Troubleshoot Smart Licensing Using Policy Issues on 9800

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

- License Usage Reporting
- RUM Reports
- Troubleshoot 9800 Smart Licensing Communication Issues with Directly Connected CSSM and SSM On-prem Server
- Trust Code
- Smart with CSSM
- Smart Using Proxy
- SSM On-Prem
- Smart Transport
- SSM On-Prem

Test Connection to Smart Receiver

Test Connection to SSM On-Prem Server

Look Up Receiver IP Address

How Does Your System Resolve the IP?

- Invalid Trustcode Processed from CSSM
- Valid Trustcode Processed from CSSM

Communication Frequency

Errors Reported in the Output of show license eventlog and/or show log

Debug

Related Information

Introduction

This document describes advanced troubleshooting steps on Smart Licensing Using Policy (SLUP) on Catalyst 9800 Wireless LAN Controller.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Smart Licensing Using Policy (SLUP)
- Catalyst 9800 Wireless LAN Controller (WLC)

Components Used

This document is not restricted to specific software and hardware versions.

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



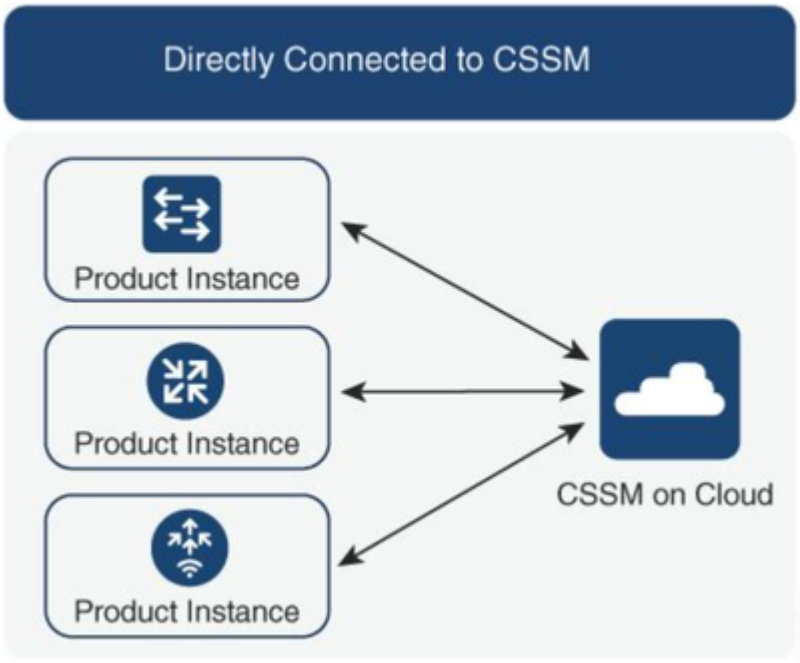
Caution: Caution: Notes in this article contain helpful suggestions or references to material not covered in the document. It is recommended that you read each Note.

- Use: All licenses on Cisco Catalyst Wireless Controllers are unenforced. This means that you do not have to complete any licensing-specific operations, such as registering or generating keys before you start using the software and the licenses that are tied to it. License usage is recorded on your device with timestamps and the required workflows can be completed at a later date.
- Report license usage to CSSM: Multiple options are available for license usage reporting. You can use SSM On-Prem, or Cisco Smart Licensing Utility (CSLU), or report usage information directly to CSSM. For air-gapped networks, a provision for offline reporting where you download usage information and upload it to CSSM, is also available. The usage report is in plain text XML format.

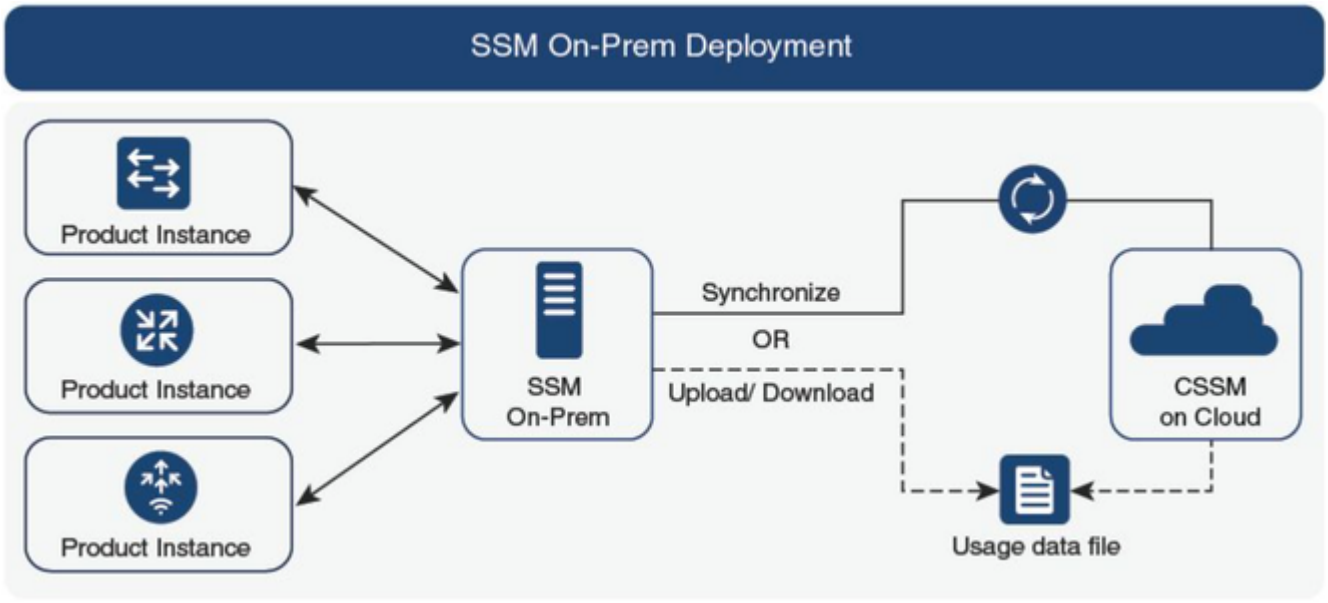
1. Direct connect to Cisco Smart Software Manager Cloud (CSSM)
2. Connected to CSSM via On-prem Smart Software Manager (On-prem SSM)

This article does not cover all the Smart Licensing scenarios on Catalyst 9800, refer to the Smart Licensing Using Policy Configuration Guide for additional information. However, this article does give a series of useful commands to troubleshoot direct connect and SSM On-Prem Smart Licensing Using Policy issues on the Catalyst 9800.

Option 1. Direct connect to Cisco Smart Licensing Cloud Servers (CSSM):



Option 2. Connection via On-prem Smart Software Manager (On-prem SSM):



Note: All commands mentioned in this article are applicable only to WLCs that run version 17.3.2 or later.

License Usage Reporting

With SLP most licenses are not enforced and would be enabled on the device when the feature/technology package gets configured. The corresponding license(s) would appear in **show license summary** as **IN USE**.

```
9800-1#show license summary

Account Information:

  Smart Account: <none>

  Virtual Account: <none>


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
```

The only 2 states available for a license are IN USE or NOT IN USE. The status is solely determined by the configuration and features applied on the Product Instance.

For each license IN USE there is a separate RUM report created. There are states as CLOSED, ACK and OPEN for Rum reports.

Optional: Confirmed with an internal command **test license smart rum-report id** command:

Router(config)# service internal

Router# test license smart rum-report id

report_id:1624247687 state:SmartAgentRumStateOpen

starting from 17.9 versions: the **show license rum id all** command:

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 Reports

RUM reports, or Resource Usage Measurement reports are data files with information about license usage and device identity. These reports are security stored in the device and are cert-signed by the hardware.

The reports change state throughout the communication between product instance and CSSM.

State	Description
SmartAgentRumStateOpen	New report created by Smart Agent on the device
SmartAgentRumStateClosed	RUM report sent to CSSM (reloads would also push the open reports to closed state)
SmartAgentRumStateUnacknowledged	RUM report pending acknowledgement from CSSM, poll ID provided
SmartAgentRumStateAcknowledged	RUM report sent to CSSM and got acknowledged for it

The Smart Licensing Using Policy feature has been introduced to the Catalyst 9800 with the code version 17.3.2. The initial 17.3.2 release misses SLUP configuration menu in the WLC webUI, which was introduced with the 17.3.3 release. The SLUP is different from traditional smart licensing in couple of ways:

- WLC now communicates with CSSM through the smartreceiver.cisco.com domain, instead of the tools.cisco.com.
- Instead of Registering, the WLC now Establishes Trust with the CSSM or SSM On-Prem.
- CLI commands have been slightly altered.
- Smart Licensing Reservation (SLR) no longer exists. Instead you can periodically report your usage manually.
- Evaluation mode no longer exists. The WLC continues to function at full capacity even without license. The system is honor-based and you are supposed to report your license usage periodically (automatically or manually in case of air-gapped networks).

Note: Warning: If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement that starts with Cisco IOS® XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller.

Troubleshoot 9800 Smart Licensing Communication Issues with Directly Connected CSSM and SSM On-prem Server

* A brand new 9800 controller must adhere to certain procedure for smart licensing workflow to get completed.

1. Create a token from CSSM portal and import the token to establish a trust id required to get authorization for license usage reporting in future. This trust id value is the key for CSSM in order to validate the report submitted from 9800 controller. This trustid token would get refreshed periodically and exchanged as part of Rum usage reporting with CSSM.

Note: Starting with Cisco IOS XE Cupertino 17.7.1, a trust code is required. Trust code is established per serial number and so 9800 HA SSO setup would have 2 trustcode installed.

Trust Code

A UDI-tied public key, which the product instance uses to:

- Sign a RUM report. This prevents tampering and ensures data authenticity.
- Enable secure communication with CSSM.

From Cisco IOS XE Cupertino 17.7.1, a trust code is automatically obtained in topologies where the product instance initiates the sending of data to CSLU and in topologies where the product instance is in an air-gapped network.

- A trust code can obtained from CSSM, using an ID token.

  Here you generate an ID token in the CSSM Web UI to obtain a trust code and install it on the product instance. You must overwrite the factory-installed trust code if there is one. If a product instance is directly connected to CSSM, use this method to enable the product instance to communicate with CSSM in a secure manner. This method of obtaining a trust code is applicable to all the options of directly connecting to CSSM. For more information, see Connected Directly to CSSM.

From Cisco IOS XE Cupertino 17.9.1, a trust code is automatically obtained in topologies where CSLU initiates the retrieval of data from the product instance.

If there is a factory-installed trust code, it is automatically overwritten. A trust code obtained this way can be used for secure communication with CSSM.

* Make sure configuration on 9800 for smart licensing is intact. 9800 uses Smart as transport to communicate with CSSM.

Smart with CSSM

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

Smart Using Proxy

license smart proxy { address address_hostname| port port_num} Device(config)#license smart url default Device(config)#license smart proxy address <proxy ip/fqdn> Device(config)#license smart proxy port <proxy port>

SSM On-Prem

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

Ensure the domain lookup and name-server are reachable via source interface.

Device(config)#ip domain name <domain-name> Device(config)#ip name server <dns-server> Device(config)#ip domain lookup

show license all command returns Transport type and URL details configured on 9800:
Ensure configuration is absolute.

Smart Transport

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

SSM On-Prem

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

* if there is any proxy between 9800 and CSSM, make sure to allow the listed IP address on proxy for seamless communication.

Test Connection to Smart Receiver

Use the curl command from a unix-based device to test the Smar Licensing access (but that device is potentially not in the same subnet and having the same access rescritions as the 9800):

- curl https://smartreceiver.cisco.com/licservice/license
- Expected response: This is the Smart Receiver!

Test Connection to SSM On-Prem Server

Use the curl command from a unix-based device to test the Smar Licensing access (but that device is potentially not in the same subnet and having the same access rescritions as the 9800):

- curl -v -k https://SSM-Onprem-FQDN-address>/cslu/v1/pi/ssmsfloodingslup2304-1
- Expected response: This is the Smart Receiver!

Look Up Receiver IP Address

Use this **nslookup** commandfrom your laptop:

- nslookup smartreceiver.cisco.com

Expected response:

- Server: 171.70.168.183 ← This is the DNS server
- Server: dns-sj.cisco.com ← Optionally this can be displayed
- Address: 10.10.10.10#53
- Name: smartreceiver.cisco.com
- Address: 146.112.59.81
- Name: smartreceiver.cisco.com
- Address: 2a04:e4c7:fffe::f

How Does Your System Resolve the IP?

Use the **dig** command from your laptop:

- dig smartreceiver.cisco.com + short

Expected result

- 146.112.59.81

Note: The Smart Receiver component at CSSM has replaced old tools.cisco.com and single point of contact for Rum reporting, Registration, Billing for MSLA customers.

---

ip http client source-interface <source-interface>

This command explicitly marks the source path to CSSM.

ip http client secure-trustpoint SLA-TrustPoint

Ensure **secure-trustpoint** is selected as SLA-TrustPoint as this is signed by Licensing Root CA. Both SSM On-Prem and CSSM is trusted by Licensing Root CA certificate.

CA Certificate:

Status: Available

Certificate Serial Number (hex): 01

Certificate Usage: Signature

Issuer:

cn=Cisco Licensing Root CA

o=Cisco

Subject:

cn=Cisco Licensing Root CA

o=Cisco

Validity Date:

start date: 19:48:47 UTC May 30 2013

end date: 19:48:47 UTC May 30 2038

Associated Trustpoints: Trustpool SLA-TrustPoint

Storage: nvram:CiscoLicensi#1CA.cer

License smart sync all is the command to initiate fresh Rum report from 9800 controller and XML format. When this command is issued on the controller where trust code is not installed on 17.9.x version, it first generates a request for the trustcode rather than Rum usage report.

Invalid Trustcode Processed from CSSM

Import TRUST CODE:

Received on Sep 17 17:35:26 2024 UTC

<smartLicenseTrust><trustCode><udi>P:C9800-L-F-K9,S:FCL2630000P</udi><status><success>false</success><message>A trust request corresponding to higher trust-id has already been processed for this device.</message><code>OLD_TRUST_ID</code><correlationID>null-null</correlationID></status></trustCode><signature>MEQCIAg71/hlcWxUiiof8VstpmPhRH8jptPZPrvaSpsuwVg

CSSM is expecting the controller to send incrementatl trustcode id as a security purpose and the implication of invalid trust code would stop CSSM to process the licensing RUM requests from controller. This would eventually result in license management issue on CSSM licensing dashabord.

Valid Trustcode Processed from CSSM

Import TRUST CODE:

<smartLicenseTrust><trustCode><udi>P:C9800-L-F-K9,S:XXXXXXXXX</udi><customerInfo><smartAccount>Cisco Demo Internal Smart Account</smartAccount><virtualAccount>0Demo-HK-PartnerA</virtualAccount></customerInfo><piid>0eb1d627-bbed-46a8-9a4b-fc5b48a7c36b</piid><dateStamp>2024-09-10T07:21:30</dateStamp></subCA><trustId>110</trustId><status><success>true</success><correlationID>null-null</correlationID></status></trustCode><signature>MEUCIGMPyt6VEmv/DMziybLDnsHRZAxfl9r1vI3BBNtr

Communication Frequency

The reporting interval you can configure in CLI or GUI has no effect.

The 9800 WLC communicates with CSSM or On-prem Smart Software Manager every 8 hours, no matter what reporting interval is configured via web interface or CLI. This means that newly joined access points can appear on the CSSM up to 8 hours after they initially joined.

You can figure out the next time licenses are calculated and reported with the show license air entities summary command. This command is not part of the typical show tech or show license all output:

show license air entitiessummary command**:**

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

Post trustcode is installed successfully on 9800 controller, the next phase is to generate the usage report of license activity via Rum (Resouce Measurement Unit) in XML format. License smart sync all/local command would initiate or generate or open new Rum measurement based on AP managed in controller. Basically, 9800 smart agent component sends an API call to licensing module to collect new Rum report with licensing information.

show license rum id all command**:**

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 command**:**

You can get details of the license reported in Rum id. This command pulls the software_identifier_tag which is the key matching element on CSSM database to validate a license type from a product instance.

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

Smart Licensing Usage Report Detail:

==========

Report Id: 1719005447

Metric Name: ENTITLEMENT

Feature Name: air-network-advantage

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

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

Previous Report Id: 1719005445, Next Report Id: 0

State: OPEN, State Change Reason: None

Close Reason: None

Start Time: Sep 10 10:00:08 2024 UTC, End Time: Sep 16 16:15:08 2024 UTC

Storage State: EXIST

Transaction ID: 0

Transaction Message: <none>

* Now, Rum report is generated. In OPEN state, it must be submitted to CSSM successfully to receive the ACK from the CSSM.

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

Errors Reported in the Output of show license eventlog and/or show log

"Communications failure with the Cisco Smart License Utility (CSLU) : No detailed information given"

This error can be observed when the HTTPS communication with On-Prem was not established. Potential reasons:

- A specific VRF is used for communication with OnPrem. The HTTP client source interface must be configured manually

- Revocation check is NOT disabled under the SLA-Trustpoint configuration

- Another trustpoint is set as the default for crypto signalling (for example: on the SIP gateway)

"HTTP Server Error 502: Bad Gateway"

This error is currently under investigation by the On-Prem development team. In most cases there is no service impact observed.

Typically, 10 seconds later, **SAEVT_COMM_RESTORED**.

Example:

Jul 9 13:15:29.902: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart License Utility (CSLU) : HTTP Server Error 502: Bad Gateway
Jul 9 13:15:39.881: %SMART_LIC-5-COMM_RESTORED: Communications with Cisco Smart License

Utility (CSLU) restored

"HTTP Server Error 404: Not Found"

This error is observed on the Cisco IOS XE device when there was an attempt to install the Trust Code while the transport URL was pointing to the On-Prem (CSLU).

The command "license smart trust idtoken <token> [all|local]" is used ONLY when the device communicates directly with CSSM.

NOTE: Depending on the platform this message can also mean that the "Validate Device" setting is turned on in the CSLU settings panel in the On-Prem Admin Workspace. Check to see if the device you are trying to register is located in the "SL Using Policy" tab of the On-Prem sever. If the devices is not in that tab then you need to turn this toggle off. Then try to have the device sync with the On-Prem server again. For a picture of this setting, refer to the end of this article.

SAEVT_INIT_CRYPTO success="False" error="Crypto Initialization has not been completed"

This error can be observed shortly after the system boots. After about 30 seconds the crypto initialization is completed - in such case there is no service impact.

Example:

2021-06-25 10:09:23.378 UTC SAEVT_INIT_SYSTEM_INIT
2021-06-25 10:09:24.383 UTC SAEVT_INIT_CRYPTO success="False" error="Crypto Initialization has not been completed"
2021-06-25 10:09:54.383 UTC SAEVT_INIT_CRYPTO success="True"

If the crypto initialization does not complete for several minutes/hours, verify if the NTP configuration is present and/or clocks are synced. Saving running configuration helps to restart the crypto initialization.

It is recommended to investigate further with Cisco TAC if the problem persists.

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

Most likely, the "Validate Device" setting is set in the CSLU settings panel in the On-Prem Admin Workspace.

This setting helps ensure the RUM reports from known product instances are being received.

SAEVT_COMM_FAIL error="Unable to resolve server hostname/domain name"

This error indicates a connectivity issue that can originate with DNS resolution. You must ensure that the device can resolve the destination URL. Usually the **ip host <url> <ipassociated>** command is misconfigured. Please check this point.

Most probably you would find communication failure.

Communication Statistics:

==========

Communication Level Allowed: INDIRECT

Overall State: <empty>

Trust Establishment:

Attempts: Total=30, Success=0, Fail=30 Ongoing Failure: Overall=30 Communication=30 <<<<<<<<<<

Last Response: NO REPLY on Feb 12 10:52:56 2023 GMT <<<<<<<<<<

Failure Reason: <none>

Last Success Time: <none>

Last Failure Time: Feb 12 10:52:56 2023 GMT

Communication Level Allowed as INDIRECT means the required trustcode is not installed successfully on the 9800 controller.

Note: Note: CSSM is the source of truth of all licensing data.

---

* If basic communication issue between 9800 and CSSM is mitigated by performing the test, enable debug on certain modules involved for smart licensing communications. Enabling debug on 9800 would spike CPU for certain time interval and hence must perform these actions during off business hours.

Debug

* There are 4 modules which are involved in smart licensing communication from 9800 to CSSM or SSM On-Prem

1. Crypto module

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 module

HTTP Server:

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 module

ssl openssl:

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

4. The smart licensing module is called as a smart agent, including the transport gateway

License:

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

Syslogs:

server identity check and SAN validation on the certificate. Trustpoint validation from crypto SSL library.

Sep 16 16:29:12.236: Server identity check with host: 10.106.43.37

Sep 16 16:29:12.236: Server identity to verify is ip address 10.106.43.37 len 12

Sep 16 16:29:12.329: CRYPTO_PKI: (A645F) Check for identical certs

Sep 16 16:29:12.329: CRYPTO_PKI(Cert Lookup) issuer="cn=Cisco Licensing Root CA,o=Cisco" serial number= 0F 42 40

Sep 16 16:29:12.329: CRYPTO_PKI: (A645F) Suitable trustpoints are: SLA-TrustPoint,Trustpool6,Trustpool6,

Sep 16 16:29:12.329: CRYPTO_PKI: (A645F) Attempting to validate certificate using SLA-TrustPoint policy

Sep 16 16:29:12.329: CRYPTO_PKI: (A645F) Using SLA-TrustPoint to validate certificate

Sep 16 16:29:12.345: SSL_connect:SSL negotiation finished successfully

Sep 16 16:29:12.345: SSL_connect:SSL negotiation finished successfully

Once Usage report is submitted to CSSM, you must see successfully update on show license history message command:

Requests would have component like UDI_SERIAL_NUMBER, hostname, software_tag_identifier which indicate what license mode ls consumed by 9800 controller and request_type as "LICENSE_USAGE"

There are multiple license types present:

1. ID_TOKEN_TRUST

2. TRUST_SYNC

3. LICENSE_USAGE

Usage Reporting:

REQUEST: Sep 16 16:30:16 2024 UTC

"{\"sender_info\":{\"connect_info\":{\"name\":\"C_agent\",\"version\":\"5.8.6_rel/15\",\"production\":true,\"addition
L-F-
K9\",\"udi_serial_number\":\"FCL2630000P\"},\"product_instance_identifier\":\"\",\"software_tag_identifier\":\"reg
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\":\"17.12.02\",\"hostname\":\"renjith-
eap-
test\",\"role\":\"Active\",\"request_type\":\"ID_TOKEN_TRUST\",\"request_line_id\":1,\"smart_license\":

Usage Reporting:

REQUEST: Sep 16 16:30:16 2024 UTC

"{\"sender_info\":{\"connect_info\":{\"name\":\"C_agent\",\"version\":\"5.8.6_rel/15\",\"production\":true,\"addition
L-F-
K9\",\"udi_serial_number\":\"FCL2630000P\"},\"product_instance_identifier\":\"\",\"software_tag_identifier\":\"reg
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\":\"17.12.02\",\"hostname\":\"renjith-
eap-test\",\"role\":\"Active\",\"request_type\":\"TRUST_SYNC\",\"request_line_id\":1,\"smart_license\":

Usage Reporting:

REQUEST: Sep 16 16:30:16 2024 UTC

{"sender_info":{"connect_info":{"name":"C_agent","version":"5.8.6_rel/15","production":true,"additional_info":"",
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":"17.12.02","hostname":"renjith-eap-
test","role":"Active","request_type":"LICENSE_USAGE","request_line_id":1,"smart_license":

* It is important to understand the response from CSSM or SSM On-Prem:

Error Response packet:

RESPONSE: Sep 16 16:30:16 2024 UTC

{

"status": "FAILED",

"message_code": "ERROR Consuming licenses",

"message": "",

"nonce": "77709655117429624"

}

The error indicates that there has been already an entry for the controller in CSSM or SSM On-Prem licensing server which is denying the addition of new record in the database. One must delete the active or stale record from CSSM or SSM On-Prem and re submit Rum report.

Valid Response Poll_id :

RESPONSE: Sep 16 16:29:14 2024 UTC

{

"sender_info": {

"connect_info": {

"name": "CSLU_V1",

"version": "v1",

"production": true,

"additional_info": "",

"capabilities": [

"UTILITY",

"DLC",

"AppHA",

"MULTITIER",

"EXPORT_2",

"OK_TRY_AGAIN",

"POLICY_USAGE",

```
      "CSLU_V1",
      "CSLU_V2",
      "TELEMETRY"
    ]
  },
  "timestamp": 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"
 },
 "status": "COMPLETE",
 "license_data": [
  {
    "status": "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": ""
  }
 ]
}
```


* How to validate poll_id is stored in 9800 local database and how often it polls to get an ACK for the Rum report submitted.

Test command to validate need to get activated via service internal.

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

* As you can understand from the explanation that initial requests submitted by 9800 controller would always be Trust code token and without it, 9800 controller would never generate new Rum usage report and hence license usage change cannot be submitted on CSSM.

* A sample requests poll_id for License_usage.

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

* if there is already an ACK processed in CSSM or SSM On-Prem database, you can force the smart agent on the 9800 controller to poll and get ACK at the earliest without waiting for the time mentioned

in the poll_id cycle.

```
WLC#test license smart  conversion sched_poll 5583279046281676962 ?

  <0-4294967295>  delta Time in Seconds
```

Related Information

- Configure Offline (Air Gapped) Licensing on 9800 WLC
- Cisco Technical Support & Downloads
- Configure Catalyst 9800 WLC Smart Licensing Using Policy with DNA Center