# Configurar o & Solucionar Problemas do Licenciamento Inteligente do Catalyst 9800 com SLUP

## Contents



## Introdução

Este documento descreve como configurar e solucionar problemas do Smart Licensing Using Policy (SLUP) no Catalyst 9800 Wireless LAN Controller (WLC) .

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

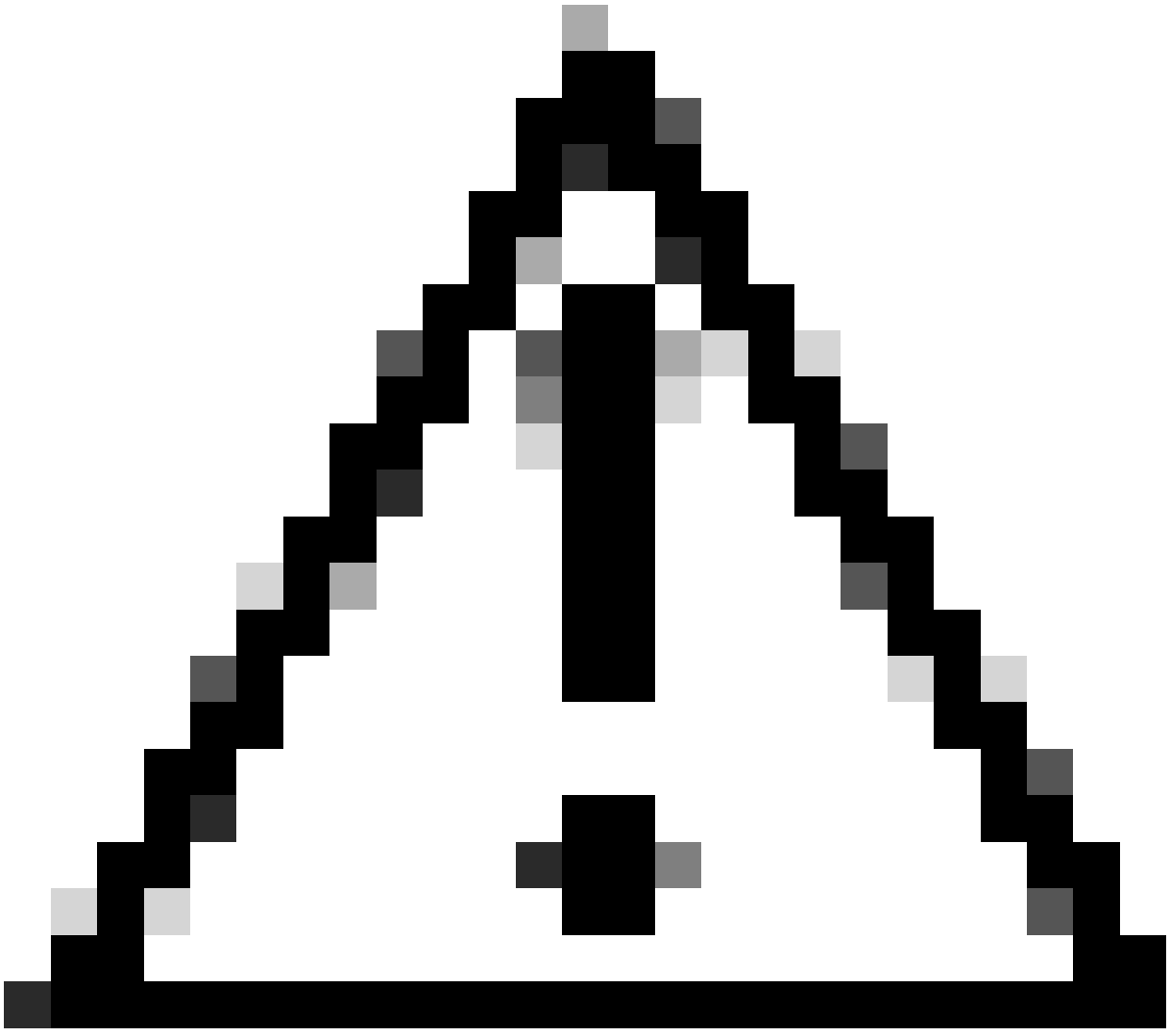
- Licenciamento inteligente usando política (SLUP)
- Controlador de LAN sem fio (WLC) Catalyst 9800

### Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

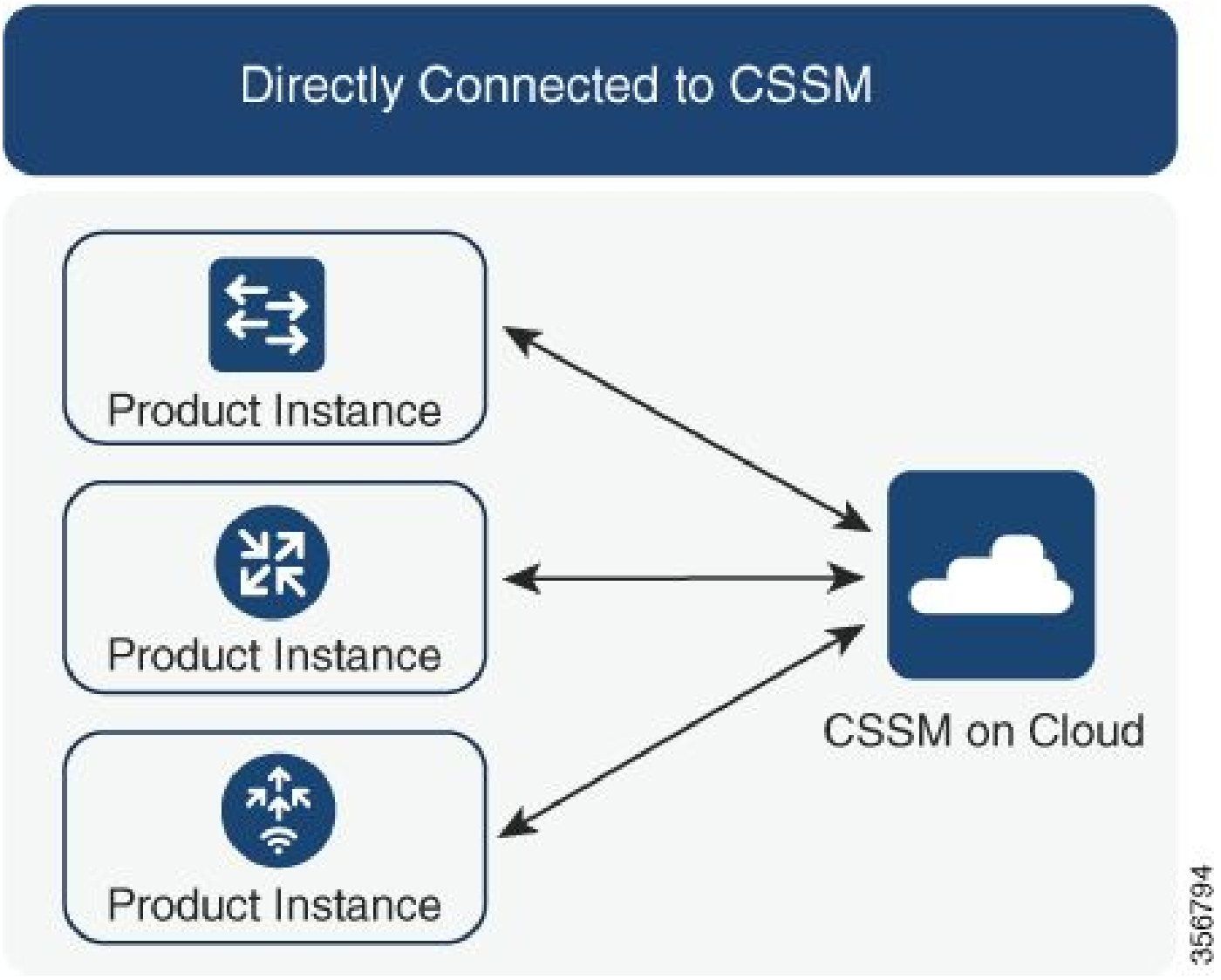
## Informações de Apoio



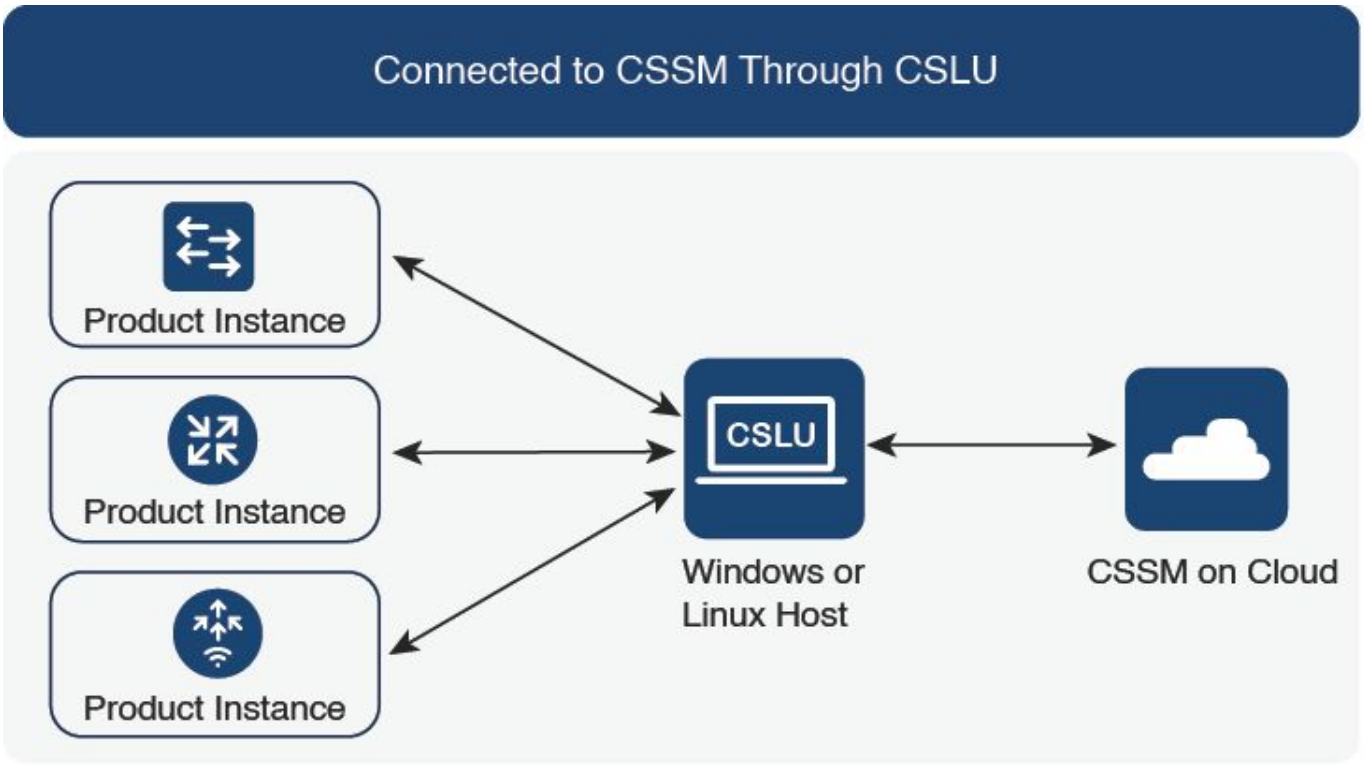
Cuidado: as notas neste artigo contêm sugestões úteis ou referências a materiais não cobertos no documento. É recomendável ler cada nota.

1. Conexão direta com o Cisco Smart Software Manager Cloud (CSSM Cloud)
2. Conectado ao CSSM via CSLU (Cisco Smart License Utility Manager)
3. Conectado ao CSSM por meio do Smart Software Manager no local (SSM no local)

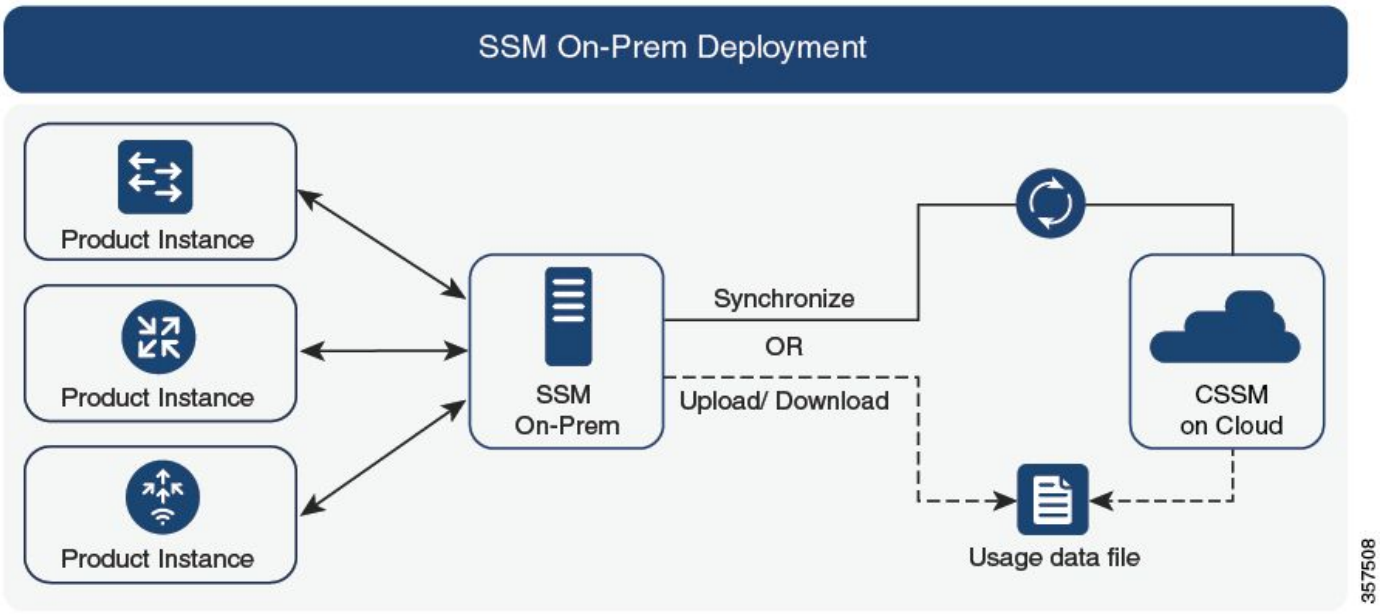
Este artigo não cobre todos os cenários de Smart Licensing no Catalyst 9800. Consulte o Guia de Configuração de Licenciamento Inteligente Usando Política para obter informações adicionais. No entanto, este artigo fornece uma série de comandos úteis para solucionar problemas de conexão direta, CSLU e Smart Licensing SSM no local usando problemas de política no Catalyst 9800.




Opção 1. Conexão direta com o Cisco Smart Licensing Cloud Servers (CSSM)




Opção 2. Conexão via CSLU




Opção 3. Conexão via Smart Software Manager no local (SSM no local)

Observação: todos os comandos mencionados neste artigo são aplicáveis somente às WLCs que executam a versão 17.3.2 ou posterior.

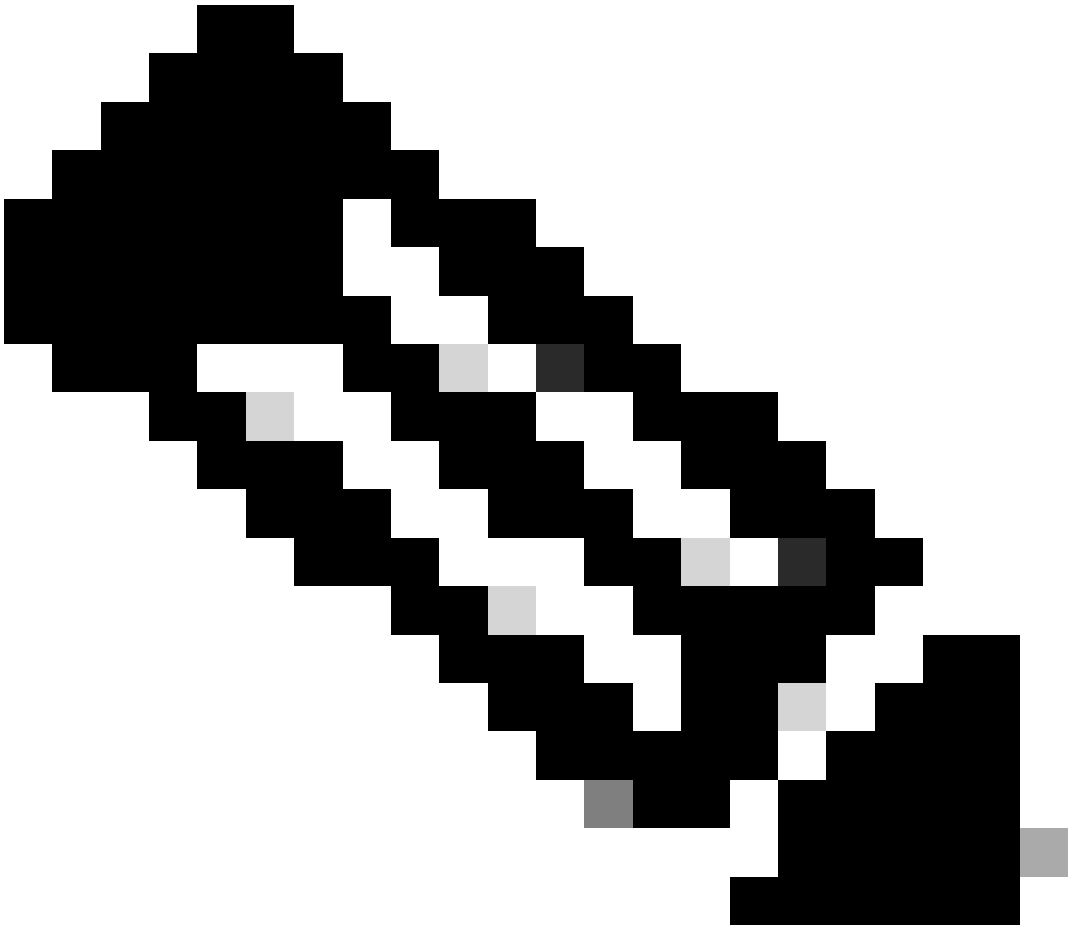
## Licenciamento tradicional x SLUP

O recurso Smart Licensing Using Policy foi introduzido no Catalyst 9800 com a versão de código 17.3.2. A versão 17.3.2 inicial perde o menu de configuração SLUP na webUI da WLC, que foi

introduzido com a versão 17.3.3. O SLUP é diferente do licenciamento inteligente tradicional de duas maneiras:

- A WLC agora se comunica com o CSSM através do domínio smartreceiver.cisco.com, em vez do domínio tools.cisco.com.
- Em vez de se registrar, a WLC agora estabelece confiança com o CSSM ou SSM no local.
- Os comandos CLI foram levemente alterados.
- Não há mais reserva de Smart Licensing (SLR). Em vez disso, você pode relatar o uso periodicamente manualmente.
- Não há mais modo de avaliação. A WLC continua a funcionar com capacidade total mesmo sem licença. O sistema é baseado em honra e você deve relatar o uso da sua licença periodicamente (automaticamente ou manualmente no caso de redes com airgapped).

---



Aviso: se estiver usando um Cisco Catalyst 9800-CL Wireless Controller, certifique-se de estar familiarizado com o requisito ACK obrigatório que começa com o Cisco IOS® XE Cupertino 17.7.1. Consulte Requisito de Relatório e Confirmação de RUM para Controlador sem Fio Cisco Catalyst 9800-CL.

---

# Configuração

## CSSM de conexão direta

Depois que o token tiver sido criado no CSSM, para estabelecer a confiança, estes comandos precisam ser executados:

---

Nota: Token Max. A contagem de número de utilizações deve ser pelo menos 2 em um caso de WLC em HA SSO.

---

```
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
```

- O comando ip http client source-interface especifica a interface L3 da qual os pacotes relacionados ao licenciamento serão originados
- O comando ip http client secure-trustpoint especifica qual ponto confiável/certificado é usado para comunicação CSSM. O nome do ponto confiável pode ser encontrado usando o comando show crypto pki trustpoints. Recomenda-se o uso de um certificado TP-self-signed-xxxxxxxxxx autoassinado ou de um certificado instalado pelo fabricante (também conhecido como MIC, disponível somente nas séries 9800-40, 9800-80 e 9800-L), normalmente chamado CISCO_IDEVID_SUDI.
- O comando Terminal monitor faz com que a WLC imprima os logs no console e ajude a confirmar se a confiança foi estabelecida com êxito. Ele pode ser desativado usando terminal no monitor.
- A palavra-chave all no último comando diz a todas as WLCs no cluster HA SSO para estabelecer a confiança com o CSSM.
- Keyword force manda que a WLC substitua qualquer uma das relações de confiança estabelecidas anteriormente e tente uma nova.

---

Observação: se a confiança não estiver sendo estabelecida, o 9800 tentará novamente 1 minuto depois que o comando for executado e não tentará novamente por algum tempo. Insira o comando token novamente para forçar um novo estabelecimento de confiança.

---

## Conectado ao CSLU

O Cisco Smart License Utility Manager (CSLU) é um aplicativo baseado em Windows (também disponível no Linux) que permite aos clientes administrar licenças e suas instâncias de produto

associadas de suas instalações, em vez de ter que conectar diretamente suas instâncias de produto habilitadas para Smart Licensed ao Cisco Smart Software Manager (CSSM).

Esta seção abrange apenas a configuração sem fio do 9800. Há outras etapas a serem executadas para configurar o licenciamento com o CSLU (como instalar o CSLU, configurar o software CSLU e assim por diante), que é abordado nos Guias de Configuração .Se você deseja implementar um método de comunicação iniciado pela instância do produto ou pelo CSLU, ou concluir a sequência de tarefas correspondente.

Instância do produto iniciada

1. Garanta a acessibilidade da rede do controlador para a CSLU
2. Certifique-se de que o tipo de transporte esteja definido como cslu:

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

3. Se quiser que a CSLU seja descoberta pelo controlador, você precisará executar a ação. Se desejar que a CSLU seja descoberta usando o DNS, nenhuma ação será necessária. Se você quiser descobri-lo usando um URL, insira estes comandos:

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

CSLU iniciado

Quando você configura a comunicação iniciada por CSLU, a única ação necessária é verificar e garantir que a rede esteja acessível para CSLU a partir do controlador.

## Conectado ao SSM no local

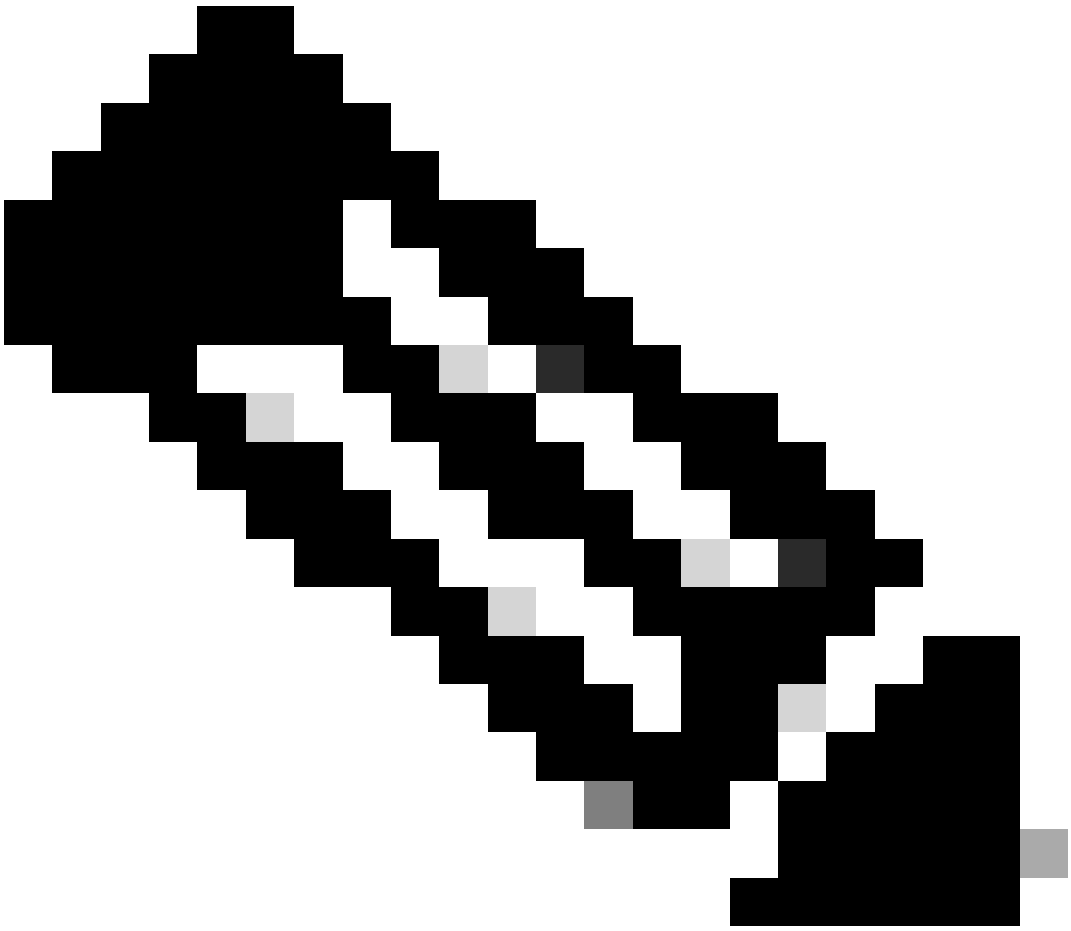
A configuração com SSM no local é bastante semelhante à conexão direta. O local precisa executar a versão 8-202102 ou mais recente. Para versões SLUP (17.3.2 e posterior), é aconselhável usar o URL da CSLU e o tipo de transporte. O URL pode ser obtido na interface da WebUI no local na seção **Smart Licensing > Inventory > <Virtual Account> > General**.

```
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
```

O SSM no local não requer o uso de um token confiável.

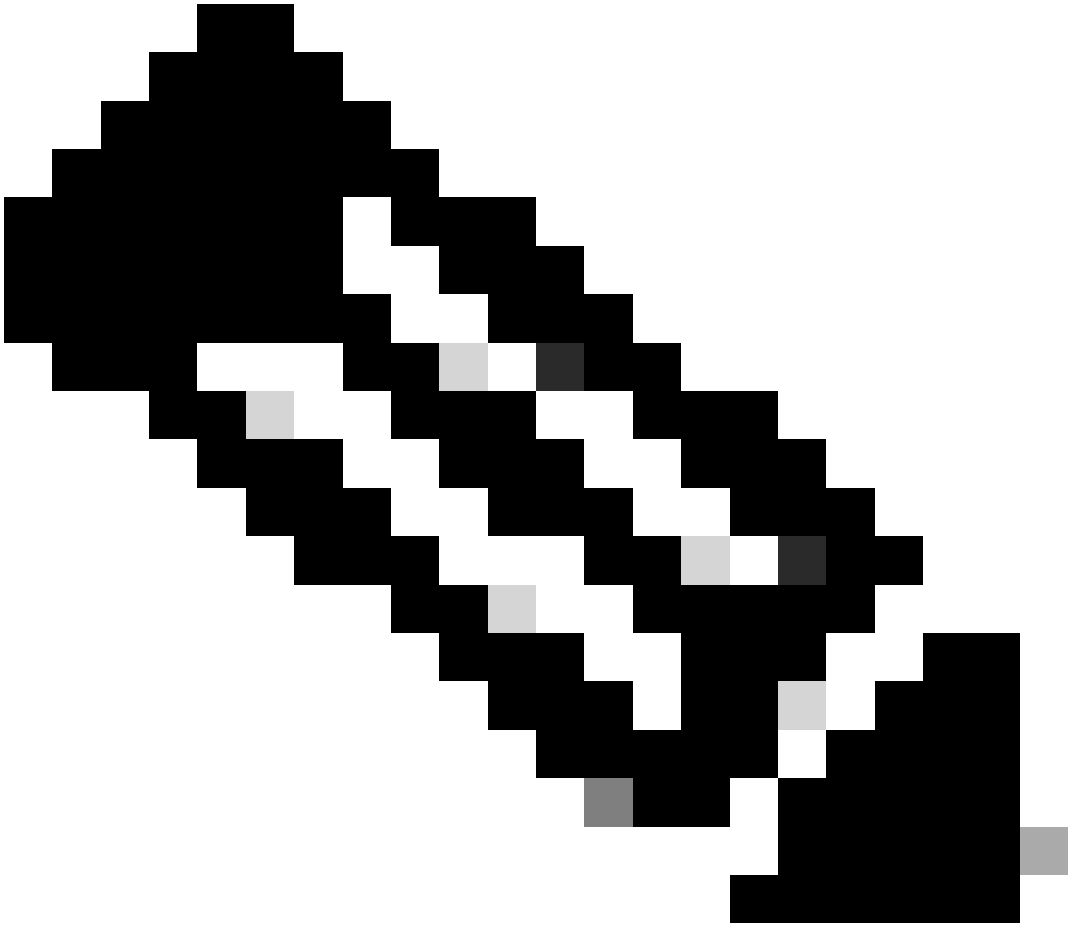
---



> Observação: se você está recebendo a mensagem, %PKI-3-CRL_FETCH_FAIL: Falha na busca de CRL para o ponto de confiança SLA-TrustPoint, é porque você não configurou a verificação de revogação como nenhuma no SLA-TrustPoint. Este é o ponto de confiança usado para o Smart Licensing. No caso de local, o certificado no servidor de licenciamento é, na maioria das vezes, um certificado autoassinado para o qual a verificação de CRL não é possível, portanto, o requisito de configurar nenhuma verificação de revogação.

---

## Configuração do Smart Transport por meio de um proxy HTTPS



Observação: Proxies autenticados ainda não são suportados a partir da versão de código 17.9.2. Se você estiver usando proxies autenticados em sua infraestrutura, considere usar o Cisco Smart License Utility Manager (CSLU), ele suporta esse tipo de servidor.

Para usar um servidor proxy para se comunicar com o CSSM ao usar o modo de transporte inteligente, siga estas etapas:

```
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
```

## Frequência de comunicação

O intervalo de relatório que você pode configurar na CLI ou na GUI não tem efeito.

A WLC 9800 se comunica com o CSSM ou o Smart Software Manager no local a cada 8 horas, independentemente do intervalo de relatório configurado por meio da interface da Web ou da CLI. Isso significa que os pontos de acesso recém-ingressados podem aparecer no CSSM até 8 horas após o ingresso inicial.

Você pode descobrir a próxima vez que as licenças forem calculadas e relatadas com o comando show license air entities summary. Este comando não faz parte da saída típica de show tech ou show license all:

<#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
```

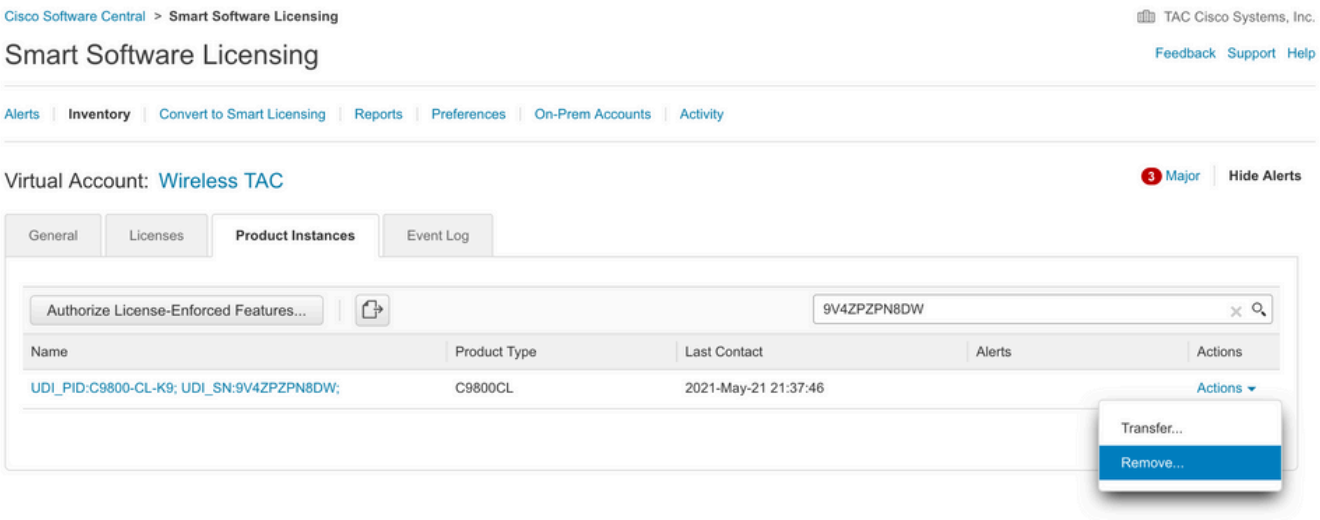
## Redefinição de fábrica da licença

A WLC do Catalyst 9800 pode ter todas as suas configurações de licenciamento e de confiança redefinidas de fábrica e ainda manter todas as outras configurações. Isso requer uma recarga da WLC:

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

## Em caso de substituição de RMA ou hardware

Se a WLC 9800 precisar ser substituída, o novo dispositivo terá que se registrar no CSSM/Gerenciador Inteligente de Software no local e será considerado como um novo dispositivo. A liberação da contagem de licenças do dispositivo anterior requer a exclusão manual em Instâncias de produto:




### Atualização de Registro de Licença Específica (SLR)

Versões mais antigas da WLC, anteriores à 17.3.2, usavam um método especial de licenciamento offline chamado Registro de Licença Específica (SLR - Specific License Registration). Este método de licenciamento foi preterido nas versões usando SLUP (17.3.2 e posterior).

Se você atualizar um controlador 9800 que estava usando o SLR para uma versão posterior à 17.3.2 ou 17.4.1, é recomendável passar para o relatório SLUP off-line em vez de depender dos comandos SLR. Salve o arquivo RUM de uso de licença e registre-o no Smart Licensing Portal. Como o SLR não existe mais em versões mais recentes, ele informa a contagem de licenças correta e libera qualquer licença não utilizada. As licenças não são mais bloqueadas, mas a contagem exata de uso é relatada.

## Troubleshooting

### Acesso à Internet, verificações de porta e pings

Em vez do tools.cisco.com usado pelo Smart Licensing tradicional, o novo SLUP usa o domínio smartreceiver.cisco.com para estabelecer confiança. No momento em que este artigo foi escrito, este domínio resolve para vários endereços IP diferentes. Nem todos esses endereços podem receber ping. Os pings não devem ser usados como um teste de acessibilidade da Internet da WLC. Não conseguir fazer ping nesses servidores não significa que eles não estejam funcionando corretamente.

Em vez de pings, o telnet na porta 443 deve ser usado como um teste de acessibilidade. O Telnet pode ser verificado no domínio smartreceiver.cisco.com ou diretamente nos endereços IP do servidor. Se o tráfego não estiver sendo bloqueado, a porta deve aparecer como aberta na saída:

```
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]
```

## Syslog

Se o comando terminal monitor estiver habilitado enquanto o token estiver sendo configurado, a WLC imprimirá os logs relevantes na CLI. Essas mensagens também podem ser obtidas se você executar o comando show logging. Os logs de uma relação de confiança estabelecida com êxito se parecem com o seguinte:

```
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
```

Logs de uma WLC sem um servidor DNS definido ou com um servidor DNS não funcional:

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

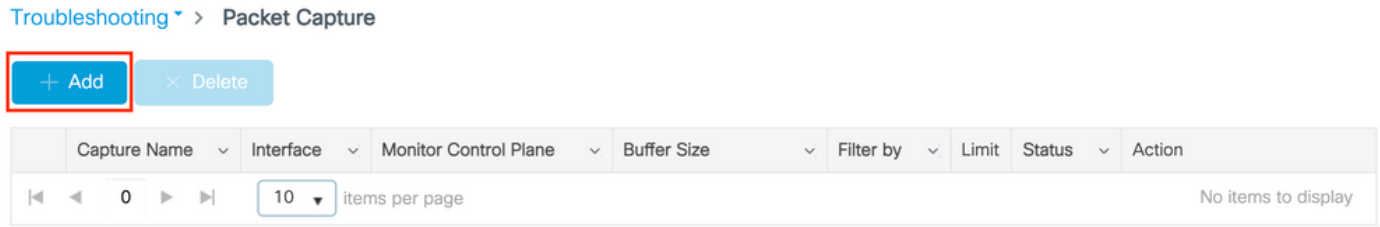
Registros de uma WLC com um servidor DNS em funcionamento, mas sem acesso à Internet:

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

## Capturas de pacotes

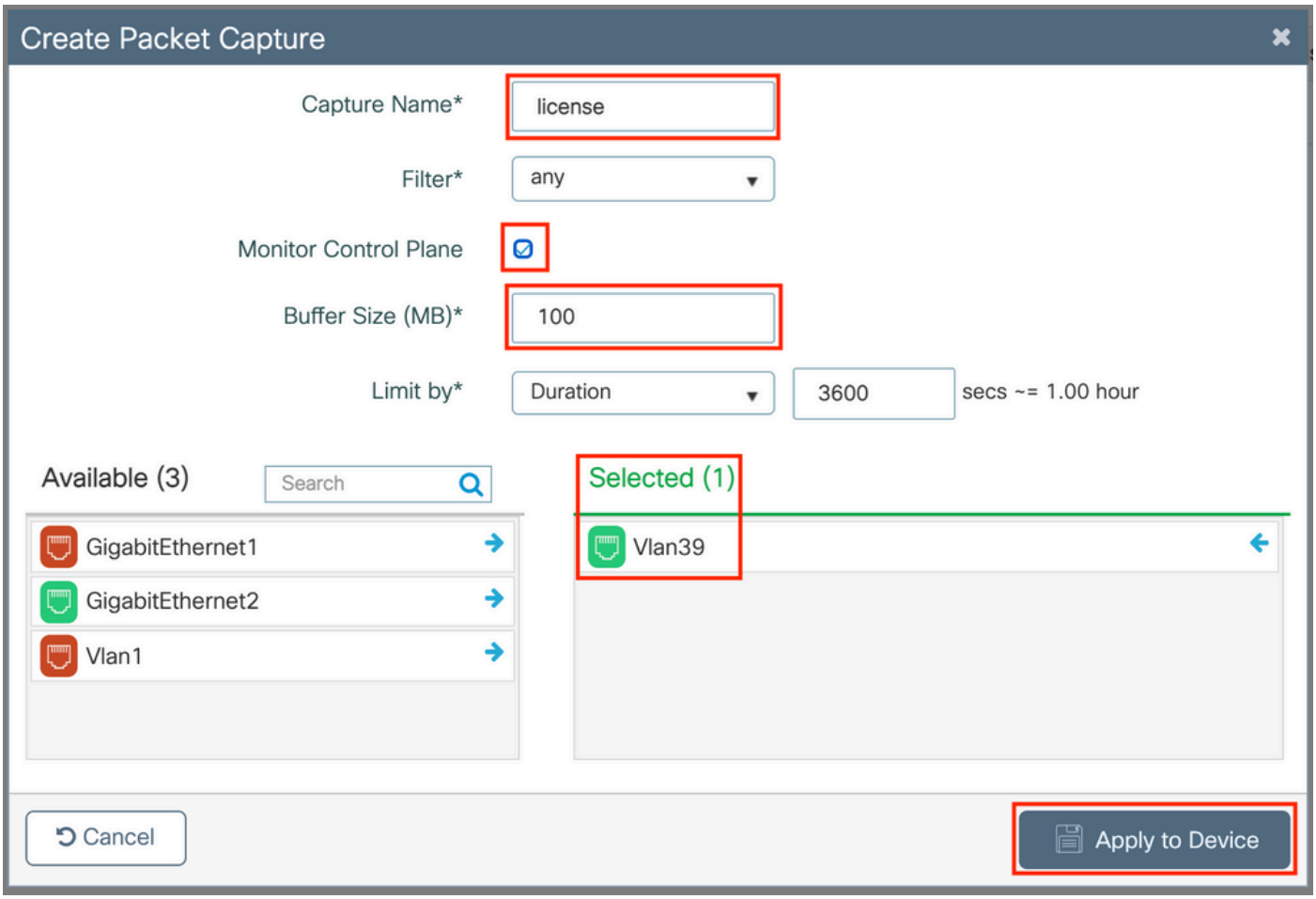
Mesmo que a comunicação entre a WLC e o CSSM/SSM no local seja criptografada e passe por HTTPS, a execução de capturas de pacotes pode revelar o que faz com que a confiança não seja estabelecida. A maneira mais fácil de coletar capturas de pacotes é através da interface Web da WLC.

Navegue até Troubleshooting > Captura de Pacotes. Crie um novo ponto de captura:




Certifique-se de que a caixa de seleção Monitor Control Plane esteja ativada. Aumente o tamanho do buffer para o máximo de 100 MB. Adicione a interface que deve ser capturada. O tráfego de licenciamento inteligente é originado da interface de gerenciamento sem fio por padrão ou da

interface definida com o comando ip http client source-interface:




Inicie as capturas e execute o comando license smart trust idtoken <token> all force:


As capturas de pacotes de um estabelecimento de confiança devem conter estas etapas:

1. Estabelecimento de sessão TCP usando sequência SYN, SYN-ACK & ACK
2. Estabelecimento de sessão TLS com troca de certificados de servidor e cliente. O estabelecimento termina com o pacote New Session Ticket
3. Troca de pacotes criptografados (quadros de dados de aplicativos) onde o WLC relata o uso da licença
4. Encerramento da sessão TCP através da sequência FIN-PSH-ACK, FIN-ACK & ACK

---

Nota: As capturas de pacote contêm muito mais quadros, incluindo múltiplos de quadros de atualização de janela TCP e de dados de aplicação.

---

Como a nuvem CSSM usa 3 endereços IP públicos diferentes, para filtrar todas as capturas de pacotes entre a WLC e o CSSM, use estes filtros do Wireshark:

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

Se estiver usando um SSM no local, filtre o endereço IP do SSM:

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

Exemplo: capturas de pacotes de um estabelecimento de confiança bem-sucedido com CSSM conectado diretamente com todas as capturas de pacotes significativas filtradas:

| 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 |

## comandos show

Estes comandos show contêm informações úteis sobre o estabelecimento de confiança:

```
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)
```

O comando show license history message é um dos comandos mais úteis, pois pode exibir as mensagens reais enviadas da WLC e recebidas de volta do CSSM.

Uma instituição de confiança bem-sucedida tem as mensagens "REQUEST: Aug 23 10:18:08 2021 Central" e "RESPONSE: Aug 23 10:18:10 2021 Central" impressas. Se não houver nada depois da linha RESPONSE, isso significa que a WLC não recebeu uma resposta do CSSM.

Este é um exemplo de uma saída de mensagem show license history para um estabelecimento de confiança bem-sucedido:

```
REQUEST: Aug 23 10:18:08 2021 Central
{"request":"{\"header\":{\"request_type\":\"POLL_REQ\",\"sudi\":{\"udi_pid\":\"C9800-CL-K9\",\"udi_seri
NB\"},\"version\":\"1.3\",\"locale\":\"en_US.UTF-8\",\"signing_cert_serial_number\":\"3\",\"id_cert_ser
\",\"product_instance_identifier\":\"\",\"connect_info\":{\"name\":\"C_agent\",\"version\":\"5.0.9_rel/
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":"eiJ7IuQaTCFxgUkwls76WZxa5DRI5A
OgMqQd5POU6VNsH2j9dHco4T1NJ/aCMbR1MRmkfxyVSWsx4lmjJL1lmpOSi3ZS4FBMvlF/EBOUfowREe2oz2lrQp1cAFpPn5SlaFezW
/Nu6SQZfIW+IdF+2qnJeNFAIZbNpgOB5d5HIJvDmDImvDu3bMRHhQAWr2KKzGFr6jPzOhs7bGY/+FlfTLQk5LFEUaKTNH/tuxJPFHlF
h9//uhsd+NaQyfdRFludkbfUBTFkvPxHW9/5w=="}}

  RESPONSE: Aug 23 10:18:10 2021 Central
{"signature":{"type":"SHA256","value":"TXZEO34fqAul2jy9V4+HoB2hDShl9au/5sgodiCVatmu671/6MyN7kZfEzREufY8
SLrjTfO4grGeQTcH7yEjOD+gztWXCOu8RBT7/Bo9aBs\n4x1iOE6flPB3BP6yu7KIEUQZ8yHzlwDT+mVtJGi6TRrtYnV3KQMpCUmF5F
wOksf3SfXreNZJuzWXzjHvtmlusCQXw7ZTBzffYsNKOOlkJlr\nvgB2PkV7JUlsA481kpIvlPul6IiJXqk+2PC2IzCrCLG57lVN3XgX
1pEl2SHyQ/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\",\
9PJK8D7OCNB\"},\"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_identifier\":\"\"},\"status_code\":\"FAILE
\"Invalid ProductInstanceIdentifier: 2e84a42f-c903-44c5-83b2-e62e258c780f provided in the polling reque
262236\",\"retry_time_seconds\":0,\"response_data\":\"\"}","sch_response":null}
```

## Depurações/btrace

Execute este comando alguns minutos após uma tentativa de estabelecimento de confiança usando um comando license smart trust idtoken all force. Os logs do IOSRP são extremamente detalhados. Anexar | inclua "smart-agent" no comando para obter apenas logs do smart licensing.

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

Você também pode executar essas depurações e depois reconfigurar os comandos de licenciamento para forçar uma nova conexão:

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

# Problemas comuns

## A WLC não tem acesso à Internet ou o firewall bloqueia/altera o tráfego

Capturas de pacotes incorporadas na WLC são uma maneira fácil de ver se a WLC recebe algo de volta do CSSM ou do SSM no local. Se não houve resposta, é possível que o firewall esteja bloqueando algo.

O comando show license history message imprime uma resposta vazia 1 segundo após a solicitação ser enviada se nenhuma resposta foi recebida da nuvem CSSM ou do SSM no local.

Por exemplo, isso pode levá-lo a acreditar que uma resposta vazia foi recebida, mas na realidade não houve nenhuma resposta:

```
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
```

---

Nota: No momento, há uma solicitação de aprimoramento com a ID de bug da Cisco CSCvy84684 que faz com que a mensagem show license history imprima uma resposta vazia quando não há resposta. Isso serve para aprimorar a saída do comando show license history message

---

## Alerta de CA desconhecido em capturas de pacotes

A comunicação com o CSSM ou SSM no local requer um certificado adequado no lado do 9800. Ele pode ser autoassinado, mas não pode ser inválido ou expirado. Nesse caso, uma captura de pacote mostra um alerta TLS para CA desconhecida enviado pelo CSSM quando o certificado do cliente HTTP 9800 expira.

O licenciamento inteligente usa a configuração do ip http client, que é diferente do ip http server que a interface da WLC usa. Isso significa que esses comandos precisam ser configurados corretamente:

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

O nome do ponto confiável pode ser encontrado com o comando show crypto pki trustpoints. Recomenda-se o uso de um certificado autoassinado TP-self-signed-xxxxxxxxxx ou de um Certificado Instalado pelo Fabricante (MIC), que geralmente é chamado de CISCO_IDEVID_SUDI e está disponível somente nas séries 9800-80, 9800-40 e 9800-L.

É importante observar que os dispositivos que fazem interceptação TLS, como um firewall com o recurso de descriptografia SSL, podem impedir que o C9800 estabeleça um handshake bem-sucedido com o servidor de licenciamento da Cisco, pois o certificado HTTPS apresentado é o certificado de firewall em vez do certificado de servidor de licenciamento da Cisco.

---

Nota: Certifique-se de configurar os comandos source-interface e secure-trustpoint. Um comando source-interface é necessário mesmo se a WLC tiver apenas uma interface L3.

---

## Informações Relacionadas

- Smart Licensing com modo Air Gap no 9800
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.