

配置 & 对带有SLUP的Catalyst 9800智能许可进行故障排除

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[传统许可与SLUP](#)

[配置](#)

[直接连接CSSM](#)

[已连接到CSLU](#)

[产品实例启动的](#)

[CSLU启动的](#)

[已连接到内部部署SSM](#)

[配置通过HTTPS代理的智能传输](#)

[通信频率](#)

[许可证出厂重置](#)

[在RMA或硬件更换的情况下](#)

[从特定许可证注册\(SLR\)升级](#)

[故障排除](#)

[互联网接入、端口检查和Ping](#)

[系统日志](#)

[数据包捕获](#)

[显示命令](#)

[调试/btrace](#)

[常见问题](#)

[WLC没有互联网接入或防火墙阻止/更改流量](#)

[数据包捕获中的未知CA警报](#)

[相关信息](#)

简介

本文档介绍如何在Catalyst 9800无线LAN控制器(WLC)上使用策略(SLUP)配置和排除智能许可故障。

先决条件

要求

Cisco 建议您了解以下主题：

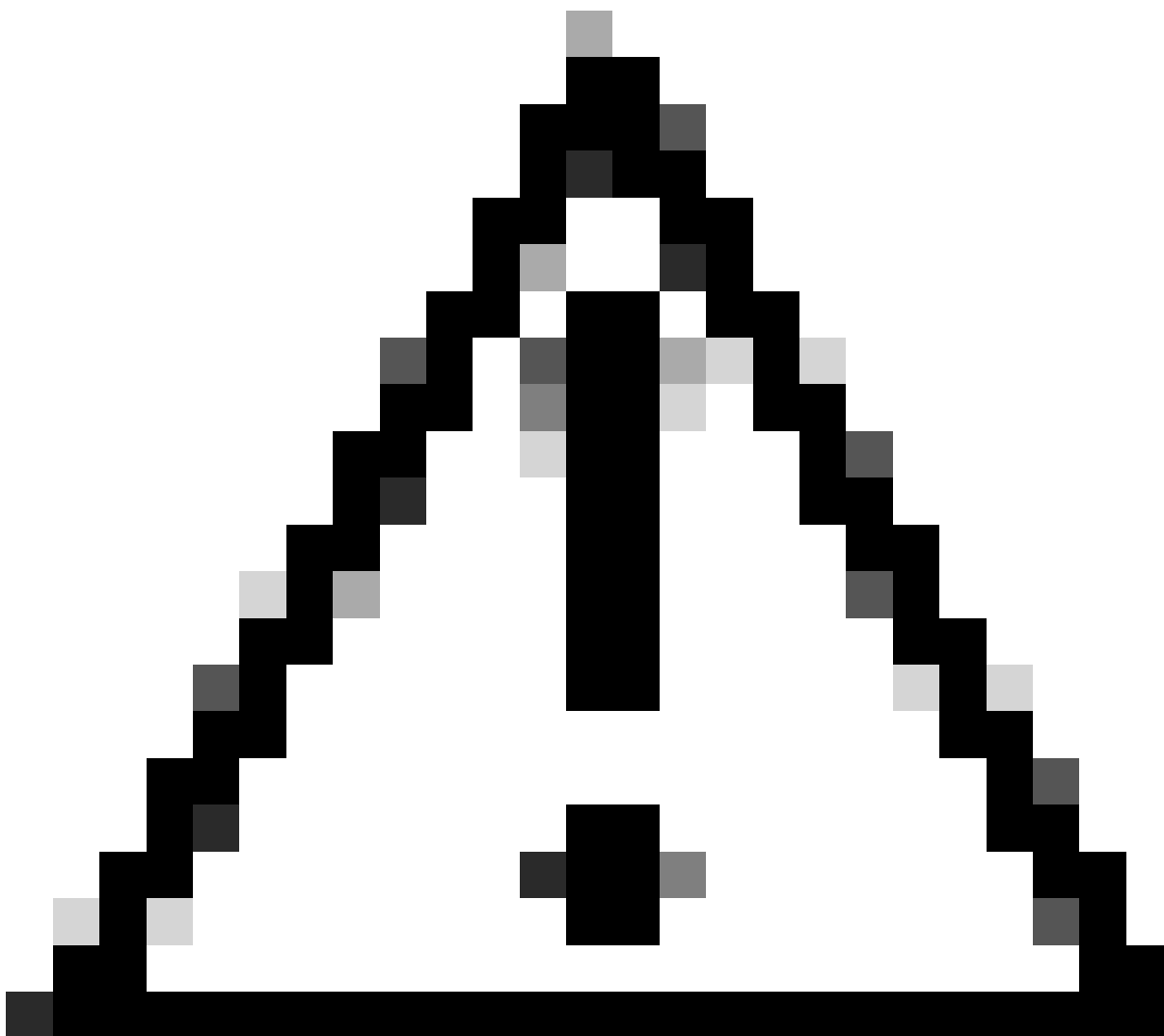
- 使用策略的智能许可(SLUP)
- Catalyst 9800无线LAN控制器(WLC)

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

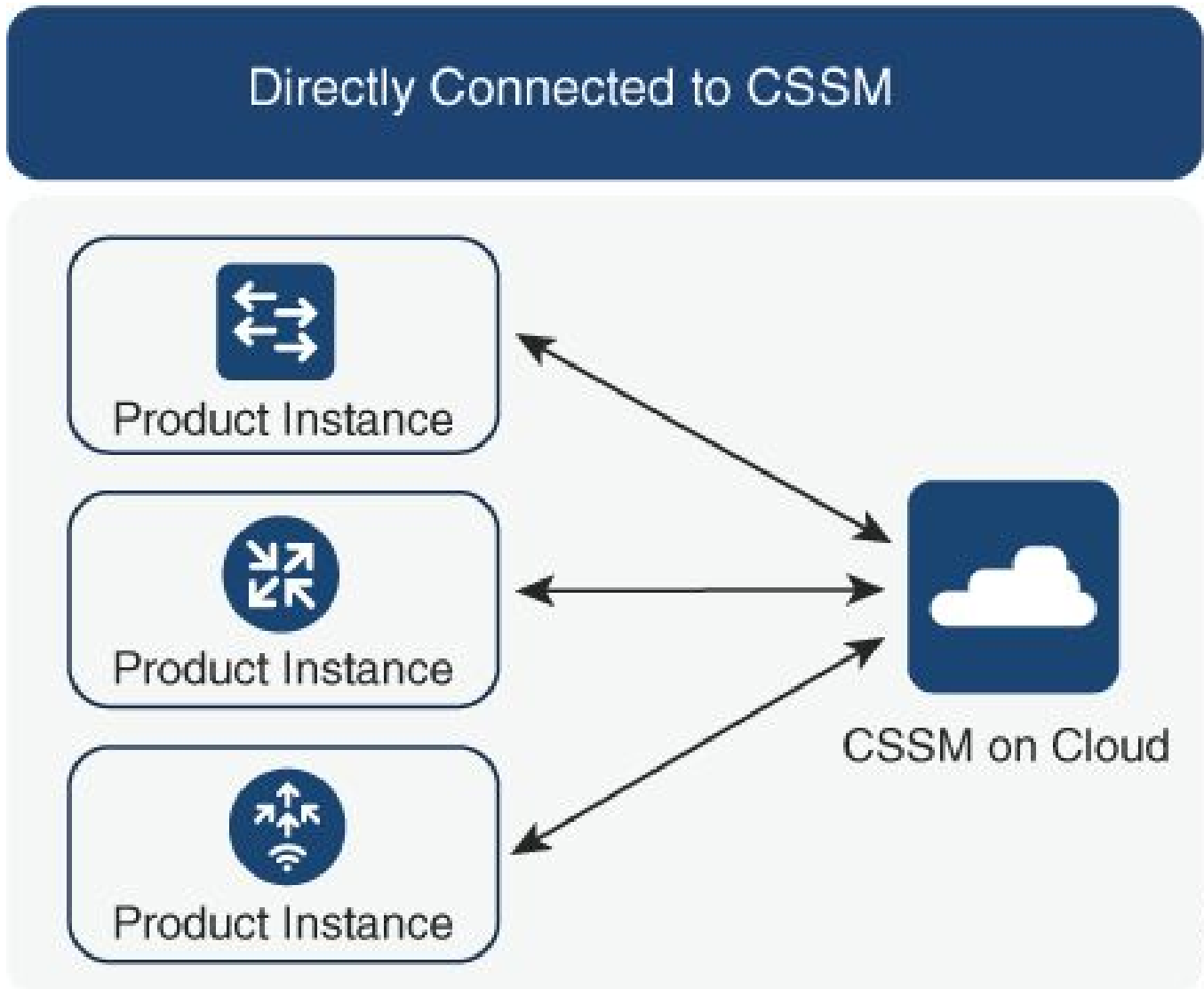
背景信息



注意：本文中的说明包含有用的建议或本文档未涵盖的材料的引用。建议您阅读每个备注。

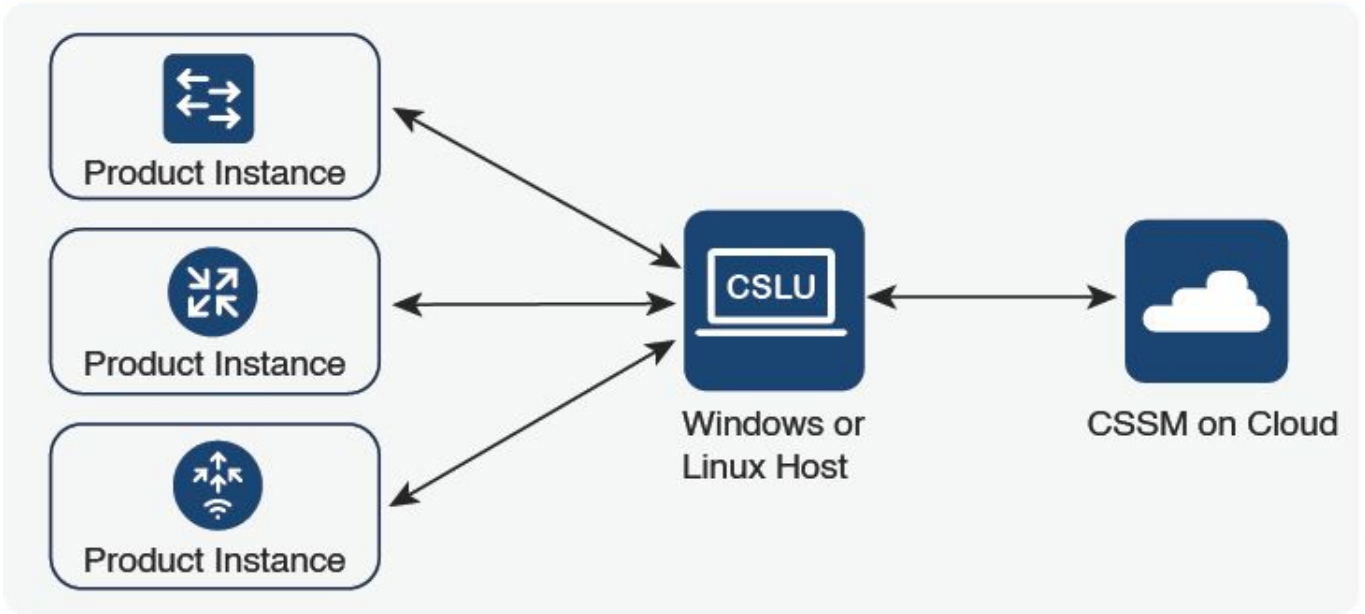
1. 直接连接到[思科智能软件管理器云](#) (CSSM云)
2. 通过[CSLU](#)(思科智能许可证实用程序管理器)连接到CSSM
3. 已通过[内部智能软件管理器](#) (内部SSM) 连接到CSSM

本文未涵盖Catalyst 9800上的所有智能许可方案，有关详细信息，请参阅[使用策略进行智能许可的配置指南](#)。但是，本文确实提供了一系列有用的命令，用于解决Catalyst 9800上使用策略问题的直接连接、CSLU和本地SSM智能许可问题。



第 1 项.直接连接到思科智能许可云服务器(CSSM)

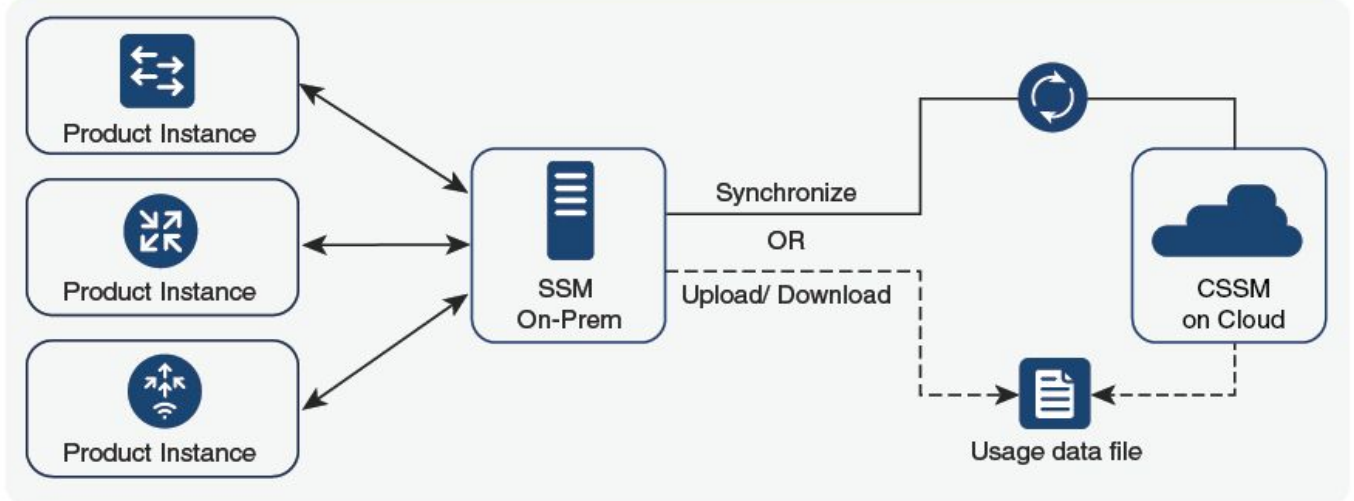
Connected to CSSM Through CSLU



356791


第 2 项.通过CSLU连接

SSM On-Prem Deployment



357508

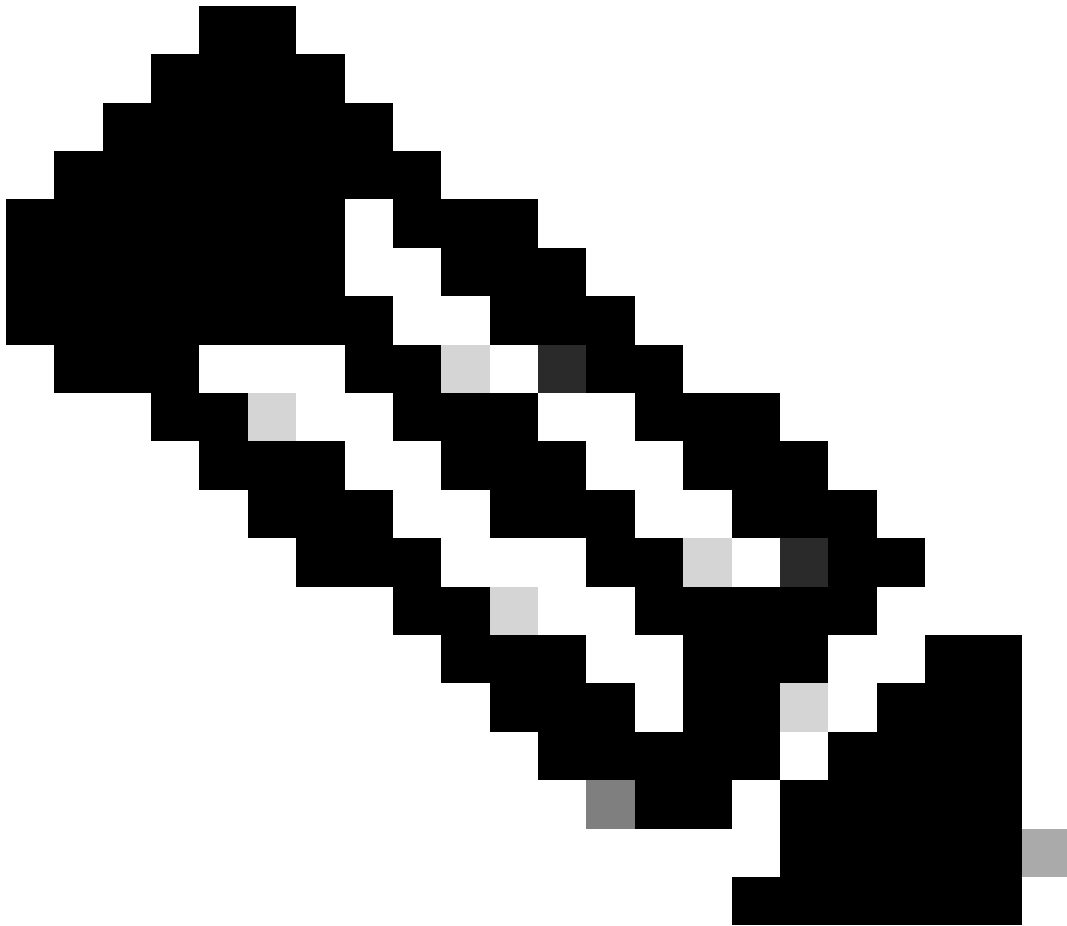
选项 3.通过本地智能软件管理器 (本地SSM) 连接

 注意：本文中提到的所有命令仅适用于运行版本17.3.2或更高版本的WLC。

传统许可与SLUP

Catalyst 9800中引入了使用策略的智能许可功能，代码版本为17.3.2。最初的17.3.2版本遗漏了WLC webUI中的SLUP配置菜单，该菜单是随17.3.3版本引入的。SLUP在以下几个方面不同于传统的智能许可：

- WLC现在通过smartreceiver.cisco.com域(而不是tools.cisco.com域)与CSSM通信。
 - 现在，WLC不再进行注册，而是与CSSM或本地SSM建立信任。
 - CLI命令已稍作修改。
 - 不再有智能许可预留(SLR)。您可以定期手动报告使用情况。
 - 不再有评估模式。即使没有许可证，WLC仍可继续以满容量运行。系统基于荣誉，您应定期（自动或手动）报告许可证使用情况（在存在空运网络的情况下）。
-




警告：如果您使用的是Cisco Catalyst 9800-CL无线控制器，请确保您熟悉以Cisco IOS® XE Cupertino 17.7.1开头的强制ACK要求。请参阅[Cisco Catalyst 9800-CL无线控制器的RUM报告和确认要求](#)。

配置


直接连接CSSM

在CSSM上创建令牌后，为了建立信任，需要执行以下命令：

 注意：最大令牌数在HA SSO中的WLC情况下，使用计数必须至少为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命令指定许可相关数据包将从中进行源的L3接口
- ip http client secure-trustpoint命令指定哪个信任点/证书用于CSSM通信。使用show crypto pki trustpoints命令可以找到信任点名称。建议使用自签名证书TP-self-signed-xxxxxxxxxxx证书或制造商安装证书（也称为MIC，仅在9800-40、9800-80和9800-L上提供），通常称为CISCO_IDVID_SUDI。
- Terminal monitor命令使WLC将日志打印到控制台并帮助确认已成功建立信任。可以使用terminal no monitor禁用。
- 最后一个命令中的关键字all告知HA SSO集群中的所有WLC建立与CSSM的信任。
- 关键字force指示WLC覆盖任何以前建立的信任并尝试建立新信任。

 注意：如果未建立信任，则9800会在执行命令1分钟后重试，并且在一段时间内不重试。再次输入token命令以强制建立新的信任。

已连接到CSLU

Cisco Smart License Utility Manager (CSLU)是基于Windows的应用程序（也适用于Linux），使客户能够从其本地管理许可证及其相关产品实例，而不必将其支持智能许可的产品实例直接连接到思科智能软件管理器(CSSM)。

本部分仅介绍9800无线配置。还有其他步骤可用来配置使用CSLU的许可（例如安装CSLU、配置CSLU软件等），具体步骤将在[配置指南](#)中介绍。是实施产品实例启动的通信方法还是CSLU启动的通信方法，还是完成相应的任务序列。

产品实例启动的

1. 确保从控制器到CSLU的网络可达性
2. 确保传输类型设置为cslu：

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

3. 如果希望控制器发现CSLU，您需要执行操作。如果您希望使用DNS发现CSLU，则无需执行

任何操作。如果要使用URL发现它，请输入以下命令：

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

CSLU启动的

配置CSLU发起的通信时，需要的唯一操作是检查并确保从控制器到CSLU的网络可接通性。

已连接到内部部署SSM

使用本地SSM的配置与直接连接非常相似。内部部署需要运行版本8-202102或更高版本。对于SLUP版本（17.3.2及更高版本），建议使用CSLU URL和传输类型。URL可以从智能许可 >资产> <虚拟帐户> >常规部分下的本地WebUI界面获取。

```
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
```

本地SSM不需要使用信任令牌。



注意：如果您正在获取消息%PKI-3-CRL_FETCH_FAIL：信任点SLA-TrustPoint的CRL获取失败，这是因为您尚未在SLA-TrustPoint下配置revocation-check none。这是用于智能许可的信任点。在内部部署中，许可服务器上的证书通常是无法进行CRL验证的自签名证书，因此要求配置无撤销检查。

配置通过HTTPS代理的智能传输

注意：从代码版本17.9.2开始，尚不支持经过身份验证的代理。如果您在基础设施中使用经过身份验证的代理，请考虑使用[思科智能许证实用程序管理器\(CSLU\)](#)，它支持此类服务器。

要在使用智能传输模式时使用代理服务器与CSSM通信，请完成以下步骤：

```
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
```

通信频率

可在CLI或GUI中配置的报告间隔无效。

无论通过Web界面或CLI配置何种报告间隔，9800 WLC都会每8小时与CSSM或内部智能软件管理器进行通信。这意味着新加入的接入点可在初次加入后8小时内显示在CSSM上。

使用show license air entities summary命令可以确定下次计算和报告许可证的时间。此命令不是典型show tech或show license all输出的一部分：

<#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
```

许可证出厂重置

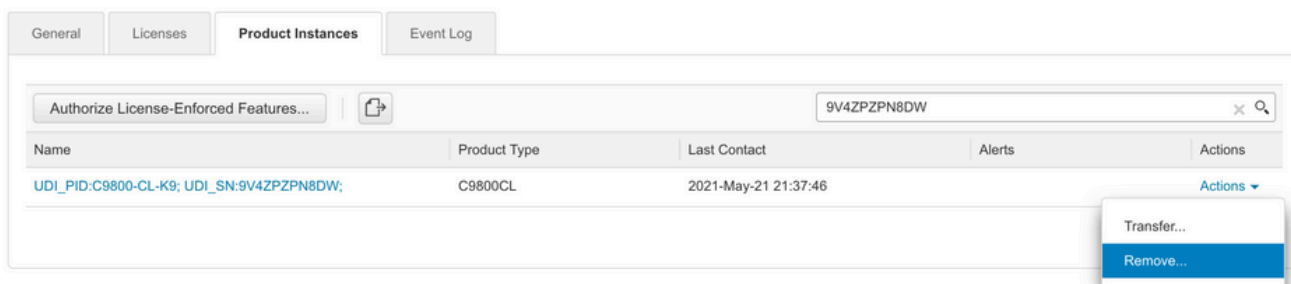
Catalyst 9800 WLC可拥有其所有许可配置和信任工厂重置，并仍保留所有其他配置。这需要WLC重新加载：

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

在RMA或硬件更换的情况下

如果需要更换9800 WLC，则新设备必须注册到CSSM/内部智能软件管理器，并被视为新设备。释放以前设备的许可证计数需要在产品实例下手动删除：

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...

从特定许可证注册(SLR)升级

早于17.3.2的早期WLC版本使用名为特定许可证注册(SLR)的特殊离线许可方法。在使用SLUP (17.3.2及更高版本) 的版本中，此许可方法已弃用。

如果您将使用SLR的9800控制器升级到17.3.2或17.4.1之后的版本，建议您迁移到离线SLUP报告，而不是依赖SLR命令。保存许可证使用RUM文件并在智能许可门户中注册该文件。由于SLR在较新版本中不再存在，因此会报告正确的许可证计数并释放所有未使用的许可证。许可证不再受阻，但会报告确切的使用数量。

故障排除

互联网接入、端口检查和Ping

新SLUP不是使用传统智能许可的tools.cisco.com，而是使用smartreceiver.cisco.com域建立信任。在撰写本文时，此域解析为多个不同的IP地址。并非所有这些地址都可执行ping操作。不得将Ping用作来自WLC的Internet可达性测试。无法ping通这些服务器并不表示它们无法正常工作。

必须使用Telnet (而不是通过ping) 通过端口443进行连通性测试。可以根据smartreceiver.cisco.com域或直接根据服务器IP地址检查Telnet。如果流量未被阻塞，端口必须在输出中显示为打开：

```
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]
```

系统日志

如果在配置令牌时启用terminal monitor命令，WLC会在CLI中打印出相关日志。如果运行show logging命令，也可以获取这些消息。成功建立的信任的日志如下所示：

```
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 st
Aug 22 12:13:08.952: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named SLA-KeyPair has been generated or impor
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 in
```

没有已定义的DNS服务器或具有不起作用的DNS服务器的WLC的日志：

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

WLC的日志，该WLC具有正常运行的DNS服务器，但无法访问Internet：

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

数据包捕获

即使WLC和CSSM/本地SSM之间的通信已加密并通过HTTPS传输，执行数据包捕获仍可揭示导致无法建立信任的原因。收集数据包捕获的最简单方法是通过WLC Web界面。

导航到故障排除 > Packet Capture。创建新的捕获点：

Troubleshooting > Packet Capture



确保启用Monitor Control Plane复选框。将缓冲区大小增加到最大100MB。添加必须捕获的接口。默认情况下，智能许可流量从无线管理接口发出，或者从使用ip http client source-interface命令定义的接口发出：

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 ←

启动捕获并运行license smart trust idtoken <token> all force命令：

Troubleshooting > Packet Capture

+ Add
× Delete

Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
<input checked="" type="checkbox"/> license	Vlan39	Yes	<input type="text" value="0%"/>	any	3600 secs	Inactive	<input style="border: 1px solid red;" type="button" value="Start"/>

◀ ▶ items per page 1 - 1 of 1 items

信任建立的数据包捕获必须包含以下步骤：

1. 使用SYN、SYN-ACK和ACK序列建立TCP会话
2. 使用服务器和客户端证书交换建立TLS会话。建立以新会话票证数据包结束
3. 加密数据包交换(应用数据帧)，其中WLC报告许可证使用情况
4. 通过FIN-PSH-ACK、FIN-ACK和ACK序列终止TCP会话

注意：数据包捕获包含大量帧，包括TCP窗口更新和应用数据帧的倍数

由于CSSM云使用3个不同的公有IP地址，为了过滤掉WLC和CSSM之间的所有数据包捕获，请使用以下wireshark过滤器：

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

如果使用内置SSM，则过滤SSM IP地址：

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

示例：使用直接连接的CSSM成功建立信任并过滤所有重要数据包捕获的数据包捕获：

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

显示命令

以下这些show命令包含有关信任建立的有用信息：

```
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命令是比较有用的命令之一，因为它可以显示从WLC发送并从CSSM返回的实际消息。

成功的信任建立已打印“REQUEST： Aug 23 10:18:08 2021 Central”和“RESPONSE： Aug 23 10:18:10 2021 Central”。如果RESPONSE行之后没有任何内容，则表示WLC未收到来自CSSM的响应。

以下是成功建立信任的show license history message输出示例：

```
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_identfier": "", "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_identfier": ""}, {"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}}
```

调试/btrace

在尝试使用license smart trust idtoken all force命令建立信任后几分钟运行此命令。IOSRP日志非常详细。附加 | include smart-agent”添加到命令中，仅获取智能许可日志。

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

您也可以运行这些调试，然后重新配置许可命令以强制建立新连接：

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

常见问题

WLC没有互联网接入或防火墙阻止/更改流量

WLC上的嵌入式数据包捕获是查看WLC是否从CSSM或本地SSM收到任何信息的简单方法。如果没有响应，防火墙可能会阻止某些内容。


如果从CSSM云或本地SSM未收到任何响应，则在发出请求后1秒，show license history message命令会打印空白响应。

例如，这会使您认为已收到空响应，但实际上根本没有任何响应：

```
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：**当前有一个增强请求Cisco Bug ID [CSCvy84684](#)，该请求使show license history消息在没有响应时打印空白响应。这是为了增强show license history message命令的输出

数据包捕获中的未知CA警报

与CSSM或本地SSM的通信要求9800端具有适当的证书。它可以自签名，但不能无效或过期。在这种情况下，当9800 HTTP客户端证书过期时，数据包捕获显示CSSM发送的未知CA的TLS警报。

智能许可使用ip http client配置，这与WLC Web界面使用的ip http server不同。这意味着需要正确配置以下命令：

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

使用show crypto pki trustpoints命令可以找到信任点名称。建议使用自签名证书TP-self-signed-xxxxxxxxxx证书或制造商安装证书(MIC)，通常称为CISCO_IDVID_SUDI，仅在9800-80、9800-40和9800-L上提供。

请注意，执行TLS拦截的设备（例如具有SSL解密功能的防火墙）可能会阻止C9800与思科许可服务器成功建立握手，因为提供的HTTPS证书是防火墙证书而不是思科许可服务器证书。

 **注意：**请确保同时配置source-interface和secure-trustpoint命令。即使WLC只有一个L3接口，也需要source-interface命令。

相关信息

- [9800上的智能许可，带气隙模式](#)
- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。