

Identificar e Solucionar Problemas de Transporte Inteligente SLP nos Switches Catalyst 9000

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como solucionar problemas do Smart Licensing Using Policy (SLP) usando o Smart Transport em switches Catalyst 9000.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento e familiaridade com este tópico:

- Licenciamento inteligente usando política em dispositivos Cisco IOS® XE.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Catalyst 9200
- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS XE 17.9.1 e versões posteriores



Note: Consulte o guia de configuração apropriado para obter os comandos usados para ativar esses recursos em outras plataformas da Cisco.

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

O Smart Licensing Using Policy é uma versão aprimorada do Smart Licensing, projetada com o objetivo principal de fornecer uma solução de licenciamento que garanta que as operações da sua rede permaneçam ininterruptas. Em vez de causar interrupções, ele estabelece uma relação de conformidade para contabilizar as licenças de hardware e software que você adquire e utiliza.

Para que os relatórios do Smart Licensing funcionem corretamente, o switch Catalyst 9000 conecta-se ao Cisco Smart Software Manager (CSSM) para relatar o uso da licença. O CSSM

serve como uma plataforma centralizada para gerenciar todas as licenças de software da Cisco e revisar o uso, o que ajuda a planejar futuras necessidades de licenciamento.

Há várias topologias através das quais um switch Catalyst 9000 pode se conectar ao CSSM, mas este documento enfoca a topologia específica na qual o switch está diretamente conectado ao CSSM. Isso significa que o switch deve ser capaz de acessar e estabelecer uma conexão com o CSSM, que é hospedado na Internet.

Nessa topologia de conexão direta, há duas opções de transporte: Smart Transport e Call Home, com o Smart Transport sendo o método recomendado. Além disso, o Smart Transport suporta o uso de um proxy HTTPS e permite a seleção de um VRF específico para lidar com a comunicação do Smart Licensing com o CSSM.

Ao usar o Transporte Inteligente, o switch Catalyst 9000 troca informações de uso de licença com o CSSM no formato JSON (JavaScript Object Notation) em uma mensagem HTTPS. Essas informações, conhecidas como Relatório RUM, são enviadas pelo switch e a resposta do CSSM é chamada de ACK.

A frequência mínima de relatório para esta topologia é limitada a um dia. Isso significa que a instância do produto não enviará mais de um relatório RUM por dia, evitando que um número excessivo de relatórios seja gerado e transmitido para determinadas licenças. Isso ajuda a resolver problemas relacionados à memória e a lentidão do sistema causados por uma superprodução de relatórios RUM.

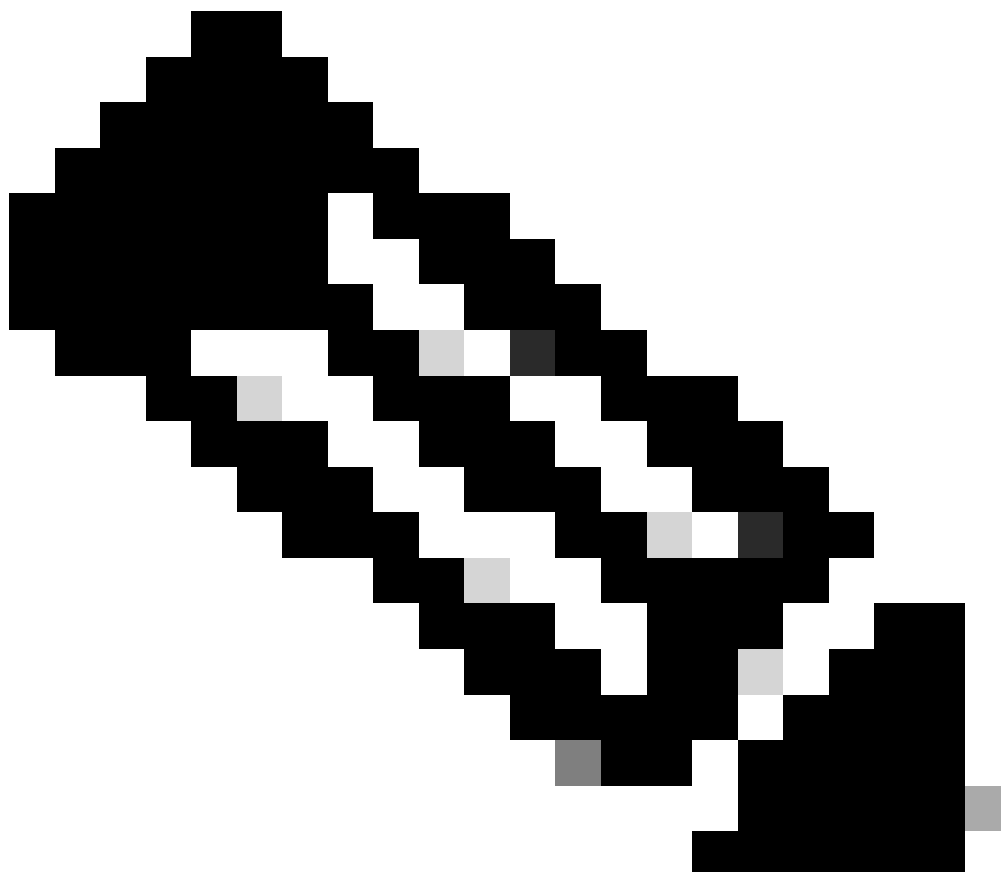
Se necessário, você pode substituir essa restrição de limitação usando o `license smart sync` comando no modo EXEC privilegiado

Configurar

Siga estas etapas para configurar o SLP com Transporte Inteligente:

1. Configure Smart como o tipo de transporte e use o URL padrão.

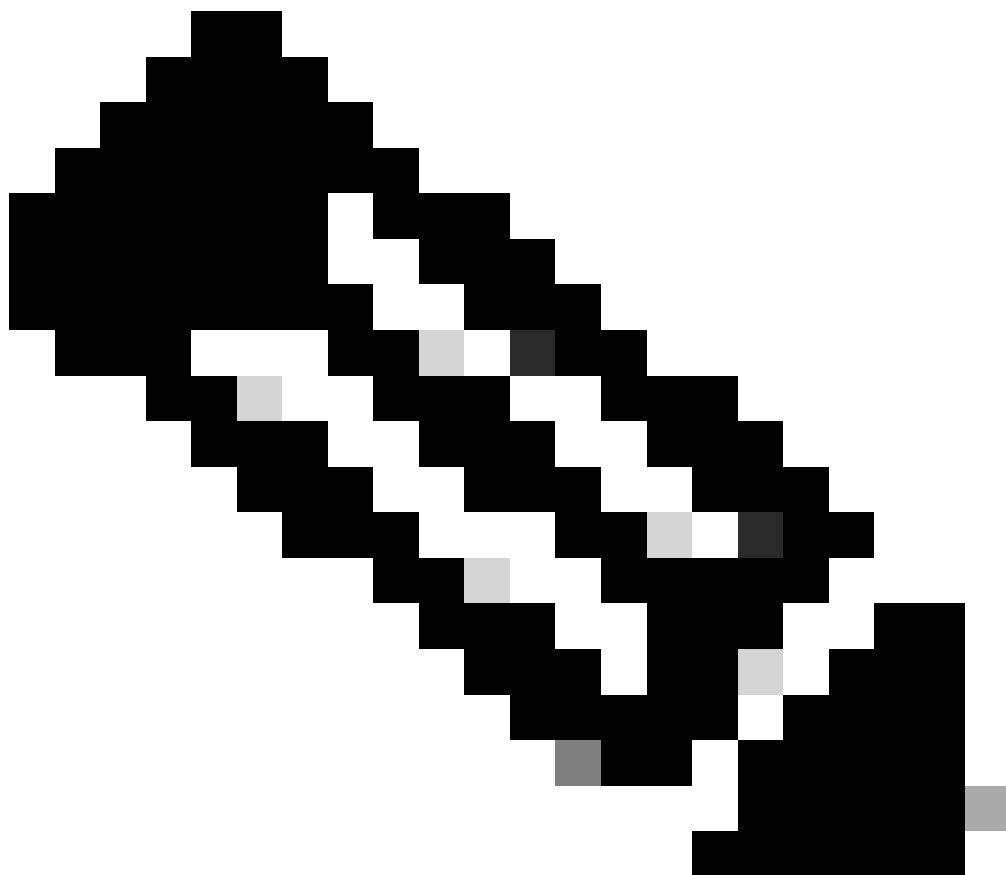
```
Switch#configure terminal
Switch(config)#license smart transport smart
Switch(config)#license smart url default
```



Note: Se um VRF for usado para Transporte Inteligente, license smart vrf precisará ser configurado.

-
2. Configure o servidor DNS e a interface de origem para a resolução DNS e as conexões de cliente HTTP.

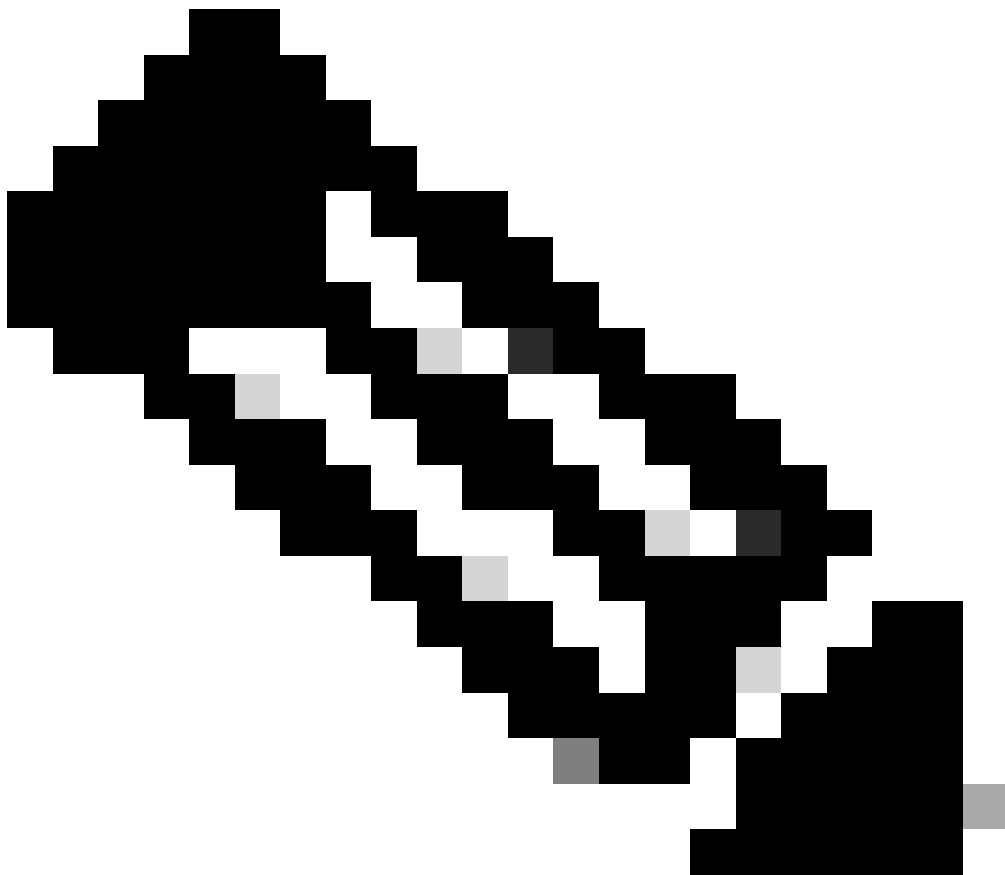
```
Switch(config)#ip domain lookup
Switch(config)#ip name-server 10.31.104.74
Switch(config)#ip domain name cisco.com
Switch(config)#ip domain lookup source-interface Vlan10
```



Note: Se um VRF for usado para Transporte Inteligente, a variante VRF desses comandos precisará ser usada.

3. Se necessário, configure um proxy HTTPS.

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



Note: O servidor proxy pode ser configurado usando seu endereço IP ou nome de host.

-
4. Gere um token na Virtual Account. Para concluir esta etapa, siga o processo descrito [neste documento](#).
 5. Instale o código de confiança no switch.

```
Switch#license smart trust idtoken NGFkODgzMGUtZmNkMS00NTRjLWI5MjUtYjI0YWYzZjU1ZGQzLTE3NDAYNjU5%OA
```

```
[OK]
```

Após o estabelecimento confiável bem-sucedido com o CSSM, um syslog semelhante a este é mostrado.

*Jan 24 23:19:05.144: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was successfully installed.

Além disso, `show license status` mostra o horário de instalação do código de confiança.

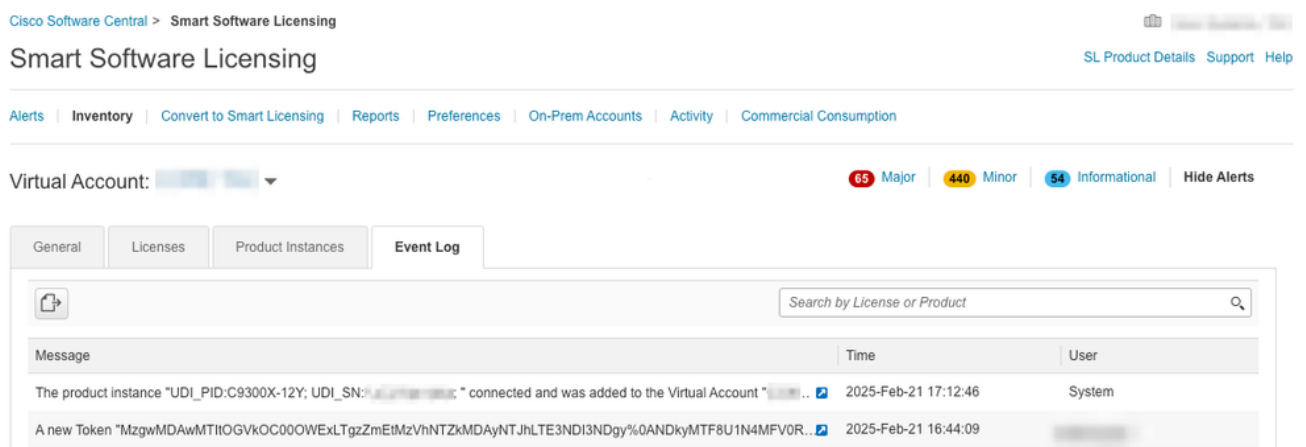
```
<#root>
```

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

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

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

Por fim, o Log de Eventos de Contas Virtuais mostra que o switch foi adicionado.



Log de Eventos de Conta Virtual que Mostra o Dispositivo.

Troubleshooting

Se o estabelecimento confiável com CSSM falhar, um syslog indicando o motivo da falha será exibido.

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

As possíveis razões para a falha de comunicação incluem:

- Não é possível resolver o nome de host/nome de domínio do servidor: O URL de Transporte Inteligente ou o nome de host do servidor proxy não foi resolvido pelo DNS. Validar configurações de resolução de nome e acessibilidade do servidor DNS.

- Tempo limite da conexão: Houve uma tentativa de conexão, mas não houve resposta. Valide se a conexão HTTPS com o CSSM está sendo estabelecida usando capturas de pacotes e verifique se um dispositivo, como um servidor proxy ou firewall, está bloqueando a conectividade. Se estiver usando um servidor proxy, verifique se a porta correta está em uso.

Siga estas etapas e os comandos de validação para solucionar problemas do SLP com o Smart Transport:

1. Validar logs de eventos do Smart Licensing.

```
<#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. Valide a conectividade com o CSSM enviando um ping e tentando uma conexão telnet. Isso verifica se a resolução de nomes está ocorrendo e se não há nenhum bloco administrativo entre o switch e o CSSM.

<#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]

Como alternativa, se um servidor proxy estiver sendo usado, você poderá tentar os mesmos comandos usando o endereço IP e a porta do servidor proxy.

<#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. Valide se os relatórios RUM estão sendo enviados e se há uma resposta.

```
<#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

Se a solicitação for enviada, mas não houver resposta do CSSM, o `show license history` comando não mostrará dados JSON para a resposta fornecida e mais detalhes sobre a falha poderão ser obtidos.

<#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. Acione o switch para enviar um relatório RUM para sincronizar com o CSSM.

<#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. Para confirmar que o switch está estabelecendo a conexão HTTPS com o CSSM, você pode fazer uma captura de pacote. Este é um exemplo de captura de pacote de uma conexão bem-sucedida usando um servidor proxy.

```
<#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.	UTC 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	15:41:21.307857	192.168.217.105	10.31.121.118	TLSv1.3	590	51547	80	Server Hello, Change Cipher Spec, Application Data
11	15:41:21.307882	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]

Captura de pacote de conexão HTTPS bem-sucedida com o CSSM usando um servidor proxy.

6. Se a captura de pacote mostrar que a conexão HTTPS está tentando ser estabelecida, mas falhar, isso pode ser devido a uma falha de handshake TLS ou SSL. Essas depurações podem ser usadas para investigação adicional.

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

7. Se, em algum momento, o código de confiança instalado precisar ser removido do switch, uma redefinição de fábrica do Smart Licensing poderá ser executada. Este processo requer um recarregamento. Após a redefinição de fábrica, um novo código de confiança pode ser instalado. O uso desse comando remove todas as informações de licenciamento, incluindo a política.

```
<#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
```

Informações Relacionadas

- [Licenciamento inteligente usando política para switches Cisco Catalyst 9000 Series](#)
- [Entender o Smart Licensing para switches Catalyst](#)
- [Cisco Live: Introdução ao Smart Licensing usando políticas](#)
- [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.