Revised: December 15, 2025

SLP Troubleshooting, System Messages, and FAQs

Overview

This article provides information about system messages and troubleshooting related to Smart Licensing using Policy (SLP) on Nexus switches along with frequently asked questions (FAQs).

Troubleshooting Smart Licensing Using Policy

The troubleshooting section is further divided into two sections that provide step-by-step instructions to resolve SLP issues on Nexus switches.

- Resolving SLP issues on Nexus switches—This section covers the common problems and solutions related to connectivity of switch to CSSM.
- Resolving SLP system messages—This section provides a list of SLP-related system messages you may encounter, possible reasons for failure, and recommended action.

Resolving SLP issues on Nexus switches

This section provides information about common problems related to connectivity of switch to CSSM and their resolution.

The issues covered in this section are:

- Trust code installation failed
- Smart Licensing communication with CSSM/CSLU/SSM On-Prem failed
- Failed to send usage Report
- Failed to get Report Acknowledgment

Trust code installation failed

Possible reasons for failure include:

- A trust code is already installed: Trust codes are linked to the **Unique Device Identifier** (UDI) of the product instance. If the UDI is already registered, and you try to install another one, installation fails.
- Timestamp mismatch: This means the product instance time is not in sync with **Cisco Smart Software Manager** (CSSM), and can cause installation to fail.

Recommended Action:

- A trust code is already installed: If you want to install a trust code in spite of an existing trust code on the product instance, re-configure the **license smart trust idtoken** *id_token_value* [**force**] command in privileged EXEC mode, and be sure to include the **force** keyword. Entering the **force** keyword asks CSSM to create a new trust code even if it exists already.
- Timestamp mismatch: Configure the **ntp server** command in global configuration mode. For example:

  switch (config)# **ntp server 10.28.13.90 prefer**

Note

If there is a difference in time between device and CSSM then it should be less than one hour.

Smart Licensing communication with CSSM/CSLU/SSM On-Prem failed

Possible reasons for failure include:

- Missing DNS configurations.
- CSSM, CSLU, SSM On-Prem is not reachable: This means that there may be network problem.

Recommended Action for DNS:

Troubleshooting steps are provided for missing DNS configurations, when CSSM/CSLU/SSM On-Prem is not reachable.

- If ping to cisco.com in the configured vrf for SLP throws error `% Invalid host/interface <URL>`:

1. Execute these commands from global configuration mode to configure DNS.

```
switch# config terminal
switch(config)# ip domain-lookup
switch(config)# ip domain-name cisco.com
switch(config)# ip name-server <dns-server-ip> use-vrf <vrf-name>
switch(config)# vrf context <vrf-name>
switch(config-vrf)# ip domain-name cisco.com
switch(config-vrf)# ip name-server <dns-server-ip>
```

2. Check if ping to cisco.com is working or not, using **vrf** <*vrf-name*>. This example shows working DNS scenario.

```
switch(config)# ping cisco.com vrf <vrf-name>
PING cisco.com (<ip-address>): 56 data bytes
64 bytes from <ip-address>: icmp_seq=0 ttl=236 time=242.279 ms
64 bytes from <ip-address>: icmp_seq=1 ttl=236 time=242.108 ms
64 bytes from <ip-address>: icmp_seq=2 ttl=236 time=242.032 ms
64 bytes from <ip-address>: icmp_seq=3 ttl=236 time=242.278 ms
64 bytes from <ip-address>: icmp_seq=4 ttl=236 time=241.968 ms
--- cisco.com ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 241.968/242.133/242.279 ms
```

Note

For transport mode CSLU, either configure **ip host cslu-local** <*cslu_address*> or cslu-local should be part of DNS server. For SSM On-Prem, the URL configured in switch should be **Fully Qualified Domain Name** (FQDN) and not the ip-address.

Recommended action for network reachability

- If the configured transport mode is **smart** transport:

1. In the **show license status** command output, under the `Transport:` header, check the following:
   a. `Type:` must be **Smart** and
   b. `URL:` must be https://smartreceiver.cisco.com/licservice/license. For example,

```
Transport:

Type: Smart
```

`URL:` https://smartreceiver.cisco.com/licservice/license

`Proxy:` Not configured

`VRF:` <*vrf-name*>

If it is not, configure using the **license smart transport smart** and **license smart url smart** https://smartreceiver.cisco.com/licservice/license commands in global configuration mode.

2. Check DNS resolution. Verify that the URL https://smartreceiver.cisco.com/licservice/license is reachable through the browser. This example shows reachability for the smart URL.

```
This is the Smart Receiver!

Environment Information:
  cisco.life = prod
  License Engine = https://swapi.cisco.com/software/csws/ssm/services
  License EngineSLE = https://swapi.cisco.com/software/csws/ssm/v2/services
  License Crypto Service = https://lcs.cisco.com/LCS
  Crypto Enabled = true
  Retry Enabled = true
  Retry Timeout = 55000
  Rate Limit Window Length = 3600
  Rate Limit Max Allowed in Window = 12
```

Optionally, you can ping smart URL (https://smartreceiver.cisco.com/licservice/license) and verify.

Example

```
bash-4.4$ ping smartreceiver.cisco.com
PING smartreceiver.cisco.com (<ip-address>) 56(84) bytes of data.
64 bytes from <ip-address> (<ip-address>): icmp_seq=1 ttl=53 time=2.57 ms
64 bytes from <ip-address> (<ip-address>): icmp_seq=2 ttl=53 time=2.79 ms
64 bytes from <ip-address> (<ip-address>): icmp _seq=3 ttl=53 time=2.54 ms
64 bytes from <ip-address> (<ip-address>): icmp_seq=4 ttl=53 time=2.43 ms
64 bytes from <ip-address> (<ip-address>): icmp_seq=5 ttl=53 time=3.23 ms
64 bytes from <ip-address> (<ip-address>): icmp_seq=6 ttl=53 time=2.100 ms
^C
--- smartreceiver.cisco.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 2.429/2.757/3.231/0.289 ms
bash-4.4$
```

- If the configured transport mode is **cslu**:

1. In the **show license status** command output, under the `Transport:` header, check the following:

   a. `Type:` must be CSLU and

   b. `Cslu address:` must be cslu-local

   Example

   ```
   Transport:

   Type: CSLU

   Cslu address: cslu-local

   VRF: <vrf-name>
   ```

   If it is not, configure using the **license smart transport cslu** and **license smart url cslu** <*cslu-local-url*> commands in global configuration mode.

2. Check DNS resolution. Verify that the configured cslu-local-url is reachable through the browser.

- If the configured transport mode is callhome,

1. in the **show license status** command output, under the `Transport:` header, check the following:

   - `Type:` must be Callhome.

     For example,

     ```
     Transport:

     Type: Callhome
     ```

     If it is not, configure using the **license smart transport callhome** command in global configuration mode.

2. Check if callhome is configured correctly. Use the **show running-config callhome all** command in privileged EXEC mode, to check callhome configuration as shown in this example.

```
switch(config)# show running-config callhome all
!Command: show running-config callhome all
!Running configuration last done at: Thu Aug  3 20:38:37 2023
!Time: Thu Aug  3 20:43:58 2023
version 10.3(1) Bios:version 05.45
callhome
  email-contact <email-address>
  destination-profile xml transport-method http
  destination-profile xml index 1 email-addr <email-address>
  destination-profile xml index 1 http https://tools.cisco.com/its/service/oddce/services/DDCEService
  transport email smtp-server <ip-address> port <port-number>
  transport email from <email-address>
  transport email reply-to <email-address>
  transport http use-vrf <vrf-name>
  enable
  periodic-inventory notification interval 1
```

3. Check DNS Resolution. Verify that the product instance can ping tools.cisco.com through configured vrf using the **ping tools.cisco.com vrf** <vrf-name> command.

   Example

```
switch(config) # ping tools.cisco.com vrf <vrf-name>
PING tools.cisco.com (<ip-address>): 56 data bytes
64 bytes from <ip-address>: icmp_seq=0 ttl=236 time=244.692 ms
64 bytes from <ip-address>: icmp_seq=1 ttl=236 time=244.532 ms
64 bytes from <ip-address>: icmp_seq=2 ttl=236 time=244.396 ms.
64 bytes from <ip-address>: icmp_seq=3 ttl=236 time=244.502 ms.
64 bytes from <ip-address>: icmp_seq=4 ttl=236 time=244.607 ms

-- tools.cisco.com ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 244.396/244.545/244.692 ms.
switch(config)#
```

   You can also ping directly to the callhome URL tools.cisco.com.

   Example

```
bash-4.4$ ping tools.cisco.com
PING tools.cisco.com (<ip-address>) 56(84) bytes of data.
64 bytes from tools2.cisco.com (<ip-address>): icmp_seq=1 ttl=242 time=43.7 ms
64 bytes from tools2.cisco.com (<ip-address>): icmp_seq=2 ttl=242 time=43.7 ms
64 bytes from tools2.cisco.com (<ip-address>): icmp_seq=3 ttl=242 time=43.7 ms
64 bytes from tools2.cisco.com (<ip-address>): icmp_seq=4 ttl=242 time=43.8 ms
```

```
64 bytes from tools2.cisco.com (<ip-address>): icmp_seq=5 ttl=242 time=43.8 ms
64 bytes from tools2.cisco.com (<ip-address>): icmp_seq=6 ttl=242 time=43.7 ms
^C
--- tools.cisco.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 43.656/43.703/43.770/0.214 ms
bash-4.4$
```

Failed to send usage Report

Possible reasons for failure include:

- Because of a communication failure, the product instance failed to send the RUM report.

Recommended action

- Check if the RUM report is due any time soon using the **show license tech support** command. If not, and the problem is with a server or link that is down, you can try again after some time.
- If the communication failure persists, check if the transport type and URL have been set as required by the topology.

Failed to receive Report Acknowledgment

Possible reasons for failure include:

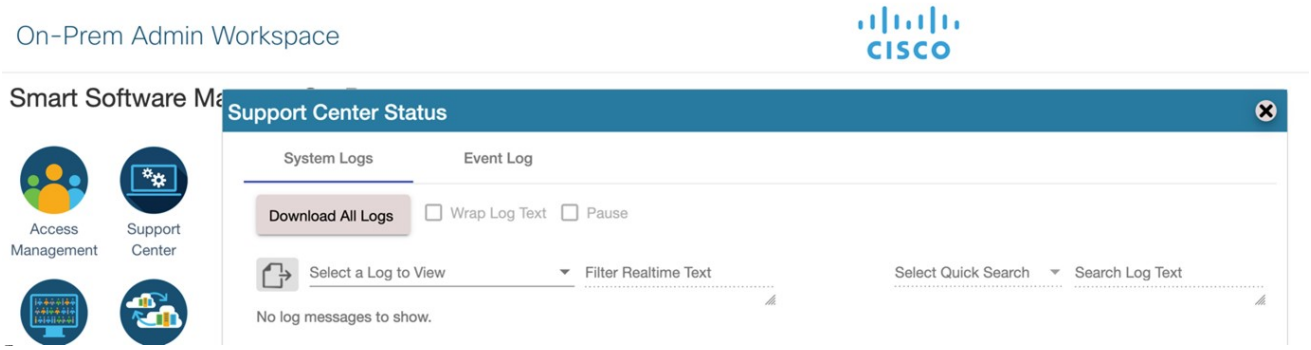
- Connectivity problems. Depending on the implemented topology, this can mean a connectivity problem with CSSM, or CSLU, or SSM On-Prem.
- Delayed communication. There may be a lag between the time that a RUM Report is sent and the RUM acknowledgment (ACK) is available on the product instance. For example, if you use CSLU or SSM On-Prem, the time at which the product instance receives information depends on when CSLU or SSM On-Prem is scheduled to synchronize with CSSM and with the product instance. In direct connectivity mode, acknowledgment takes around 15 minutes to be updated on the switch.
- The ACK received can fail, if the product instance (switch) was previously registered with a different On-Prem account.

  Recommended action

  To troubleshoot this issue, perform these steps:

  1. Navigate to **On-Prem Admin Workspace** > **Support Center**. The **Support Center Status** window opens.
  2. In the **Support Center Status** window, click the **System Logs** tab and click **Download All Logs**. After a few seconds, a dialog window opens to save the zip file.
  3. Save the **AllFiles.zip** file.

4. Extract the **AllFiles.zip**



5. Check for the following symptoms inside the file named **messages** and search for the error:

```
failed due to the following error: record not found.
```

For example,

```
Aug 7 17:02:36 rtp-dcrs-licensing cf881d42a1b7: 2023/08/07
 17:02:36#011[ERROR]#011adapters/pi_routes_impl.go:1322#011
 Finding SL product by UDI {<switch> FDO212100YT} failed due to the following error: record
not found.
```

6. It is also possible that the CSSM does not have the product instance but `On-Prem` has the product instance.

Recommended action

1. Ensure that the trust code is installed.
2. When the trust code is installed, check for `Usage reporting:` in **show license status** to know whether the report is synced or not. The `Next report push:` field displays this information about the synchronization:

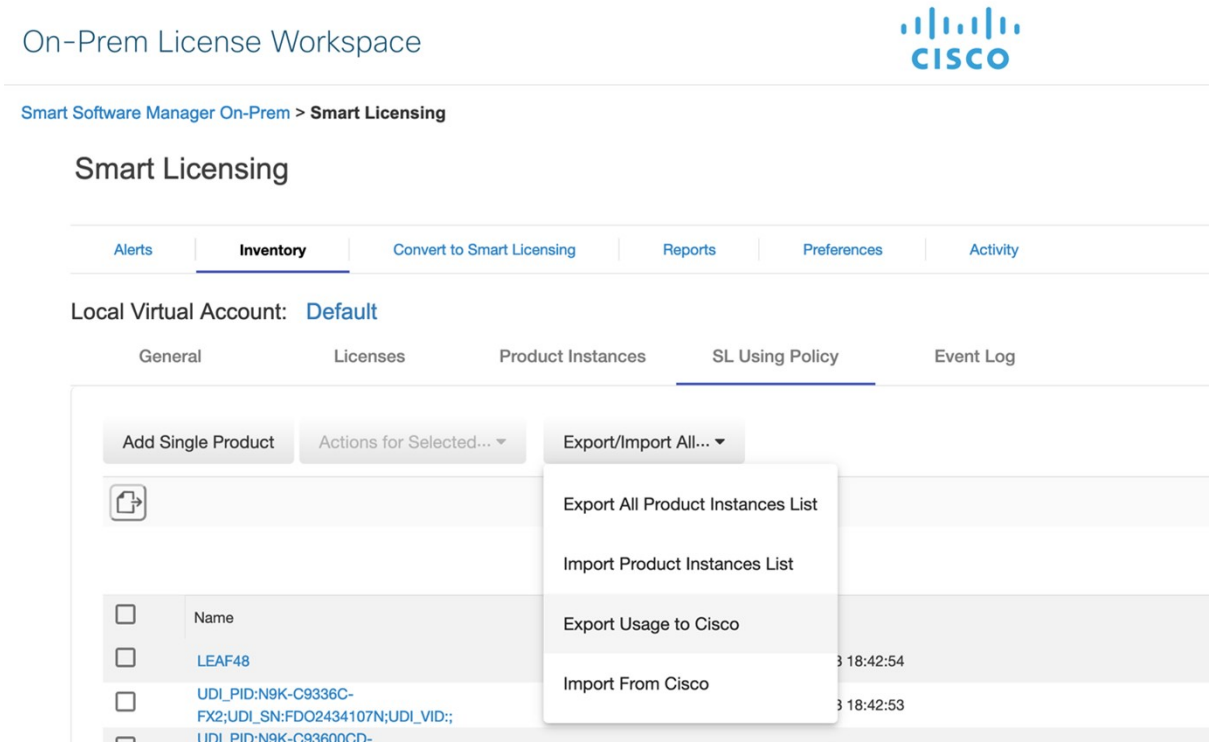
```
Usage reporting:
         Last ACK received: <none>
         Next ACK deadline: <none>
         Reporting push interval: <none>
         Next ACK push check: <none>
         Next report push: <none>
         Last report push: <none>
         Last report file write: <none>
Trust Code installed: Jul 14 11:40:36 2023 UTC
         Active: PID: <device_pid>, SN: <device_sn>
                 Jul 14 11:40:36 2023 UTC
```

3. If the synchronization does not take place automatically, then initiate an on-demand synchronization based on the implemented topology as follows:
   - For online topologies, use the **license smart sync** command in privileged EXEC mode. If SSM On-Prem is used in topology, then, additionally, sync to Cisco as well as the switch on SSM On-Prem.
   - For offline topologies, upload the RUM report to CSSM and install the ACK back on the switch.
4. After the sync is completed, wait for 15 minutes to receive acknowledgment for the CSSM.
5. Perform On-Prem Report Synchronization out-of-band (**Export/Import Cisco Usage Report/ACK**) if acknowledgment fails due to already registered device reason on On-Prem.

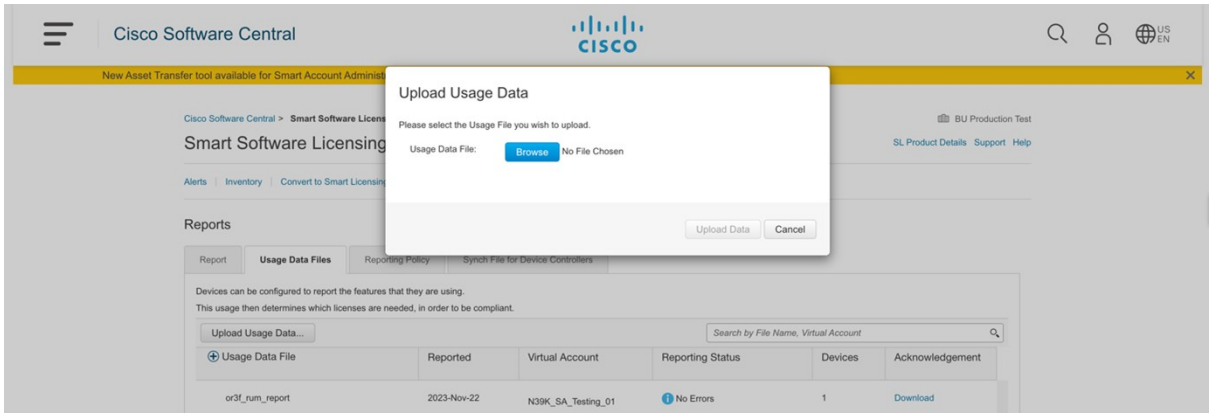
a. On the On-Prem server, navigate to **Smart Software Manager On-Prem** > **Smart Licensing** > **Inventory** > **SL Using Policy**.

Then, select the product names for which you require the acknowledgment.

Next, from the **Export/Import All** drop-down menu, select **Export Usage to Cisco** and download the exported report onto your system.



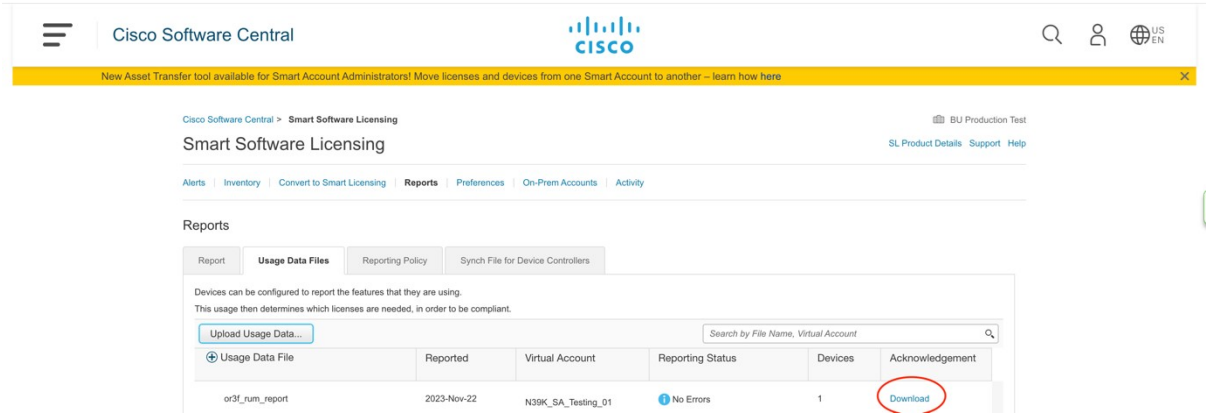
b. To upload the downloaded report and generate the ACK report, go to the respective CSSM On-Prem account and navigate to **Reports** > **Usage Data Files** > **Upload Usage Data File**. Click the **Upload Usage Data** button. The **Upload Usage Data** dialog box opens.



c. In the **Upload Usage Data** dialog box, click the **Browse** button and select the report from your system (downloaded earlier) that you want to upload and then click the **Upload Data** button.

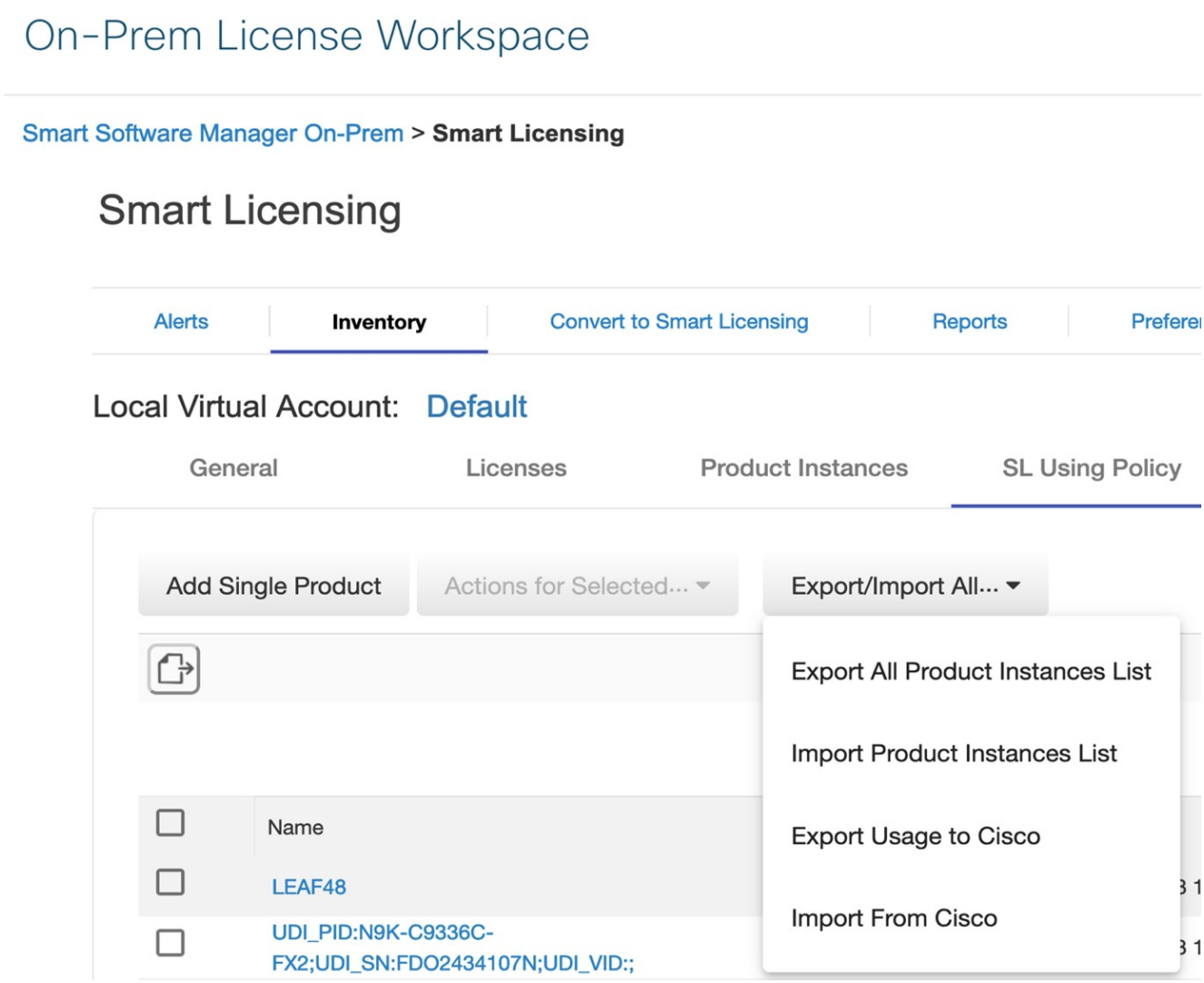
Wait for a while as it takes some time to process. Ignore the errors that appear, if any. The file is uploaded to the **Usage Data Files** tab.

d. To download the ACK report for the uploaded Usage Data File, select the file and click the **Download** link in the **Acknowledgment** column.



e. Upload the downloaded ACK file to On-Prem. To do so, navigate to **Smart Software Manager On-Prem** > **Smart Licensing** > **Inventory** > **SL Using Policy**.

Then, from the **Export/Import All** drop-down menu, select **Import From Cisco** and upload the downloaded acknowledgment report.



f. After the report is uploaded, the respective devices reflect the received acknowledgment status.

Note

Not receiving acknowledgment does not affect any function of the switch. You can receive syslog for not reporting, if the reporting period is expired or near to expiry as per the configured policy. If you do not receive an acknowledgment, you can contact our technical support representative.

System message components

The system software sends system messages to the console (and, optionally, to a logging server on another system). Not all system messages mean problems with your system. Some messages are informational, and others can help diagnose problems with communications lines, internal hardware, or the system software.

How to read system messages

System log messages can contain up to 80 characters. This section provides explanation of how each system message begins with a percent sign (%) and is structured.



%FACILITY

Two or more uppercase letters that show the facility to which the message refers. A facility can be a hardware device, a protocol, or a module of the system software.

SEVERITY

A single-digit code from 0 to 7 that reflects the severity of the condition. The lower the number, the more serious the situation.

Table 1: Message severity levels

Severity Level	**Description**
0 – emergency	System is unusable
1 – alert	Immediate action required
2 – critical	Critical condition
3 – error	Error condition
4 – warning	Warning condition
5 – notification	Normal but significant condition
6 – informational	Informational message only
7 - debugging	Message that appears during debugging only

MNEMONIC

A code that uniquely identifies the message.

Message-text

Message-text is a text string describing the condition. This portion of the message sometimes contains detailed information about the event, including terminal port numbers, network addresses, or addresses that correspond to locations in the system memory address space. Because the information in these variable fields changes from message to message, it is represented here by short strings enclosed in square brackets ([ ]). A decimal number, for example, is represented as [dec].

Table 2: Variable fields in messages

Severity Level	**Description**
[char]	Single character
[chars]	Character string
[dec]	Decimal number
[enet]	Ethernet address (for example, 0000.FEED.00C0)

Severity Level	Description
[hex]	Hexadecimal number
[inet]	Internet address (for example, 192.0.2.16)
[int]	Integer
[node]	Address or node name
[t-line]	Terminal line number in octal (or in decimal if the decimal-TTY service is enabled)
[clock]	Clock (for example, 01:20:08 UTC Tue Mar 2 1993

System messages

This section provides the list of SLP-related system messages you may encounter, possible reasons for failure (in case it is a failure message), and recommended action (if action is required).

For all error messages, if you are not able to solve the problem, contact your technical support representative with the following information:

- The message, exactly as it appears on the console or in the system log.
- The output from the show license tech support and show license history message commands.

SLP-related system messages:

- %LICMGR-3-LOG_SMART_LIC_POLICY_INSTALL_FAILED
- %LICMGR-3-LOG_SMART_LIC_AUTHORIZATION_INSTALL_FAILED
- %LICMGR-3-LOG_SMART_LIC_COMM_FAILED
- %LICMGR-3-LOG_SMART_LIC_COMM_RESTORED
- %LICMGR-3-LOG_SMART_LIC_POLICY_REMOVED
- %LICMGR-3-LOG_SMART_LIC_TRUST_CODE_INSTALL_FAILED
- %LICMGR-4-LOG_SMART_LIC_REPORTING_NOT_SUPPORTED
- %LICMGR-6-LOG_SMART_LIC_POLICY_INSTALL_SUCCESS
- %LICMGR-6-LOG_SMART_LIC_AUTHORIZATION_INSTALL_SUCCESS
- %LICMGR-6-LOG_SMART_LIC_AUTHORIZATION_REMOVED
- %LICMGR-6-LOG_SMART_LIC_REPORTING_REQUIRED
- %LICMGR-6-LOG_SMART_LIC_TRUST_CODE_INSTALL_SUCCESS

Error message

```
%LICMGR-3-LOG_SMART_LIC_POLICY_INSTALL_FAILED: The installation of a new licensing policy
has failed: [chars].
```

Explanation

A policy was installed, but an error was detected while parsing the policy code, and installation failed. [chars] is the error string with details of the failure.

Possible reasons for failure include:

- A signature mismatch: This means that the system clock is not accurate.
- A timestamp mismatch: This means the system clock on the product instance is not synchronized with CSSM.

Recommended action

For both possible failure reasons, ensure that the system clock is accurate and synchronized with CSSM. Configure the ntp server command in global configuration mode. For example:

Device(config)# **ntp server 198.51.100.100 version 2 prefer**

If the above does not work and policy installation still fails, contact your technical support representative.

Error message

```
%LICMGR-3-LOG_SMART_LIC_AUTHORIZATION_INSTALL_FAILED: The install of a new licensing
authorization code has failed on [chars]: [chars].
```

This message is not applicable to Nexus Switches, because there are no enforced or export-controlled licenses on these product instances.

Error message

```
%LICMGR-3-LOG_SMART_LIC_COMM_FAILED: Communications failure with the [chars] : [chars]
```

Explanation

Smart Licensing communication either with CSSM or with CSLU failed. The first [chars] is the currently configured transport type, and the second [chars] is the error string with details of the failure. This message appears for every communication attempt that fails.

Possible reasons for failure include:

- CSSM or CSLU is not reachable: This means that there is a network reachability problem.
- 404 host not found: This means that the CSSM server is down.

For topologies where the product instance initiates the sending of RUM reports (Connected to CSSM Through CSLU: Product Instance-Initiated Communication, Connected Directly to CSSM, and CSLU Disconnected from CSSM: Product Instance-Initiated Communication) if this communication failure message coincides with scheduled reporting (**license smart usage interval** `interval_in_days` global configuration command), the product instance attempts to send out the RUM report for up to four hours after the scheduled time has expired. If it is still unable to send out the report (because the communication failure persists), the system resets the interval to 15 minutes. Once the communication failure is resolved, the system reverts the reporting interval to the value that you last configured.

Recommended action

Troubleshooting steps are provided for when CSSM is not reachable and when CSLU is not reachable. If CSSM is not reachable and the configured transport type is smart:

1. Check if the smart URL is configured correctly. Use the **show license status** command in privileged EXEC mode, to check if the URL is exactly as follows: https://smartreceiver.cisco.com/licservice/license . If it is not, reconfigure the **license smart url smart** `smart_URL` command in global configuration mode.
2. Check DNS resolution. Verify that the product instance can ping smartreceiver.cisco.com or the nslookup translated IP. The following example shows how to ping the translated IP:

```
Device# ping 198.51.100.100 Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.51.100.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

If CSSM is not reachable and the configured transport type is **callhome** :

1. Check if the URL is entered correctly. Use the **show license status** command in privileged EXEC mode, to check if the URL is exactly like https://tools.cisco.com/its/service/oddce/services/DDCEService .
2. Check if Call Home profile **CiscoTAC-1** is active and destination URL is correct. Use the **show call-home profile all** command in privileged EXEC mode:

   ```
   Current smart-licensing transport settings: Smart-license messages: enabled
   Profile: CiscoTAC-1 (status: ACTIVE)
   Destination  URL(s): https://tools.cisco.com/its/service/oddce/services/DDCEService
   ```
3. Check DNS Resolution. Verify that the product instance can ping tools.cisco.com, or the nslookup translated IP.

   ```
   Device# ping tools.cisco.com Type escape sequence to abort.
   Sending 5, 100-byte ICMP Echos to 198.51.100.100, timeout is 2 seconds:
   !!!!!
   Success rate is 100 percent (5/5), round-trip min/avg/max = 41/41/42 ms
   ```

   If the above does not work check the following: if the product instance is set, if the product instance IP network is up. To ensure that the network is up, configure the **no shutdown** command in interface configuration mode.

   Check if the device is subnet that is masked with a subnet IP, and if the DNS IP is configured.
4. Verify that the HTTPs client source interface is correct.

   Use the **show ip http client** command in privileged EXEC mode to display current configuration. Use **ip http client source-interface** command in global configuration mode to reconfigure it. In case the above does not work, double-check your routing rules, and firewall settings.

If CSLU is not reachable:

- Check if CSLU discovery works.
  - Zero-touch DNS discovery of cslu-local or DNS discovery of your domain.

    In the **show license all** command output, check if the Last ACK received: field. If this has a recent timestamp, it means that the product instance has connectivity with CSLU. If it is not, proceed with the following checks:

    Check if the product instance can ping **cslu-local** . A successful ping confirms that the product instance is reachable.

    If the above does not work, configure the name server with an entry where hostname **cslu-local** is mapped to the CSLU IP address (the Windows host where you installed CSLU). Configure the **ip domain name** domain-name and **ip name-server** server-address commands in global configuration mode. Here the CSLU IP is 192.168.0.1 and name-server creates entry **cslu-local.example.com** :

    ```
    Device(config)#
    ip domain name example.com
    ```

    ```
    Device(config)#
    ip name-server 192.168.0.1
    ```

- CSLU URL is configured.

  In the **show license all** command output, under the **Transport:** header check the following: The **Type:** must be **cslu** and **Cslu address:** must have the hostname or the IP address of the Windows host where you have installed CSLU. Check if the rest of the address is configured as shown below and check if the port number is 8182.

  ```
  Transport:
  Type: cslu
  Cslu address: http://192.168.0.1:8182/cslu/v1/pi
  ```

  If it is not, configure the **license smart transport cslu** and **license smart url cslu** *http://<cslu_ip_or_host>:8182/cslu/v1/pi* commands in global configuration mode.

If the above does not work and policy installation still fails, contact your technical support representative.

Error message

```
%LICMGR-3-LOG_SMART_LIC_COMM_RESTORED: Communications with the [chars] restored. [chars] - depends on the
transport type
-  Cisco Smart Software Manager (CSSM)
-  Cisco Smart License utility (CSLU)
Smart Agent communication with either the Cisco Smart Software Manager (CSSM) or the Cisco Smart License
utility (CSLU) has been restored. No action required.
```

Explanation

Product instance communication with either the CSSM or CSLU is restored.

Recommended action

No action required.

Error message

```
%LICMGR-3-LOG_SMART_LIC_POLICY_REMOVED: The licensing policy has been removed.
```

Explanation

A previously installed licensing policy has been removed. The default policy is then automatically effective. This may cause a change in the behavior of smart licensing.

Possible reasons for failure include:

If you have entered the **license smart factory reset** command in privileged EXEC mode all licensing information including the policy is removed.

Recommended action

If the policy was removed intentionally, then no further action is required.

If the policy was removed inadvertently, you can reapply the policy. Depending on the topology you have implemented, follow the corresponding method to retrieve the policy:

- Connected Directly to CSSM:

  Enter **show license status** , and check field **Trust Code Installed:** . If trust is established, then CSSM will automatically return the policy again. The policy is automatically re-installed on product instances of the corresponding Virtual Account.

  If trust has not been established, complete these tasks: See the *Generating a New Token for a Trust Code from CSSM* and *Installing a Trust Code* topics in Common Tasks for Configuring Smart Licensing Using Policy . When you have completed

these tasks, CSSM will automatically return the policy again. The policy is then automatically installed on all product instances of that Virtual Account.

- Connected to CSSM Through CSLU:
  - For product instance-initiated communication), enter the **license smart sync** command in privileged EXEC mode. The synchronization request causes CSLU to push the missing information (a policy or authorization code) to the product instance.
- CSLU Disconnected from CSSM:
  - For product instance-initiated communication), enter the **license smart sync** command in privileged EXEC mode. The synchronization request causes CSLU to push the missing information (a policy or authorization code) to the product instance. Then complete these tasks in the given order: *Download All For Cisco (CSLU Interface)* > *Uploading Usage Data to CSSM and Downloading an ACK* > *Upload From Cisco (CSLU Interface)*. See the *Uploading Usage Data to CSSM and Downloading an ACK* task in Common Tasks for Configuring Smart Licensing Using Policy . .
- No Connectivity to CSSM and No CSLU

  If you are in an entirely air-gapped network, from a workstation that has connectivity to the internet and CSSM complete this task: See the *Downloading a Policy File from CSSM* and *Installing a a File on the Switch* topics in Common Tasks for Configuring Smart Licensing Using Policy .

Error message

```
%LICMGR-3-LOG_SMART_LIC_TRUST_CODE_INSTALL_FAILED: The install of a new licensing trust
code has failed on [chars]: [chars].
```

Explanation

Trust code installation has failed. The first [chars] is the UDI where trust code installation was attempted. The second [chars] is the error string with details of the failure.

Possible reasons for failure include:

- A trust code is already installed: Trust codes are node-locked to the UDI of the product instance. If the UDI is already registered, and you try to install another one, installation fails.
- Smart Account-Virtual Account mismatch: This means the Smart Account or Virtual Account (for which the token ID was generated) does not include the product instance on which you installed the trust code. The token generated in CSSM, applies at the Smart Account or Virtual Account level, and applies only to all product instances in that account.
- A signature mismatch: This means that the system clock is not accurate.
- Timestamp mismatch: This means the product instance time is not synchronized with CSSM and can cause installation to fail.

Recommended action

- A trust code is already installed: If you want to install a trust code despite an existing trust code on the product instance, re-configure the **license smart trust idtoken** `id_token_value` { **local** | **all** }[**force**] command in privileged EXEC mode, and be sure to include the **force** keyword this time. Entering the **force** keyword sets a force flag in the message sent to CSSM to create a new trust code even if one exists.
- Smart Account-Virtual Account mismatch: Log in to the CSSM Web UI at https://software.cisco.com/software/smart-licensing/alerts and click **Smart Software Licensing** > **Inventory** > **Product Instances** .
- Check if the product instance on which you want to generate the token is listed in the selected Virtual Account. If it is, proceed to the next step. If not, check and select the correct Smart Account and Virtual Account. Then complete these tasks again: See

the *Generating a New Token for a Trust Code from CSSM* and *Installing a Trust Code* topics in Common Tasks for Configuring Smart Licensing Using Policy .

- Timestamp mismatch and signature mismatch: Configure the ntp server command in global configuration mode. For example:

```
Device(config)# ntp server 198.51.100.100 version 2 prefer
```

Error message

```
%LICMGR-4-LOG_SMART_LIC_REPORTING_NOT_SUPPORTED: The CSSM OnPrem that this product instance
is connected to is down rev and does not support the enhanced policy and usage reporting
mode.
```

Explanation

Cisco Smart Software Manager On-Prem (formerly known as Cisco Smart Software Manager satellite) is not supported in the SLP environment. The product instance behaves as follows:

- Stop sending registration renewals and authorization renewals.
- Start recording usage and saving RUM reports locally.

Recommended action

Refer to and implement one of the supported topologies instead. See: Supported deployment models and topologies .

Error message

```
%LICMGR-6-LOG_SMART_LIC_POLICY_INSTALL_SUCCESS: A new licensing policy was successfully
installed.
```

Explanation

A policy was installed as part of an ACK response.

Recommended action

No action is required. If you want to know which policy is applied (the policy in-use) and its reporting requirements, enter the **show license all** command in privileged EXEC mode.

```
Error Message %LICMGR-6-LOG_SMART_LIC_AUTHORIZATION_INSTALL_SUCCESS: A new licensing
authorization code was successfully installed on: [chars].
```

This message is not applicable to Nexus Switches, because there are no enforced or export-controlled licenses on these product instances.

Error message

```
%LICMGR-6-LOG_SMART_LIC_AUTHORIZATION_REMOVED: A licensing authorization code has been
removed from [chars]
```

Explanation

[chars] is the UDI where the authorization code was installed. The authorization code has been removed. This removes the licenses from the product instance and may cause change in the behavior of smart licensing and the features using licenses.

Recommended action

No action is required. If you want to see the current state of the license, enter the **show license all** command in privileged EXEC mode.

Error message

```
%LICMGR-6-LOG_SMART_LIC_REPORTING_REQUIRED: A Usage report acknowledgement will be required
in [dec] days.
```

Explanation

This is an alert which means that RUM reporting to Cisco is required. [dec] is the amount of time (in days) left to meet this reporting requirements.

Recommended action

Ensure that RUM reports are sent within the requested time.

- If the product instance is directly connected to CSSM, or to CSLU and the product instance is configured to initiate communication complete this step on the product instance, the product instance will automatically send usage information at the scheduled time.
- If it is not sent at the scheduled time, because of technical difficulties, you can **license smart sync** command in privileged EXEC mode. For syntax details, see the license smart (privileged EXEC) in the Command Reference.
- If the product instance is connected to CSLU, but CSLU is disconnected from CSSM, complete these tasks: *Download All For Cisco (CSLU Interface)*, *Uploading Usage Data to CSSM and Downloading an ACK* , and *Upload From Cisco (CSLU Interface)* . See the *Uploading Usage Data to CSSM and Downloading an ACK* task in Common Tasks for Configuring Smart Licensing Using Policy .
- If the product instance is disconnected from CSSM and you are not using CSLU either, enter the **license smart save usage** command in privileged EXEC mode, to save the required usage information in a file. Then, from a workstation where you have connectivity to CSSM, complete these tasks: First perform the *Uploading Usage Data to CSSM and Downloading an ACK* task and then perform the *Installing a File on the Product Instance* task from Common Tasks for Configuring Smart Licensing Using Policy . .

Error message

```
%LICMGR-6-LOG_SMART_LIC_TRUST_CODE_INSTALL_SUCCESS: A new licensing trust code was
successfully installed on [chars].
```

Explanation

[chars] is the UDI where the trust code was successfully installed.

Recommended action

No action is required. If you want to verify that the trust code is installed, enter the show license status command in privileged EXEC mode. Look for the updated timestamp under header **Trust Code Installed:** in the output.

Smart Licensing Using Policy FAQs

This topic consists of frequently asked questions about Smart Licensing Using Policy (SLP) on Nexus 9000 and 3000 switches.

1. What is Smart Licensing Using Policy?

The Smart Licensing Using Policy is an evolved version of Smart Licensing.

The Smart Licensing Using Policy simplifies the day-0 operations for customers. The product will not boot in evaluation-mode, per product software registration is not required, and ongoing communication every 30 days with the Cisco Cloud is not required. However, license use compliance does require software reporting. Reporting is and can be done:

- From Cisco factory, when all new purchases include a Smart Account on an order
- Smart Software Manager (SSM) On-Prem (Version XXXX)

- Cisco Smart Licensing Utility (CSLU) lite-windows application
- Through APIs / command line interface for any 3rd party system
- Directly to a Smart Account

2. Which platform and software release supports Smart Licensing Using Policy?

Smart Licensing Using Policy is required from Cisco NX-OS Release 10.2(1)F onwards and is supported on Cisco Nexus 9000 and 3000 platform switches. Enforced and Export licenses are not supported on Cisco Nexus 9000 platform switches.

3. What are the key differences between Smart Licensing and Smart Licensing Using Policy?

Smart Licensing	**Smart Licensing Using Policy**
Mandatory evaluation mode	No registration, No evaluation mode
Day0 registration to CSSM or SSM On-Prem per device for software compliance	Allows unenforced license change, but reporting required
On-going license reporting every 30 days	On-change reporting policies and customer-specific reporting policies
Software compliance is a preuse per product activity requirement	Software compliance is managed on-change, automation tools that are provided to assist with SW

4. What is different in CSSM with Cisco NX-OS Release 10.1(2) and Cisco Nexus Release 10.2(1)F?

In CSSM, users need not register devices before use. However, to set up automated reporting a Cisco tool, API reporting, or direct connection from a product using a trusted connection to CSSM can be used. Alternatively, users can manually upload software use records (RUM reports) directly to CSSM via the Upload Usage Data button under the Reporting and Usage Data Files tabs. An active Smart Account is required to submit software use RUM reports.

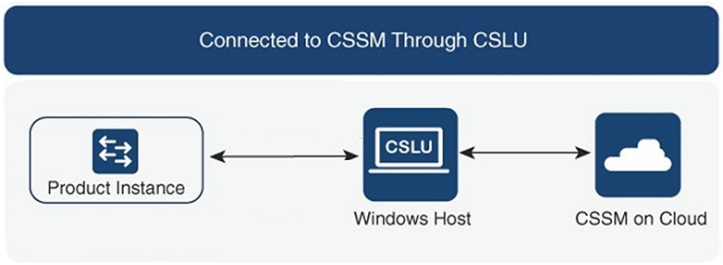
5. How often is reporting required?

- Report is required within 90 days only when there is a change in software use.
- Ongoing reporting frequency: 365 days.
- Unenforced/Non-Export, first report is required within 90 days.

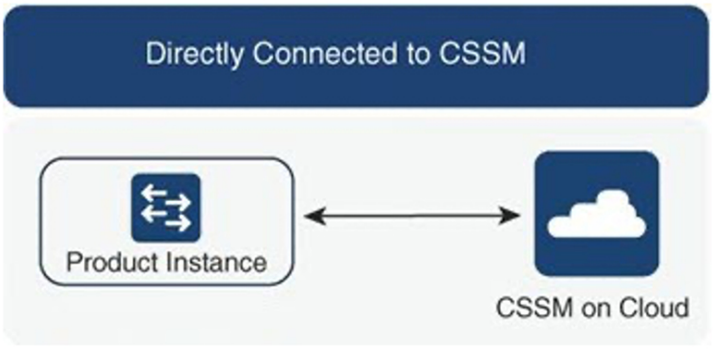
6. What are the supported topologies for connecting to Cisco Smart Software Manager (CSSM)?

The following are the supported topologies.

Topology 1: Connected to CSSM Through CSLU



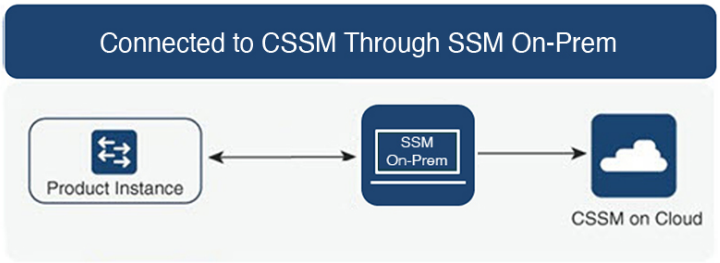
Topology 2: Connected Directly to CSSM



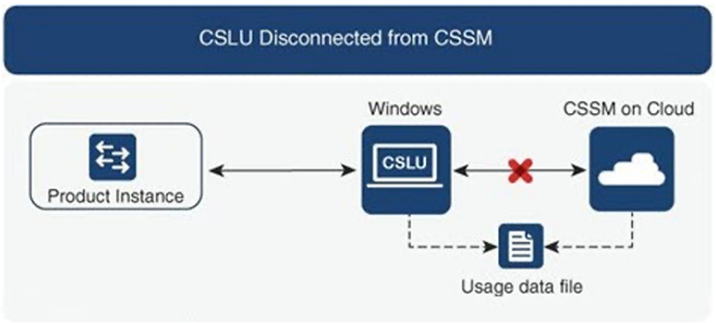
Note

A trust token is required only for this topology.

Topology 3: Connected to CSSM Through SSM On-Prem



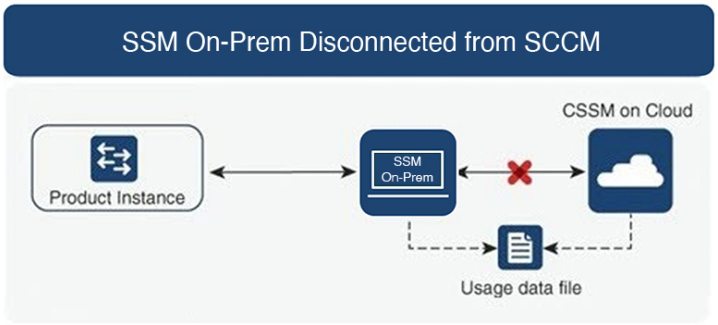
Topology 4: CSLU Disconnected from CSSM



Topology 5: No Connectivity to CSSM and No CSLU



Topology 6: SSM On-Prem Disconnected from CSSM



7. How do customers Report software use?

Cisco Smart Licensing Using Policy provides various reporting options using online and offline modes to report software use.

- From the switch in off-line or direct connect mode.
- Cisco Smart License Utility (CSLU) Lite-Windows application
- SSM On-Prem
- Direct to CSSM via APIs

8. Does the customer require to install a trust token?

No, unless customer is using a direct connection to CSSM then a one-time trust exchange is established.

9. What will happen if customers upgrade from legacy licenses or from Smart Licensing to a Smart Licensing Using Policy for non-export-controlled software?

When a customer migrates from a legacy licensing scheme [such as PAK (Product Activation Key) files or traditional Smart Licensing] to a Smart Licensing Using Policy, license conversion is expected to happen automatically.

Note

- For Topology 5: No Connectivity to CSSM and No CSLU, we recommend waiting for one hour after Smart Licensing Using Policy migration to generate the first RUM report.
- If the transport mode is off, you must collect the first rum report after an hour of migration to SLP to support PAK-based license conversion. Ensure that before you gather the rum report, show license data conversion is not blank.

10. Will the Smart Account/Virtual Account migrate to Smart Licensing Using Policy by default, or does it must be requested?

Smart Account/Virtual Account will be enabled with Smart Licensing Using Policy functionality. No migration of Smart Account is necessary.

11. Are all Virtual Accounts inside a Smart Account enabled for Smart Licensing Using Policy?

Yes.

12. Can a Smart Licensing Using Policy-enabled SA/VA handle non-Smart Licensing Using Policy Images?

Yes.

13. Can a non-Smart Licensing Using Policy connect to a Smart Licensing Using Policy SA/VA?

Yes.

14. Does anything change with the existing software subscription tiers?

There is no change in the software subscription tier, it remains the same.

15. Does Release 10.2(1)F support only Smart Licensing Using Policy?

Starting with Release 10.2(1)F devices will only support Smart Licensing Using Policy. There is no support for traditional licensing and smart licensing in this release.

16. After migrating to Smart Licensing Using Policy, what's the maximum amount of time I get before I send the first report.

If at least one feature on the Nexus requires a license, a report is required within 90 days.

17. Who determines the policy and how many policies can be applied on a single device?

CSSM determines the policy that is applied to a product. Only one policy is in use at a given point in time.

18. Is the Policy a hard requirement?

The policy is a requirement from Cisco. It is a soft requirement on device and not an enforcement.

19. What is Cisco Smart Licensing Utility (CSLU)?

Cisco Smart Licensing Utility (CSLU) is a Windows application that is used to automate receiving or pulling software use reports from a Cisco product and report the software use to a Smart Account on Cisco Smart Software Manager (CSSM).

20. What are the minimum Windows system requirements to install CSLU?

Component	**Minimum**	**Recommended**
Hard disk	100 GB	200 GB
RAM	8 GB	8 GB
CPU	x86 Dual Core	x86 Quad Core
Ethernet NIC	1	1

21. What are the key features of CSLU?

- Collect license usage reports from the product instances in either a push or pull modes.
- Store and forward usage reports to CSSM for billing and analytics.
- Obtain and distribute policy and authorization codes from CSSM.
- It can be deployed as standalone micro service:
    - Windows host (up to 10,000 Product Instances (PI))
- It can also be integrated as software component with controller-based products.
- Regardless how the micro service is deployed, it is able to deliver an on-line or off-line connectivity model for the license data.

22. What is the report format in CSLU?

The CSLU report format is based on ISO 19770-4 standard RUM report format. It is delivered in JSON format and is signed per trust model.

23. What are the various tools to collect software use report?

Customers can use various sets of APIs that are available on NX-OS.

24. Which data does Cisco care about?

Below are the required data fields for software reconciliation for each Cisco product that supports Smart Licensing Using Policy.

UDI	**HardwareProduct serial number**
SN	Software Unique ID Serial Number
Software Package and Reg ID	Software product package and entitlement tag
Count	Software use count per license entitlement
Time and date stamp	Per license entitlement change and use

Below are optional data fields for software reconciliation for each Cisco product that support Smart Licensing Using Policy.

SA-VA Level 1	**example, Entity (map to a SA)**
SA-VA Level 2	example, GEO (map to a SA)
SA-VA Level 3	example, department (map to a SA)
SA-VA Level 4	example, building (map to a SA)
SA-VA Level 5	example, room (map to a SA)
Free form	Data does not go back to Cisco
Free form	Data does not go back to Cisco

(SA = Smart Account, VA = Virtual Account)

25. How does Smart Licensing Using Policy work with device replacement (RMA)?

The Smart Licensing Using Policy configuration from the replaced device must be applied to the replacement device. If the existing configuration is unavailable or not functional on the new device, see Supported deployment models and topologies and Migrating to Smart Licensing Using Policy.

26. What are Licenses Enforcement types?

The enforcement type indicates if the license requires authorization before use. Following are the two types of license enforcement.

- Unenforced - Unenforced licenses do not require authorization before use in air-gapped networks or in connected networks. The terms of use for such licenses are as per the End User License Agreement (EULA)
- Enforced - Licenses that belong to this enforcement type require authorization before use. The required authorization is in the form of an authorization code, which must be installed in the corresponding product instance.

Note

Only unenforced licenses are supported in Release 10.2(1)F.

27. When we order hardware along with licenses, how much time does it take to reflect smart licenses under a particular smart account after allocation?

Smart Licenses will be reflected on CSSM in about 24 to 96 hours.

28. What happens if customers upgrade from smart licensing to a SLP for non-export-controlled software?

If a customer upgrades from a legacy license to a SLP, there will be no operational changes. All keys will persist through the upgrade

29. When the SLP Report doesn't sync automatically after ASCII Reload, should the sync be triggered manually?

This is a rare scenario. When the SLP transport mode is SMART, trust is established, report is synced, and ACK received, if the **copy r s** and **reload** command is issued, then when the box comes up, the report syncs automatically and the ACK is received as expected. However, if the **ascii reload** command is issued, and, when the box comes up, if the report does not sync automatically, then, to initiate the process, run the **license smart sync all** command.

30. Among the vPC peers, would it suffice to register just one of the vPC peer switches with SLP?

No. With regard to SLP, every vPC peer switch acts as a separate entity, so you should register both the switches.

Reference

For more information about SLP, see Cisco Nexus 9000 and 3000 Series NX-OS Smart Licensing Using Policy User Guide.