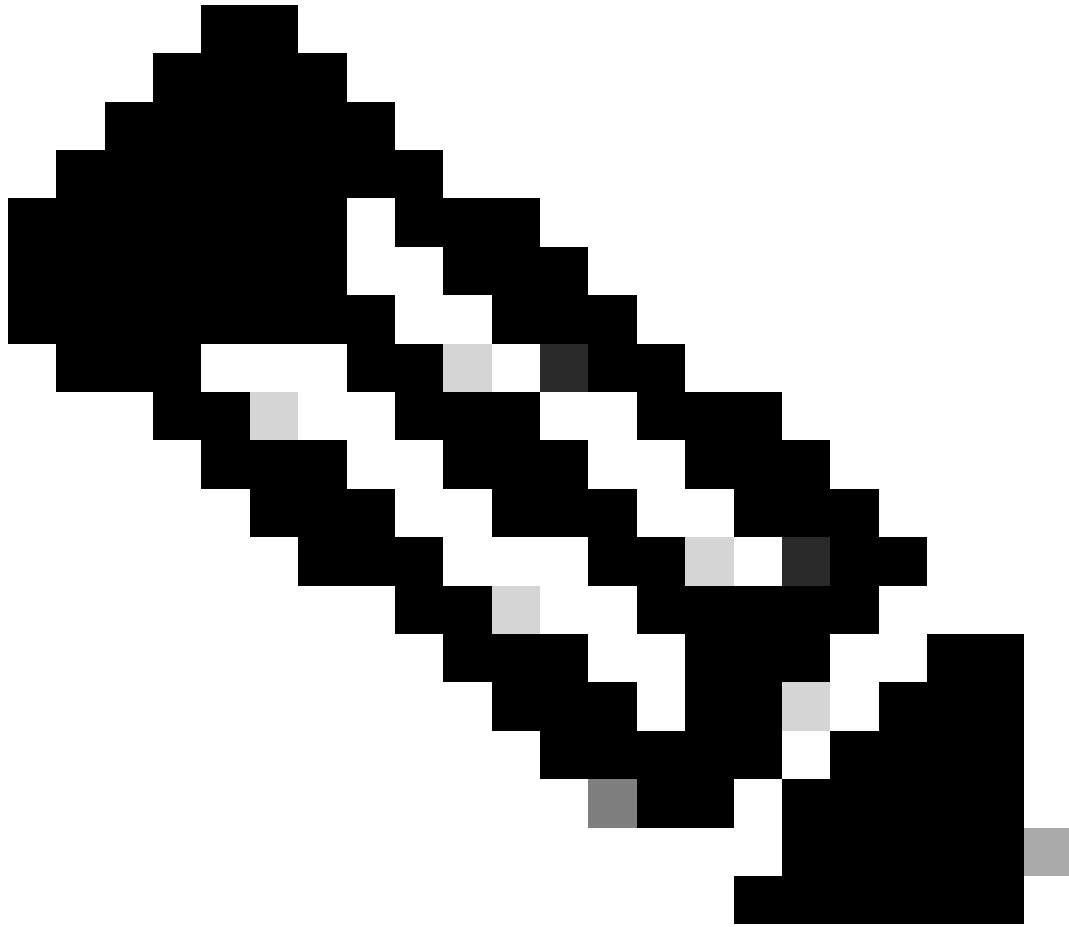
配置CSLU啟動的通訊時，唯一需要的操作是檢查並確保從控制器到CSLU的網路可接通性。

已連線到內建SSM

使用內建SSM的配置與直接連線非常相似。內部部署需要運行版本8-202102或更高版本。對於SLUP版本（17.3.2及更高版本），建議使用CSLU URL和傳輸型別。URL可以從智慧許可 >資產> <虛擬賬戶> >常規部分下的內部WebUI介面獲取。

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

內部SSM不需要使用信任令牌。



注意：如果您收到以下消息：`%PKI-3-CRL_FETCH_FAIL : CRL fetch for trustpoint SLA-TrustPoint`失敗，這是因為您尚未在SLA-TrustPoint下配置`revocation-check none`。這是用於智慧許可的信任點。在內部版本的情況下，許可伺服器上的證書通常是無法進行CRL驗證的自簽名證書，因此要求配置無撤銷檢查。

配置透過HTTPS代理的智慧傳輸

注意：自代碼版本17.9.2起，尚不支援經身份驗證的代理。如果您在基礎設施中使用經過身份驗證的代理，請考慮使用[思科智慧許可證實用程式管理器\(CSLU\)](#)，它支援此型別的伺服器。

要在使用智慧傳輸模式時使用代理伺服器與CSSM通訊，請完成以下步驟：

```
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
```

通訊頻率

可在CLI或GUI中配置的報告間隔無效。

9800 WLC每8小時與CSSM或內部智慧軟體管理器進行通訊，而不管透過Web介面或CLI配置了什麼報告間隔。這表示新加入的存取點可在初次加入後8小時內出現在CSSM上。

您可使用show license air entities summary命令計算和報告許可證的下一期。此命令不是典型show tech或show license all輸出的一部分：

```
<#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
```

許可證工廠重置

Catalyst 9800 WLC可以擁有其所有許可配置和信任工廠重置，並且仍然保留所有其他配置。這需要WLC重新載入：

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

在RMA或硬體更換的情況下

如果需要更換9800 WLC，新裝置必須註冊到CSSM/On-prem智慧軟體管理器，且被視為新裝置。釋放以前裝置的許可證計數需要在產品例項下手動刪除：

Smart Software Licensing

[Feedback](#) [Support](#) [Help](#)[Alerts](#) | [Inventory](#) | [Convert to Smart Licensing](#) | [Reports](#) | [Preferences](#) | [On-Prem Accounts](#) | [Activity](#)Virtual Account: [Wireless TAC](#)3 Major | [Hide Alerts](#)

Name	Product Type	Last Contact	Alerts	Actions
UDI_PID:C9800-CL-K9; UDI_SN:9V4ZPZPN8DW	C9800CL	2021-May-21 21:37:46		Actions ▾ Transfer... Remove...

從特定授權註冊(SLR)升級

舊版WLC 17.3.2之前使用稱為特定授權註冊(SLR)的特殊離線授權方法。在使用SLUP (17.3.2及更高版本) 的發行版本中，此授權方法已被取代。

如果您將使用SLR的9800控制器升級至17.3.2或17.4.1之後的版本，建議您改為離線SLUP報告，而不要依賴SLR指令。儲存許可證使用情況RUM檔案並在智慧許可門戶中註冊。由於SLR在較新版本中不再存在，因此會報告正確的許可證計數，並釋放所有未使用的許可證。許可證不再被阻止，但會報告確切的使用計數。

疑難排解

網際網路存取、連線埠檢查與Ping

新SLUP不是傳統智慧許可使用的tools.cisco.com，而是使用smartreceiver.cisco.com域建立信任。在撰寫本文時，此域解析為多個不同的IP地址。並非所有這些地址都可進行ping操作。不得將Ping用作來自WLC的Internet可達性測試。無法ping通這些伺服器並不意味著它們無法正常工作。

必須使用telnet透過埠443而不是ping作為可達性測試。可以根據smartreceiver.cisco.com域或直接根據伺服器IP地址檢查Telnet。如果沒有封鎖流量，則連線埠必須在輸出中顯示為開啟：

```
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]
```

系統日誌

如果在配置令牌時啟用terminal monitor命令，WLC將在CLI中列印出相關日誌。如果運行show logging命令，也可以獲取這些消息。成功建立的信任的記錄如下所示：

```
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 store
Aug 22 12:13:08.952: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named SLA-KeyPair has been generated or imported
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 installed
```

沒有已定義的DNS伺服器或具有無法運作之DNS伺服器的WLC記錄：

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

具有正常運作的DNS伺服器但沒有網際網路存取的WLC記錄：

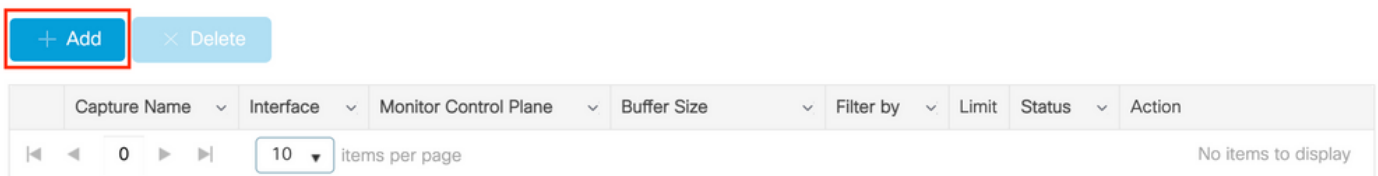
```
Aug 23 09:23:30.701: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart Software Manager
```

封包擷取

即使WLC與CSSM/On-prem SSM之間的通訊已加密並透過HTTPS進行，執行資料包捕獲仍可揭示導致無法建立信任的原因。收集封包擷取的最簡單方法是透過WLC Web介面。

導航到故障排除 > Packet Capture。建立新的擷取點：

Troubleshooting > Packet Capture



確保啟用Monitor Control Plane覈取方塊。將緩衝區大小增加到最大100MB。增加必須捕獲的介面。預設情況下，智慧許可流量來自無線管理介面或使用ip http client source-interface命令定義的介面：

Create Packet Capture

Capture Name*

Filter*

Monitor Control Plane

Buffer Size (MB)*

Limit by* secs == 1.00 hour

Available (3)

- GigabitEthernet1 →
- GigabitEthernet2 →
- Vlan1 →

Selected (1)

- Vlan39 ←

啟動捕獲並運行license smart trust idtoken <token> all force命令：


Troubleshooting > Packet Capture

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

10 items per page 1 - 1 of 1 items

信任建立的資料包捕獲必須包含以下步驟：

1. 使用SYN、SYN-ACK和ACK序列建立TCP會話
2. 透過伺服器 and 客戶端證書交換建立TLS會話。建立以新作業階段票證封包結束
3. 加密的資料包交換(應用資料幀)，其中WLC報告許可證使用情況
4. 透過FIN-PSH-ACK、FIN-ACK和ACK序列終止TCP會話

 注意：資料包捕獲包含很多幀，包括TCP窗口更新和應用資料幀的倍數

由於CSSM雲使用3個不同的公共IP地址，因此為了過濾掉WLC和CSSM之間的所有資料包捕獲，請使用以下wireshark過濾器：

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

如果使用內建SSM，請對SSM IP地址進行過濾：

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

示例：使用直接連線的CSSM成功建立信任的資料包捕獲，所有重要資料包捕獲都已過濾：

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

顯示命令

以下show命令包含有關建立信任的有用資訊：

```
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)

show license history message命令是一個比較有用的命令，因為它可以顯示從WLC傳送並從CSSM接收回的實際消息。

成功建立信任後，會同時列印「請求：8月23日10:18:08 2021 Central」和「響應：8月23日10:18:10 2021 Central」消息。如果RESPONSE行之後沒有任何響應，則表示WLC未收到來自CSSM的響應。

下面是成功建立信任的show license history消息輸出的示例：

```
REQUEST: Aug 23 10:18:08 2021 Central
{"request":{"header":{"request_type":"POLL_REQ"},"sudi":{"udi_pid":"C9800-CL-K9"},"udi_ser...
```

```
NB\}}, {"version": "1.3", "locale": "en_US.UTF-8", "signing_cert_serial_number": "3", "id_cert_ser  
", {"product_instance_identifer": "", "connect_info": {"name": "C_agent", "version": "5.0.9_re1/  
e, {"additional_info": "", "capabilities": ["UTILITY", "DLC", "AppHA", "MULTITIER", "EXPORT_2", "  
Y_USAGE"]}}, {"request_data": {"sudi": {"udi_pid": "C9800-CL-K9", "udi_serial_numbe  
"}, {"timestamp": 1629713888600, "nonce": "11702702165338740293", "product_instance_ide  
"original_request_type": "LICENSE_USAGE", "original_piid": "2e84a42f-c903-44c5-83b2-e62  
": 7898262236}}}, {"signature": {"type": "SHA256", "key": "59152896", "value": "eiJ7IuQaTCFxfUkwlS76WZxa5DRI5A  
OgMqQd5POU6VNSH2j9dHco4T1NJ/aCmBR1MRmkfxyVSWsx41mjJL1mp0Si3ZS4FBMv1F/EBOUfowREe2oz21rQp1cAFpPn5S1aFezW  
/Nu6SQZfIW+IdF+2qnJeNFAIZbNpgOB5d5HIJvDmDIvDu3bMRHhQAwr2KKzGFr6jPz0hs7bGY/+F1fTLQk5LFEUaKTNH/tuxJPFH1F  
h9//uhsd+NaQyfdRF1udkbfUBTFkvPxHW9/5w=="}}
```

```
RESPONSE: Aug 23 10:18:10 2021 Central  
{"signature": {"type": "SHA256", "value": "TXZE034fqAu12jy9V4+HoB2hDSh19au/5sgodiCVatmu671/6MyN7kZfEzREufY8  
SLrjTf04grGeQTCh7yEj0D+gztWXC0u8RBT7/Bo9aBs\n4x1i0E6f1PB3BP6yu7KIEUQZ8yHz1wDT+mVtJGi6TRrtYnV3KQMpCUMF5F  
w0ksf3SfXreNZJuzWXzjHvtm1usCQXw7ZTBzffYsNK001k1J1r\nngvB2PkV7JU1sA481kpIv1Pu16IiJXqk+2PC2IzCrCLG571VN3XgX  
1pE12SHyQ/DAw=="}, {"piid": null, "cert_sn": null}, {"response": {"header": {"version": "1.3", "locale": "  
mp": 1629713890172, "nonce": null, "request_type": "POLL_REQ", "sudi": {"udi_pid": "C9800-CL-K9", "  
9PJK8D70CNB"}, {"agent_actions": null, "connect_info": {"name": "SSM", "version": "1.3", "producti  
s": ["DLC", "AppHA", "EXPORT_2", "POLICY_USAGE", "UTILITY"], "additional_info": ""}, {"signing_c  
", {"id_cert_serial_number": "59152896", "product_instance_identifer": ""}, {"status_code": "FAILE  
"Invalid ProductInstanceIdentifier: 2e84a42f-c903-44c5-83b2-e62e258c780f provided in the polling requ  
262236", "retry_time_seconds": 0, "response_data": ""}, {"sch_response": null}}
```

調試/btrace

在嘗試使用license smart trust idtoken all force命令建立信任幾分鐘後運行此命令。IOSRP日誌非常詳細。附加 | include smart-agent (包括smart-agent) 命令僅獲取智慧許可日誌。

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

您還可以運行這些調試，然後重新配置許可命令以強制建立新連線：

```
debug license events  
debug license errors  
debug license agent all
```

常見問題

WLC沒有網際網路存取或防火牆封鎖/變更流量

WLC上的嵌入式封包擷取可以很容易地檢視WLC是否從CSSM或內部版SSM收到任何回覆。如果沒有回應，防火牆可能會封鎖某些專案。


如果從CSSM雲或內部SSM未收到響應，則在發出請求後1秒，show license history message命令會列印空白響應。

例如，這可以讓您相信已收到空的回應，但實際上根本沒有回應：

```
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
```

 注意：當前有一個增強請求思科漏洞ID [CSCvy84684](#)，該請求在不存在響應時使show license history消息顯示空白響應。這是為了增強show license history message命令的輸出

資料包捕獲中存在未知的CA警報

與CSSM或內建SSM通訊時，9800端需要適當的憑證。它可以自簽名，但不能無效或過期。在這種情況下，資料包捕獲顯示當9800 HTTP客戶端證書過期時，CSSM傳送的未知CA的TLS警報。

智慧許可使用ip http client配置，它與WLC Web介面使用的ip http server不同。這表示需要正確設定以下命令：

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

信任點名稱可使用show crypto pki trustpoints命令找到。建議使用自簽名證書TP-self-signed-xxxxxxxxxx證書或製造商安裝證書(MIC)，通常稱為CISCO_IDEVID_SUDI，僅適用於9800-80、9800-40和9800-L。

必須注意的是，執行TLS攔截的裝置（例如具有SSL解密功能的防火牆）可能會阻止C9800與思科許可伺服器成功建立握手，因為顯示的HTTPS證書是防火牆證書而不是思科許可伺服器證書。

 注意：請確保同時配置了source-interface和secure-trustpoint命令。即使WLC只有一個L3介面，也需要source-interface命令。

相關資訊

- [9800上具有Air Gap模式的智慧許可](#)
- [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）。