Troubleshoot SLP Smart Transport on Catalyst 9000 Switches

Contents

Introduction

This document describes how to troubleshoot Smart Licensing Using Policy (SLP) using Smart Transport on Catalyst 9000 switches.

Prerequisites

Requirements

Cisco recommends that you have knowledge of and familiarity with this topic:

- Smart Licensing Using Policy on Cisco IOS® XE devices.

Components Used

The information in this document is based on these software and hardware versions:

- Catalyst 9200
- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS XE 17.9.1 and later versions

Note: Consult the appropriate configuration guide for the commands that are used in order to enable these features on other Cisco platforms.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Smart Licensing Using Policy is an enhanced version of Smart Licensing, designed with the primary goal of providing a licensing solution that ensures your network's operations remain uninterrupted. Rather than being disruptive, it establishes a compliance relationship to account for the hardware and software licenses you purchase and utilize.

For Smart Licensing reporting to function properly, the Catalyst 9000 switch connects with Cisco Smart Software Manager (CSSM) to report license usage. CSSM serves as a centralized platform to manage all Cisco software licenses and review usage, which helps plan for future licensing needs.

There are multiple topologies through which a Catalyst 9000 switch can connect to CSSM, but this document focuses on the specific topology in which the switch is directly connected to CSSM. This means that the switch must be capable of reaching and establishing a connection with CSSM, which is hosted on the Internet.

In this direct connection topology, there are two transport options: Smart Transport and Call Home, with Smart Transport being the recommended method. Additionally, Smart Transport supports the use of an HTTPS proxy and allows for the selection of a specific VRF to handle Smart Licensing communication with CSSM.

When using Smart Transport, the Catalyst 9000 switch exchanges license usage information with CSSM in JavaScript Object Notation (JSON) format within an HTTPS message. This information, known as the RUM Report, is sent by the switch, and the response from CSSM is referred to as an ACK.

The minimum reporting frequency for this topology is throttled to one day. This means the product instance will send no more than one RUM report per day, preventing an excessive number of reports from being generated and transmitted for certain licenses. This helps resolve memory-related issues and system slowdowns caused by an overproduction of RUM reports.

If needed, you can override this throttling restriction by using the license smart sync command in privileged EXEC mode

Configure

Follow these steps to configure SLP with Smart Transport:

1. Configure Smart as the transport type, and use the default URL.

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

Note: If a VRF is used for Smart Transport, license smart vrf <vrf-name> needs to be configured.

2. Configure the DNS server and source interface for DNS resolution and HTTP client connections.

```
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: If a VRF is used for Smart Transport, the VRF variant of these commands needs to be used.

3. If needed, configure an HTTPS proxy.

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

Note: The proxy server can be configured using its IP address or hostname.

4. Generate a token in the Virtual Account. To complete this step, follow the process outlined in [this document](#).
5. Install the trust code on the switch.

```
Switch#license smart trust idtoken NGFkODgzMGUtZmNkMS00NTRjLWI5MjUtYjI0YWYzZjU1ZGQzLTE3NDAyNjU5%0A

[OK]
```

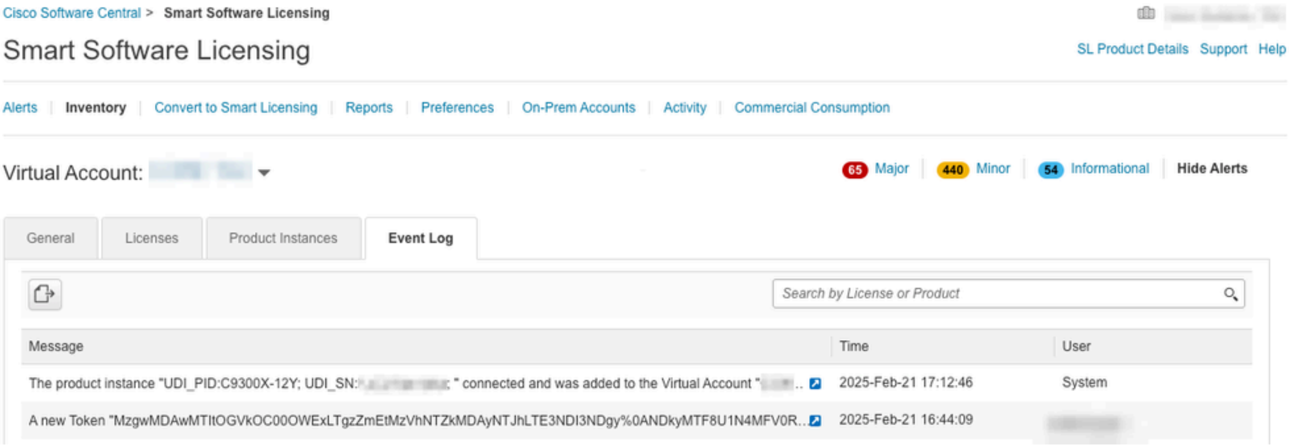
Upon successful Trust Establishment with CSSM, a syslog similar to this is shown.

```
*Jan 24 23:19:05.144: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was successfu
```

Additionally, show license status shows the time of the Trust code installation.

```
<#root>

Switch#show license status  | i Trust

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


<--- Trust code was installed
```

Finally, the **Virtual Account Event Log** shows that the switch was added.



Cisco Software Central > Smart Software Licensing

Smart Software Licensing

[redacted]

SL Product Details Support Help

Alerts | Inventory | Convert to Smart Licensing | Reports | Preferences | On-Prem Accounts | Activity | Commercial Consumption

Virtual Account: [redacted]

65 Major | 440 Minor | 54 Informational | Hide Alerts

General | Licenses | Product Instances | Event Log

Search by License or Product

Message	Time	User
The product instance "UDI_PID:C9300X-12Y; UDI_SN:[redacted]; " connected and was added to the Virtual Account "[redacted]..	2025-Feb-21 17:12:46	System
A new Token "MzgwMDAwMTItOGVkOC00OWExLTgzZmEtMzVhNTZkMDAyNTJhLTE3NDI3NDgy%0ANDkyMTF8U1N4MFV0R..	2025-Feb-21 16:44:09	[redacted]

Virtual Account Event Log Showing Device.

Troubleshoot

If Trust Establishment with CSSM fails, a syslog indicating the reason for failure is shown.

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

Possible reasons for communication failure include:

- Unable to resolve server hostname/domain name: The Smart Transport URL or the proxy server hostname was not resolved by DNS. Validate name resolution configurations and reachability of the DNS server.
- Connection timed out: The connection was attempted, but there was no response. Validate that the HTTPS connection with CSSM is being established using packet captures, and check if a device, such as a proxy server or firewall, is blocking connectivity. If using a proxy server, ensure the correct port is in use.

Follow these steps and validation commands to troubleshoot SLP with Smart Transport:

1. Validate Smart Licensing event logs.

<#root>

```
Switch#

show license eventlog 1

**** Event Log ****

2025-01-24 13:58:23.900 UTC SAEVT_INIT_START version="5.5.29_rel/114"
2025-01-24 13:58:23.922 UTC SAEVT_INIT_CRYPTO success="False" error="Crypto Initialization has not
2025-01-24 13:58:23.922 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmfRegister"
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="SmartAgentEvtHArmfInitialize"
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="SmartAgentEvtHAchkptRegister"
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_CRYPTO success="False" error="Crypto Initialization has not
2025-01-24 13:59:14.143 UTC SAEVT_INIT_CRYPTO 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. Validate connectivity with CSSM by sending a ping and attempting a telnet connection. This verifies that name resolution is occurring and that there is no administrative block between the switch and 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]
```

Alternatively, if a proxy server is being used, you can try the same commands using the IP address and port of the proxy server.

<#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. Validate that RUM reports are being sent and if there is a response.

<#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:<SN>, state[2], Trust Data INSTALLED  TrustId:612
Overall Trust: INSTALLED (2) <--- Trust code installed
```

If there request is sent but there is no response from CSSM, show license history message command shows no JSON data for the given response and more details about the failure can be obtained.

<#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. Trigger the switch to send a RUM report to synchronize with 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 rema

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. To validate that the switch is establishing the HTTPS connection with the CSSM, you can take a packet capture. This is an example packet capture of a successful connection using a proxy server.

<#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
```

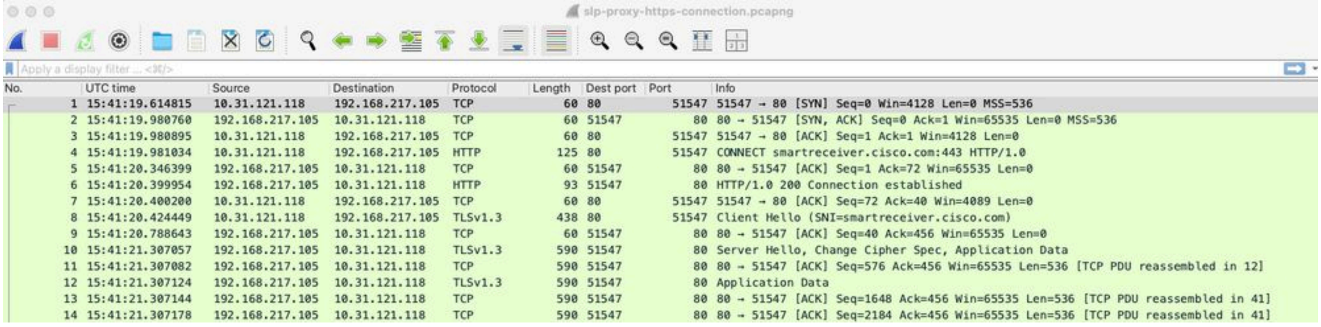
```
  ARPA   Vlan10
```

```
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
```


slp-proxy-https-connection.pcapng
Apply a display filter ... <⌘/>

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	15:41:21.307057	192.168.217.105	10.31.121.118	TLSv1.3	590	51547	80	Server Hello, Change Cipher Spec, Application Data
11	15:41:21.307082	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]

Packet Capture of Successful HTTPS Connection with CSSM Using a Proxy Server.

6. If the packet capture shows that the HTTPS connection is attempting to be established but fails, it could be due to a TLS or SSL handshake failure. These debugs can be used for further investigation.

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

7. If at any point the installed trust code needs to be removed from the switch, a Smart Licensing factory reset can be performed. This process requires a reload. After the factory reset, a new trust code can be installed. Using this command removes all licensing information, including the policy.

<#root>

```
Switch#

license smart factory reset


%Warning: reload required after "license smart factory reset" command

Switch#

show license status | include Trust


Trust Code Installed: <none>  <--- Installed trust code now shows none



Switch#

reload
```

Related Information

- [Smart Licensing Using Policy for Cisco Catalyst 9000 Series Switches]
- [Understand Smart Licensing for Catalyst Switching]
- [Cisco Live: Introduction to Smart Licensing Using Policy]
- [Cisco Technical Support & Downloads]