

使用9800上的策略問題排除智慧許可故障

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[許可證使用情況報告](#)

[RUM報告](#)

[解決直連CSSM和SSM本地伺服器上的9800智慧許可通訊問題](#)

[信任代碼](#)

[通過CSSM實現智慧化](#)

[智慧使用代理](#)

[SSM內部](#)

[智慧傳輸](#)

[SSM內部](#)

[測試與智慧接收器的連線](#)

[測試與SSM內部伺服器的連線](#)

[查詢接收方IP地址](#)

[您的系統如何解析IP?](#)

[從CSSM處理的信任代碼無效](#)

[從CSSM處理的有效信任代碼](#)

[通訊頻率](#)

[在show license eventlog和/或show log的輸出中報告錯誤](#)

[偵錯](#)

[相關資訊](#)

簡介

本檔案將介紹Catalyst 9800無線LAN控制器上使用原則(SLUP)的智慧授權進階疑難排解步驟。

必要條件

需求

思科建議您瞭解以下主題：

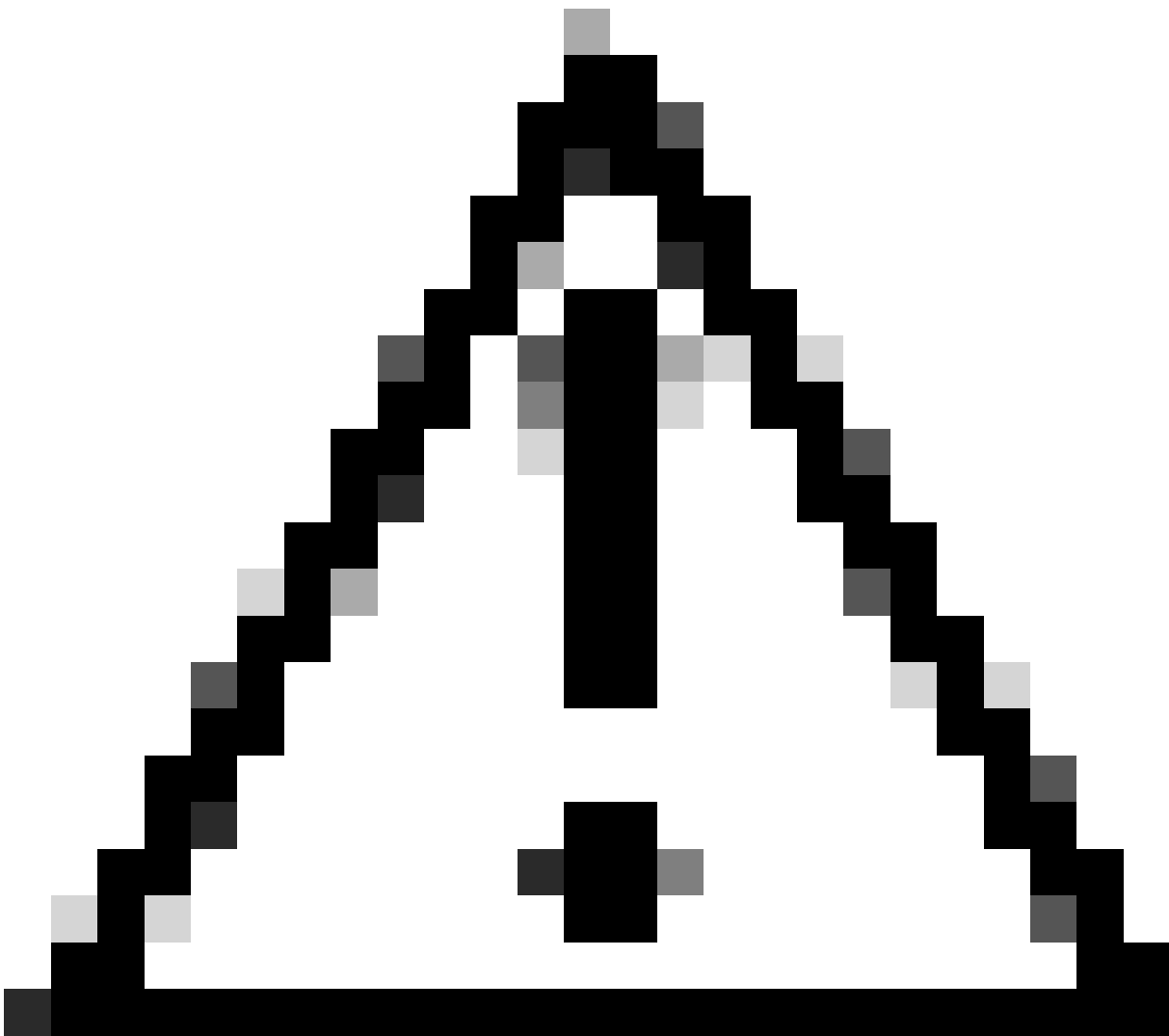
- 使用策略的智慧許可(SLUP)
- Catalyst 9800無線LAN控制器(WLC)

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：注意：本文中的說明包含對文檔中未涵蓋的材料的有用建議或參考。建議您閱讀每個備註。

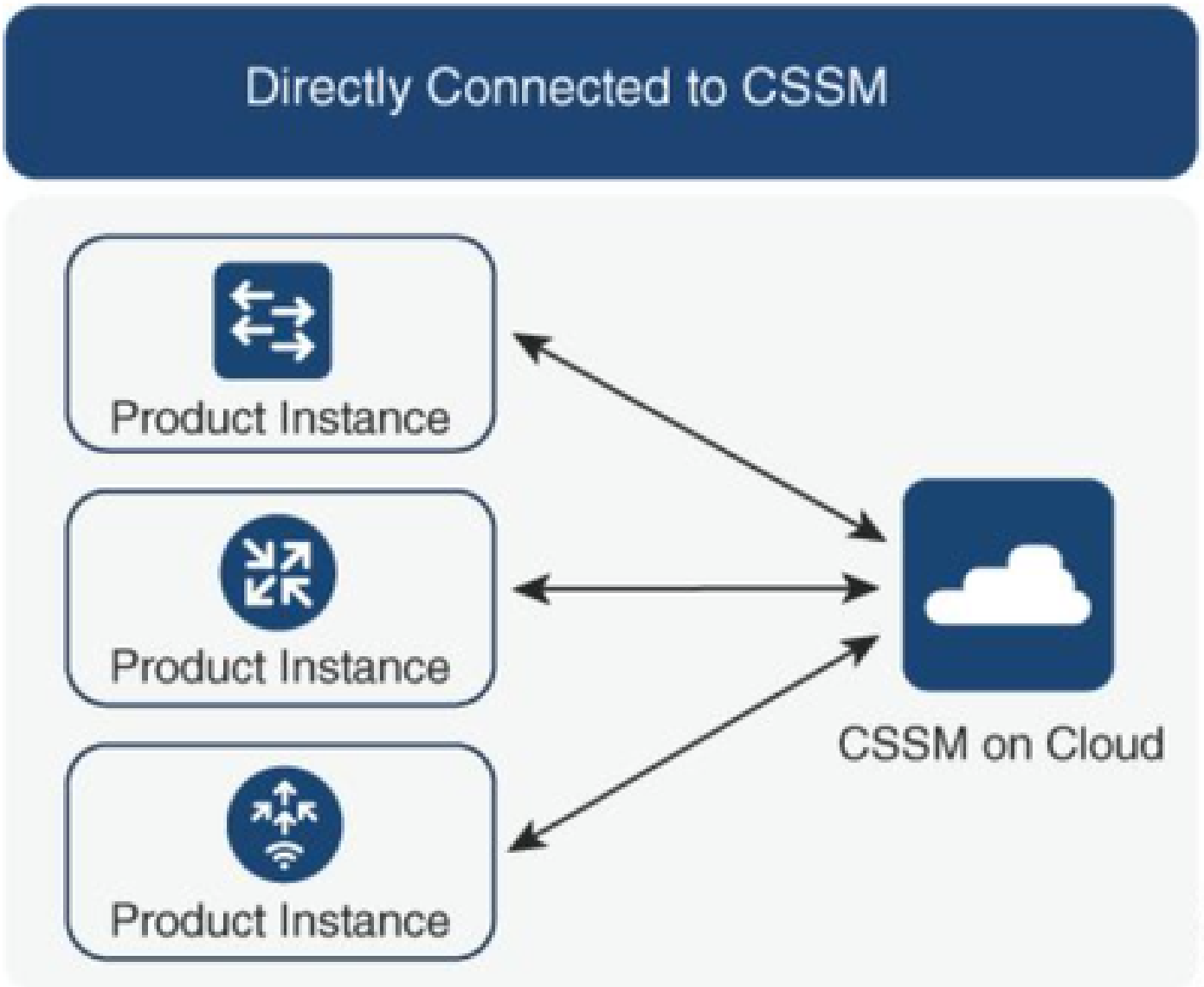
- 使用: Cisco Catalyst無線控制器上的所有許可證均未執行。這表示在開始使用軟體以及與之關聯的許可證之前，不必完成任何特定於許可的操作，如註冊或生成金鑰。許可證使用情況記錄在裝置上並帶有時間戳，所需的工作流程可在以後完成。
- 向CSSM報告許可證使用情況：許可證使用報告有多個選項。您可以使用SSM On-Prem或思科智慧許可實用程式(CSLU)，或者直接向CSSM報告使用資訊。對於氣隙網路，還可以提供離線報告功能，您可以在該功能中下載使用資訊並將其上傳到CSSM。使用情況報告採用純文

字檔案XML格式。

1. 直接連線到思科智慧軟體管理員雲端(CSSM)
2. 通過本地智慧軟體管理器 (本地SSM) 連線到CSSM

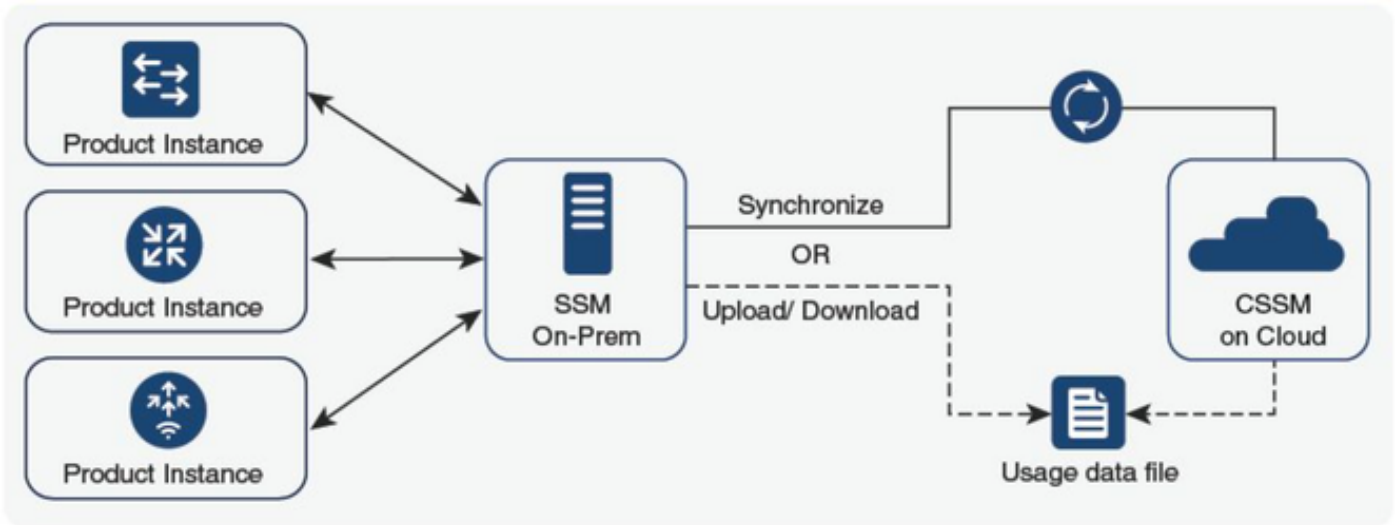
本文未涵蓋Catalyst 9800上的所有智慧許可方案，請參閱[使用策略進行智慧許可的配置指南](#)以瞭解其他資訊。但是，本文確實提供了一系列有用的命令，用於在Catalyst 9800上使用策略問題對直接連線和SSM內部智慧許可進行故障排除。

選項1.直接連線到思科智慧許可雲伺服器(CSSM):



選項2.通過本地智慧軟體管理器 (本地智慧軟體管理器) 連線：

SSM On-Prem Deployment



附註：本文中提到的所有命令僅適用於執行17.3.2版或更高版本的WLC。

許可證使用情況報告

使用SLP時，大多數許可證不會強制實施，並且在配置功能/技術包時在裝置上啟用。相應的許可證將顯示在**show license summary**中，如**IN USE**。

```
9800-1#show license summary Account Information: Smart Account:
```

```
Virtual Account:
```

```
License Usage: License Entitlement Tag Count Status ----- lic_c9800l_perf  
(LIC_C9800L_PERF) 1 IN USE air-network-advantage (DNA_NWStack) 2 IN USE air-dna-advantage (AIR-DNA-A) 2 IN USE
```

許可證僅有的兩種狀態處於使用中或未使用中。狀態完全由產品例項上應用的配置和功能決定。

對於每個正在使用的許可證，會建立一個單獨的RUM報告。Rum報表有CLOSED、ACK和OPEN狀態。

可選：已使用內部命令**test license smart rum-report id**命令確認：

```
Router(config)# service internal
```

```
Router# test license smart rum-report id
```

```
report_id:1624247687 state:SmartAgentRumStateOpen
```

從17.9版本開始：**show license rum id all**指令：

```
Smart Licensing Usage Report: ===== Report Id, State, Flag, Feature Name 1682489268 CLOSED  
P lic_c9800l_perf 1682489269 CLOSED P air-network-advantage 1682489270 CLOSED P air-dna-advantage 1682489271 CLOSED P air-  
network-advantage 1682489272 CLOSED P air-dna-advantage 1682489273 ACK N lic_c9800l_perf
```

RUM報告

RUM報告或資源使用測量報告是包含有關許可證使用和裝置標識資訊的資料檔案。這些報告是儲存在裝置中的安全，並由硬體進行認證。

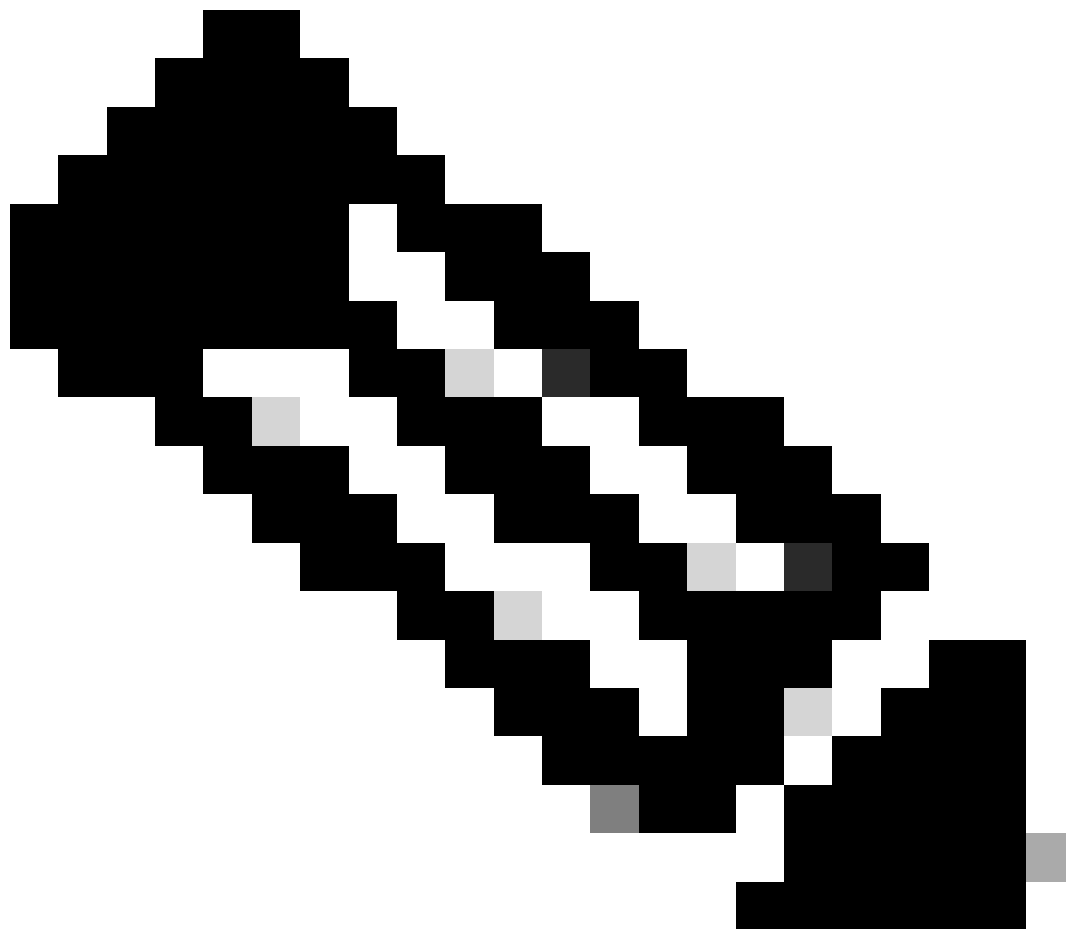
報告在產品例項和CSSM之間的整個通訊過程中更改狀態。

狀態	說明
SmartAgentRumStateOpen	由裝置上的智慧代理建立的新報告
SmartAgentRumStateClosed	傳送到CSSM的RUM報告 (重新載入還會將開啟的報告推送到關閉狀態)
SmartAgentRumStateUnacknowledged	RUM報告等待來自CSSM的確認，已提供輪詢ID

SmartAgentRumStateAcknowledged	RUM報告傳送到CSSM並獲得確認
--------------------------------	-------------------

使用策略的智慧許可功能已引入到Catalyst 9800的代碼版本為17.3.2。初始17.3.2版本遺漏了WLC webUI中隨17.3.3版本引入的SLUP配置選單。SLUP與傳統智慧許可有以下幾個方面的不同：

- WLC現在通過smartreceiver.cisco.com域(而不是tools.cisco.com)與CSSM通訊。
- 現在，WLC不再註冊，而是與CSSM或SSM內部建立信任。
- CLI命令略有改動。
- 智慧許可保留(SLR)不再存在。您可以定期手動報告使用情況。
- 評估模式不再存在。即使沒有許可證，WLC仍繼續以滿容量運行。系統基於榮譽，您應定期報告許可證使用情況（自動或手動報告空隙網路）。

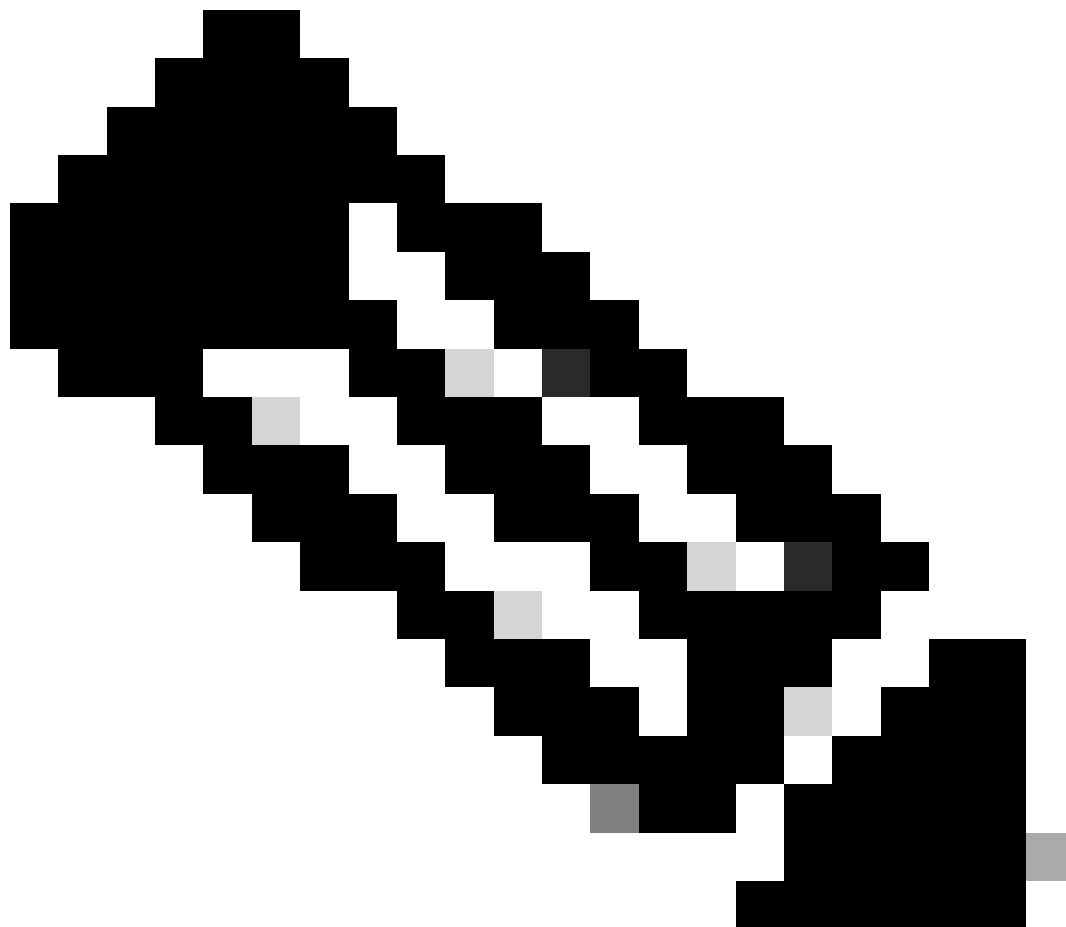


附註：警告：如果您使用的是Cisco Catalyst 9800-CL無線控制器，請確保您熟悉以Cisco IOS® XE Cupertino 17.7.1開始的強制ACK要求。請參閱Cisco Catalyst 9800-CL無線控制器的RUM報告和確認要求。

解決直連CSSM和SSM本地伺服器上的9800智慧許可通訊問題

* 全新9800控制器必須遵循智慧許可工作流程的特定步驟才能完成。

1. 從CSSM門戶建立令牌並匯入該令牌以建立將來獲取許可證使用報告授權所需的信任ID。此信任ID值是CSSM的金鑰，用於驗證從9800控制器提交的報告。作為CSSM的Rum使用情況報告的一部分，此信任令牌將定期刷新並交換。



附註：從Cisco IOS XE Cupertino 17.7.1開始，需要信任代碼。信任代碼按序列號建立，因此9800 HA SSO安裝程式將安裝2個信任代碼。

信任代碼

UDI繫結的公鑰，產品例項用於執行以下操作：

- 簽署RUM報告。這可以防止篡改並確保資料真實性。

- 啟用與CSSM的安全通訊。

從Cisco IOS XE Cupertino 17.7.1中，在產品例項發起向CSLU傳送資料的拓撲和產品例項位於空隙網路中的拓撲中，自動獲取信任代碼。

- 可以使用ID令牌從CSSM獲取信任代碼。

在此，您可以在CSSM Web UI中生成ID令牌以獲取信任代碼，並將其安裝在產品例項上。如果存在出廠安裝的信任代碼，則必須覆蓋它。如果產品例項直接連線到CSSM，請使用此方法使產品例項能夠與CSSM以安全方式通訊。這種獲得信任代碼的方法適用於直接連線到CSSM的所有選項。有關詳細資訊，請參閱[直接連線到CSSM](#)。

從Cisco IOS XE Cupertino 17.9.1中，在CSLU啟動從產品例項檢索資料的拓撲中自動獲取信任代碼。

如果存在出廠安裝的信任代碼，則會自動覆蓋該代碼。通過這種方式獲得的信任代碼可用於與CSSM的安全通訊。

*確保9800上的智慧許可配置完好無損。9800使用Smart as transport與CSSM通訊。

通過CSSM實現智慧化

Device(config)#license smart transport smart Device(config)#license smart url <https://smartreceiver.cisco.com/licservice/license>

智慧使用代理

license smart proxy { address address_hostname| port port_num} Device(config)#license smart url default Device(config)#license smart proxy address

Device(config)#license smart proxy port

SSM內部

Device(config)#license smart transport cslu Device(config)#license smart url cslu <https://SSM-Onprem-FODN-address>/cslu/v1/pi/ssmsfloodingslup2304-1>

確保可通過源介面訪問域查詢和名稱伺服器。

Device(config)#ip domain name

Device(config)#ip name server

Device(config)#ip domain lookup

show license all命令返回在9800上配置的傳輸型別和URL詳細資訊：確保配置是絕對的。

智慧傳輸

Type: Smart URL: <https://smartreceiver.cisco.com/licservice/license> Proxy: Not Configured VRF:

SSM內部

Transport: Type: cslu Cslu address: <https://SSM-Onprem-FQDN-address>cslu/v1/pi/ssmsfloodingslup2304-1>

*如果9800和CSSM之間存在任何Proxy，請確保允許在Proxy上列出的IP地址以實現無縫通訊。

測試與智慧接收器的連線

使用curl命令：

- curl <https://smartreceiver.cisco.com/licservice/license>
- 預期響應：這是智慧接收器！

測試與SSM內部伺服器的連線

使用curl命令：

- curl -v -k <https://SSM-Onprem-FQDN-address>cslu/v1/pi/ssmsfloodingslup2304-1>
- 預期響應：這是智慧接收器！

查詢接收方IP地址

使用此nslookup命令：

- nslookup smartreceiver.cisco.com

預期響應：

- 伺服器: 171.70.168.183 ←這是DNS伺服器
- 伺服器: dns-sj.cisco.com ← (可選) 可以顯示
- 地址 : 10.10.10.10#53
- 姓名 : smartreceiver.cisco.com
- 地址 : 146.112.59.81
- 姓名 : smartreceiver.cisco.com
- 地址 : 2a04:e4c7:ffe::f

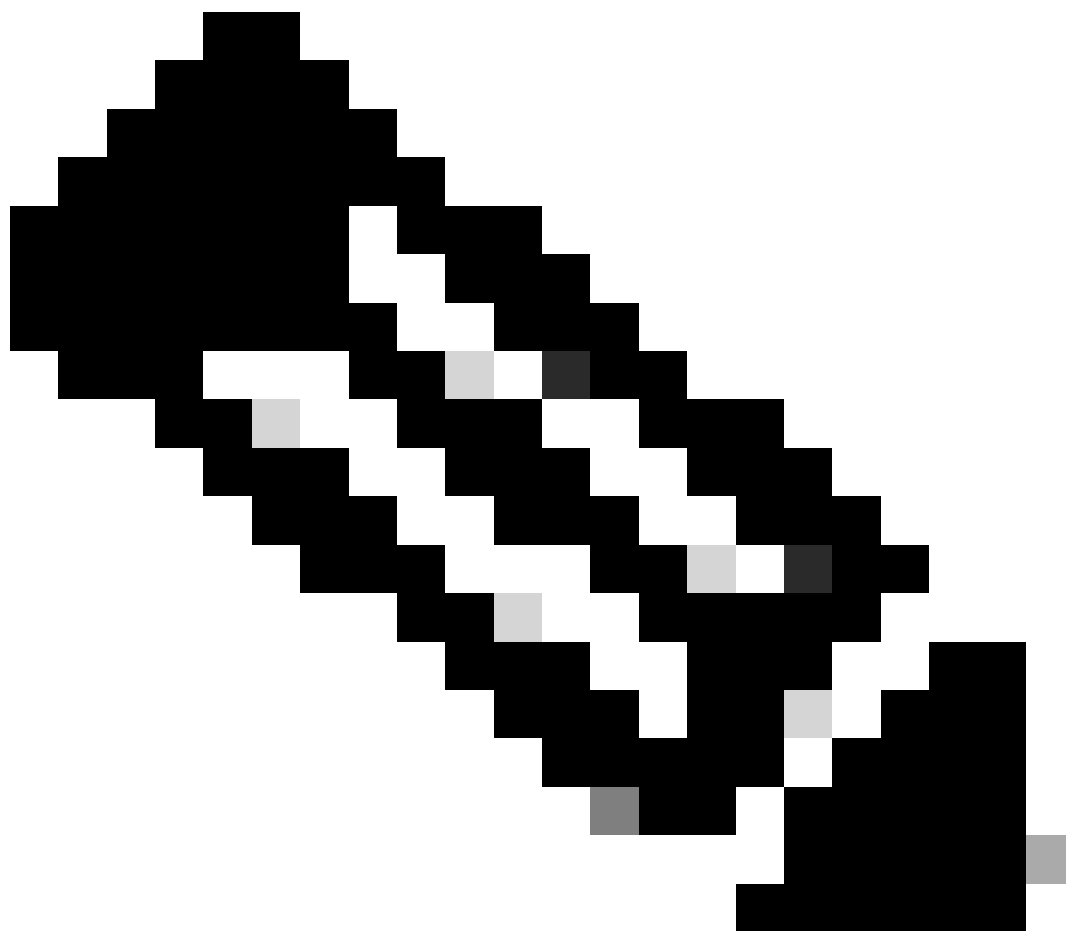
您的系統如何解析IP?

使用dig命令：

- 挖掘smartreceiver.cisco.com +短

預期結果

- 146.112.59.81
-



附註：CSSM的智慧接收器元件取代了舊的tools.cisco.com和MSLA客戶的Rum報告、註冊和計費的單一聯絡點。

ip http client source-interface <source-interface>

此命令顯式標籤CSSM的源路徑。

ip http client secure-trustpoint SLA-TrustPoint

確保將secure-trustpoint選為SLA-TrustPoint，因為此名稱由授權根CA簽署。SSM On-Prem和CSSM都受授權根CA證書的信任。

CA證書：

狀態：可使用：

證書序列號（十六進位制）：01

證書使用：簽名

頒發者：

cn=Cisco授權根CA

o=思科

主題：

cn=Cisco授權根CA

o=思科

有效日期：

開始日期：世界協調時2013年5月30日19時48分47秒

結束日期：世界協調時2038年5月30日19時48分47秒

關聯的信任點：Trustpool SLA-TrustPoint

儲存：nvram:CiscoLicensi#1CA.cer

License smart sync all是從9800控制器和XML格式啟動新Rum報告的命令。在控制器上發出此命令時，如果控制器未在17.9.x版上安裝信任代碼，則它會首先生成對信任代碼而不是對Rum使用情況報告的請求。

從CSSM處理的信任代碼無效

匯入信任代碼：

世界協調時2024年9月17日17時35分26秒收到

```
<smartLicenseTrust><trustCode><udi>P:C9800-L-F-K9,S:FCL2630000P</udi><status><success>>false</success><message>已為此裝置處理了對應於更高信任ID的信任請求。</message><code>OLD_TRUST_ID</code><correlationID>null-null</correlationID></status></trustCode><signature>MEQCIAg71/hlcWxUiof8VstpmPhRH8jptPZPrvaSpsuwVgLAiAQ3IUVMuS8bOHwySOB/j/3RmG4uSDq/EbUp+vfrYD9nQ=
```

CSSM期望控制器傳送增量信任代碼ID作為安全目的，而無效信任代碼將阻止CSSM處理來自控制器的授權RUM請求。這最終會導致CSSM許可的許可證管理問題dashabord。

從CSSM處理的有效信任代碼

匯入信任代碼：

```
<smartLicenseTrust><trustCode><udi>P:C9800-L-F-
K9,S:XXXXXXXXXX</udi><customerInfo><smartAccount>Cisco Demo內部智慧帳戶
</smartAccount><virtualAccount>0Demo-HK-
PartnerA</virtualAccount></customerInfo><piid>0eb1d627-bbed-46a8-9a4b-fc5b48a7c
6b</piid><dateStamp>2024-09-
10T07:21:30</dateStamp></subCA><trustId>110</trustId><status><success>>true</success><correlation
null</correlationID></status></trustCode><signature>MEUCIGMPyt6VEmv/DMZiYBLDnsHRZAxfI9r
l3BBNtrdpBtAiEAojAqDYkGn206meTHt8+dqra0LAcIHEZKxmqueurKOU0g=</signature></smartLicenseTr
```

通訊頻率

您可以在CLI或GUI中配置的報告間隔無效。

9800 WLC每8小時與CSSM或本地智慧軟體管理器通訊，而不管通過Web介面或CLI配置了什麼報告間隔。這意味著新加入的接入點可以在初次加入後8小時內出現在CSSM上。

您可以使用show license air entities summary命令確定下次計算並報告許可證的時間。此命令不是典型的show tech或show license all輸出的一部分：

show license air entities summary命令：

```
Last license report time.....: 10:00:07.753 UTC Mon Sep 16 2024 Upcoming license report time.....: 18:00:07.808 UTC
Mon Sep 16 2024 No. of APs active at last report.....: 3 No. of APs newly added with last report.....: 1 No. of APs deleted with last
report.....: 0
```

在9800控制器上成功安裝信任碼後，下一階段將通過XML格式的Rum（資源度量單位）生成許可證活動的使用報告。License smart sync all/local命令將基於控制器中管理的AP啟動或生成或開啟新的Rum度量。基本上，9800智慧代理元件向許可模組傳送API呼叫，以收集包含許可資訊的新Rum報告。

show license rum id all 指令：

```
This command would list CLOSED, ACK and OPEN state of Rum report on the controller. 1719005447 OPEN N air-network-advantage
1719005448 OPEN N air-dna-advantage
```

show license rum id 1719005447 detail 指令：

您可以獲取在Rum id中報告的許可證的詳細資訊。此命令將提取software_identifier_tag，它是CSSM資料庫上的金鑰匹配元素，用於從產品例項驗證許可證型別。

regid.2018-06.com.cisco.DNA_NWStack , 1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896

智慧許可使用情況報告詳細資訊：

=====

報告Id:1719005447

度量名稱：權利

功能名稱：空中網路優勢

指標值：regid.2018-06.com.cisco.DNA_NWStack , 1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896

UDI:PID:C9800-L-F-K9,SN:FCL2630000P

上一個報告Id:1719005445 , 下一個報告Id:0

狀態:OPEN , 狀態更改原因：無

關閉原因：無

開始時間：9月10日10:00:08 2024 UTC , 結束時間：世界協調時2024年9月16日16時15分8秒

儲存狀態：存在

事務ID:0

交易消息：<無>

*現在，生成Rum報告。在OPEN狀態下，必須將其成功提交到CSSM才能從CSSM接收ACK。

A) Verify which licenses are activated/in use - show version - show license summary - show license usage <<< it would also indicate which licenses are Perpetual vs Subscription C) Verify if enforced/export controlled license is authorized: - show license authorization D) Verify what messages were sent to/received from SSM On-Prem/CSSM - show license history message E) Check for errors - show license eventlog F) Collect detailed information/counters: - show license tech support G) Collect license tech support file - show tech-support license

在show license eventlog和/或show log的輸出中報告錯誤

「使用思科智慧許可證實用程式(CSLU)通訊失敗：未提供詳細資訊」

當未建立與內部的HTTPS通訊時，可能會發生此錯誤。潛在原因：

- 特定VRF用於與OnPrem通訊。必須手動配置HTTP客戶端源介面
- 在SLA-Trustpoint配置下未禁用吊銷檢查
- 另一個信任點被設定為加密信令的預設值(例如：在SIP網關上)

"HTTP伺服器錯誤502:錯誤的網關"

On-Prem開發團隊目前正在調查此錯誤。在多數情況下，未觀察到服務影響。

通常，10秒後，SAEVT_COMM_RESTORED。

範例：

7月9日 13:15:29.902:%SMART_LIC-3-COMM_FAILED：使用思科智慧許可證實用程式(CSLU)通訊失敗：HTTP伺服器錯誤502:錯誤的網關

7月9日 13:15:39.881:%SMART_LIC-5-COMM_RESTORED:已恢復與思科智慧許可證實用程式(CSLU)的通訊

"HTTP伺服器錯誤404:未找到"

當傳輸URL指向內部模式(CSLU)時，嘗試安裝信任代碼時，在Cisco IOS XE裝置上觀察到此錯誤。

僅當裝置直接與CSSM通訊時，才使用命令「license smart trust idtoken <token> [all|local]」。

附註：根據平台的不同，此消息也可能表示在On-Prem Admin Workspace的CSLU設定面板中啟用了「驗證裝置」設定。檢查您嘗試註冊的裝置是否位於本地伺服器的「SL Using Policy」頁籤中。如果裝置不在該頁籤中，則需要關閉此開關。然後再次嘗試讓裝置與On-Prem伺服器同步。有關此設定的圖片，請參閱本文的結尾。

SAEVT_INIT_CRYPTO success="False" error="加密初始化尚未完成"

系統啟動後不久即可觀察到此錯誤。約30秒後完成加密初始化 — 在這種情況下，沒有服務影響。

範例：

2021-06-25 10:09:23.378 UTC SAVET_INIT_SYSTEM_INIT

2021-06-25 10:09:24.383 UTC SAEVT_INIT_CRYPTO success="False" error="加密初始化未完成"

2021-06-25 10:09:54.383 UTC SAEVT_INIT_CRYPTO success="True"

如果加密初始化沒有完成幾分鐘/小時，請驗證NTP配置是否存在，和/或時鐘是否同步。儲存運行配置有助於重新啟動加密初始化。

如果問題仍然存在，建議與Cisco TAC進一步調查。

SAVE_UTILITY_RUM_FAIL error="[HOST_NOT_FOUND] Device Host is not found"

「驗證裝置」設定很可能是在本地管理工作區的CSLU設定面板中設定的。

此設定幫助確保接收來自己知產品例項的RUM報告。

SAEVT_COMM_FAIL error="無法解析伺服器主機名/域名"

此錯誤表示可能由DNS解析引起的連線問題。必須確保裝置可以解析目標URL。通常ip host <url>

<ipassociated>命令配置錯誤。請檢查這一點。

你最有可能發現通訊失敗

通訊統計資訊：

=====

允許的通訊級別：間接

總體狀態：<空>

信任建立：

嘗試次數：Total=30, Success=0, Fail=30持續故障：總體=30通訊=30 <<<<<<<<

上次響應：2月12日10:52:56 2023 GMT <<<<<<<<

失敗原因：<無>

上次成功時間：<無>

上次失敗時間：2月12日10:52:56 2023格林尼治標準時

Communication Level Allowed as INDIRECT表示在9800控制器上未成功安裝所需的信任碼。



附註：附註：CSSM是所有許可資料的真實來源。

*如果通過執行測試緩解了9800和CSSM之間的基本通訊問題，請在智慧許可通訊涉及的某些模組上啟用調試。在9800上啟用調試將使CPU在某個時間間隔內突增，因此必須在非工作時間執行這些操作。

偵錯

*從9800到CSSM或SSM On-Prem的智慧許可通訊涉及4個模組

1.加密模組

PKI:

Crypto PKI Msg debugging is on Crypto PKI Trans debugging is on Crypto PKI callbacks debugging is on Crypto PKI Validation Path debugging is on

2. Http模組

HTTP伺服器：

HTTP Server transaction debugging is on HTTP Server tokens debugging is on HTTP Server EZSetup debugging is on HTTP Server URL debugging is on HTTP Server Authentication debugging is on HTTP Server Side Includes debugging is on HTTP Application Inout debugging is on HTTP Application Detail debugging is on HTTP Server Error debugging is on HTTP SSL Error debugging is on HTTP CTC trace debug debugging is on HTTP CTC error debug debugging is on HTTP SESSION debugging is on HTTP TPS Trace debugging is on HTTP TPS Error debugging is on HTTP WSMAN debugging is on

3. Openssl模組

ssl openssl:

TLS state debugging is on TLS msg debugging is on TLS errors debugging is on

4.智慧許可模組稱為智慧代理，包括傳輸網關

授權：

License IPC communication debugging is on License Events debugging is on License warnings and errors debugging is on

系統日誌：

證書上的伺服器身份檢查和SAN驗證。來自加密SSL庫的信任點驗證。

2016年9月16日16:29:12.236:對主機進行伺服器身份檢查：10.106.43.37

2016年9月16日16:29:12.236:要驗證的伺服器身份是ip address 10.106.43.37 len 12

2016年9月16日16:29:12.329:CRYPTO_PKI:(A645F)檢查相同的證書

2016年9月16日16:29:12.329:CRYPTO_PKI (證書查詢) issuer="cn=Cisco Licensing Root CA , o=Cisco" serial number= 0F 42 40

2016年9月16日16:29:12.329:CRYPTO_PKI:(A645F)合適的信任點包括：SLA-TrustPoint、Trustpool6、Trustpool6、

2016年9月16日16:29:12.329:CRYPTO_PKI:(A645F)嘗試使用SLA-TrustPoint策略驗證證書

2016年9月16日16:29:12.329:CRYPTO_PKI:(A645F)使用SLA-TrustPoint驗證證書

2016年9月16日16:29:12.345:SSL_connect:SSL協商已成功完成

2016年9月16日16:29:12.345:SSL_connect:SSL協商已成功完成

將使用情況報告提交到CSSM後，您必須看到在show license history message命令上成功更新：

請求將具有UDI_SERIAL_NUMBER、hostname、software_tag_identifier等元件，這些元件指示9800控制器使用的許可證模式，並且request_type為"LICENSE_USAGE"

存在多種許可證型別：

1.—D_TOKEN_TRUST

2. TRUST_SYNC

3. LICENSE_USAGE

使用情況報告：

請求：世界協調時2024年9月16日16時30分16秒

```
{\"sender_info\":{\"connect_info\":{\"名稱\":\"C_agent\",\"版本\":\"5.8.6_rel/15\",\"生產\":true,\"additional_info\":{\"功能\":[\"實用程式\",\"DLC\",\"AppHA\",\"多層\",\"EXPORT_2\",\"OK_TRY_USAGE\",\"POLICY_USAGE\",\"TELEMETRY\",\"CSLU_V1\"]},\"timestamp\":1726504244391,\"nonce\":\"13980553869667320622\"},\"udi_serial_number\":\"FCL2630000P\",\"product_instance_identifier\":\"06.com.cisco.C980000_L_F_K9,1.0_9529f872-1b08-4cac-9279-71c391233fc2\",\"device_list\":{\"sudi\":{\"udi_pid\":\"C9800-L-F-K9\",\"udi_serial_number\":\"FCL2630000P\"},\"software_tag_identifier\":\"regid.2019-06.com.ciC9800_L_F_K9,1.0_9529f872-1b08-4cac-9279-71c391233fc2\",\"product_instance_identifier\":\"\",\"product_version\":\"17.12.02\",\"hostname\":\"renjith-eap-test\",\"角色\":\"活動\",\"請求型別\":\"ID_TOKEN_TRUST\",\"請求行id\":1,\"智慧許可證\":
```

使用情況報告：

請求：世界協調時2024年9月16日16時30分16秒

```
{\"sender_info\":{\"connect_info\":{\"名稱\":\"C_agent\",\"版本\":\"5.8.6_rel/15\",\"生產\":true,\"additional_info\":{\"功能\":[\"實用程式\",\"DLC\",\"AppHA\",\"多層\",\"EXPORT_2\",\"OK_TRY_USAGE\",\"POLICY_USAGE\",\"TELEMETRY\",\"CSLU_V1\"]},\"timestamp\":1726504153254,\"nonce\":\"10743401694998030696\"},\"udi_serial_number\":\"FCL2630000P\",\"product_instance_identifier\":\"06.com.cisco.C980000_L_F_K9,1.0_9529f872-1b08-4cac-9279-71c391233fc2\",\"device_list\":{\"sudi\":{\"udi_pid\":\"C9800-L-F-K9\",\"udi_serial_number\":\"FCL2630000P\"},\"software_tag_identifier\":\"regid.2019-06.com.ciC9800_L_F_K9,1.0_9529f872-1b08-4cac-9279-71c391233fc2\",\"product_instance_identifier\":\"\",\"product_version\":\"17.12.02\",\"hostname\":\"renjith-eap-test\",\"role\":\"活動\"請求型別\":\"TRUST_SYNC\",\"request_line_id\": \"智慧許可證\":
```

使用情況報告：

請求：世界協調時2024年9月16日16時30分16秒

```
{
  "sender_info": {
    "connect_info": {
      "name": "C_agent",
      "version": "5.8.6_rel/15",
      "production": true,
      "additional_info": {
        "77709655117429624",
        "nonce": "nonce",
        "sudi": {
          "udi_pid": "C9800-L-F-K9",
          "udi_serial_number": "FCL2630000P"
        },
        "product_instance_identifier": "",
        "software_tag_identifier": "regid.2019-06.com.cisco.C9800_L_F_K9,1.0_9529f872-1b08-4cac-9279-71c391233fc2"
      },
        "device_list": {
          "sudi": {
            "udi_pid": "C9800-L-F-K9",
            "udi_serial_number": "FCL2630000P"
          },
          "software_tag_identifier": "regid.2019-06.com.cisco.C9800_L_F_K9,1.0_9529f872-1b08-4cac-9279-71c391233fc2",
          "product_instance_identifier": "",
          "product_version": "1.12.02",
          "hostname": "renjith-eap-test",
          "role": "Active",
          "request_type": "LICENSE_USAGE",
          "request_line_id": 1,
          "smart_license":

```

*瞭解來自CSSM或SSM內部版本的響應非常重要：

錯誤響應資料包：

回應：世界協調時2024年9月16日16時30分16秒

```
{
  "狀態": "失敗",
  "message_code": "使用許可證時出錯",
  "消息": "",
  "nonce": "77709655117429624"
}
```

此錯誤表示在CSSM或SSM本地許可伺服器中已存在拒絕在資料庫中新增新記錄的控制器條目。必須從CSSM或SSM內部版本中刪除活動或陳舊記錄，然後重新提交Rum報告。

有效響應Poll_id：

回應：世界協調時2024年9月16日16時29分14秒

```
{
  "sender_info": {
    "connect_info": {
      "名稱": "CSLU_V1",
      "版本": "v1",
      "生產": "沒錯",
      "additional_info": "",
      "功能": [

```

```
"實用程式",
"DLC",
"AppHA",
"多層",
"EXPORT_2",
"OK_TRY_AGAIN",
"POLICY_USAGE",
"CSLU_V1",
"CSLU_V2",
"遙測"
]
},
"時間戳":1726504153302,
"nonce":"10743401694998030696",
"sudi":{
  "udi_pid":"C9800-L-F-K9",
  "udi_serial_number":"FCL2630000P"
},
"product_instance_identifier":"","
"software_tag_identifier":"regid.2019-06.com.cisco.C9800_L_F_K9,1.0_9529f872-1b08-4cac-9279-71c391233fc2"
},
"狀態":"完成",
"license_data":[
{
  "狀態":"OK_POLL",
  "request_line_id":1,
```

```
"sudi":{
  "udi_pid":"C9800-L-F-K9",
  "udi_serial_number":"FCL2630000P"
},
"poll_id":5583279046281676962,
"poll_interval":86739,
"smart_license":""
}
]
}
```

*如何驗證poll_id儲存在9800本地資料庫中，以及為了獲得提交的Rum報告的ACK而進行輪詢的頻率。

測試命令，以驗證是否需要通過內部服務啟用。

```
conf t service internal exit test license smart conversion list-poll-info Poll Request Information: PollID | Type | Delta | Poll Time
5583279046281676962 | TRUST_SYNC | 86673 | Sep 17 17:33:05 2024 UTC
```

*從說明中可以理解，9800控制器提交的初始請求將始終是信任代碼令牌，如果沒有它，9800控制器將永遠不會生成新的Rum使用情況報告，因此許可證使用情況更改無法在CSSM上提交。

* License_usage的poll_id請求示例。

```
test license smart conversion list-poll-info Poll Request Information: PollID | Type | Delta | Poll Time 5583279046281677674 |
LICENSE_USAGE | 87656 | Sep 17 17:33:05 2024 UTC
```

*如果在CSSM或SSM On-Prem資料庫中已處理ACK，則可以強制在9800控制器上執行智慧代理輪詢並儘早獲取ACK，而無需等待上述時間

在poll_id循環中。

```
test license smart conversion sched_poll 5583279046281676962 ? <0-4294967295> delta Time in Seconds
```

相關資訊

- [在9800 WLC上設定離線\(Air Gapped\)授權](#)
- [思科技術支援與下載](#)
- [使用DNA Center策略配置Catalyst 9800 WLC智慧許可](#)

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）。