

Revised: September 30, 2024

# SLP Troubleshooting, System Messages, and FAQs

## Overview

This article provides information about troubleshooting Smart Licensing using Policy (SLP) on MDS 9000 switches and frequently asked questions (FAQs).

## Troubleshooting SLP

The troubleshooting section is further divided into two sections that provide step-by-step instructions to resolve SLP issues on MDS 9000 switches.

- [Resolving SLP Issues on MDS 9000 Switches](#) — This section covers the common problems and solutions related to connectivity of switch to CSSM.
- [System Message Overview](#) — This section provides a list of SLP-related system messages you may encounter, possible reasons for failure, and recommended action.

## Resolving SLP Issues on MDS 9000 Switches

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

The following issues are covered in this section:

- [Issue: Trust code installation failed](#)
- [Issue: Smart Licensing communication with CSSM/CSLU/SSM On-Prem failed](#)
- [Issue: Failed to send usage Report](#)
- [Issue: Failed to receive Report Acknowledgment](#)

### Issue: 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.

---

### Issue: 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 the following 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>**. The following 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. The following example shows reachability for the smart URL.

This is the Smart Receiver!

```
Environment Information:
  cisco.life = prod
  License Engine = https://swapi.cisco.com/software/csww/ssm/services
  License EngineSLE = https://swapi.cisco.com/software/csww/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** commands 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 follows:

```
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](https://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](https://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$

```

### Issue: 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.

### Issue: Failed to receive Report Acknowledgment

#### Possible reasons for failure include:

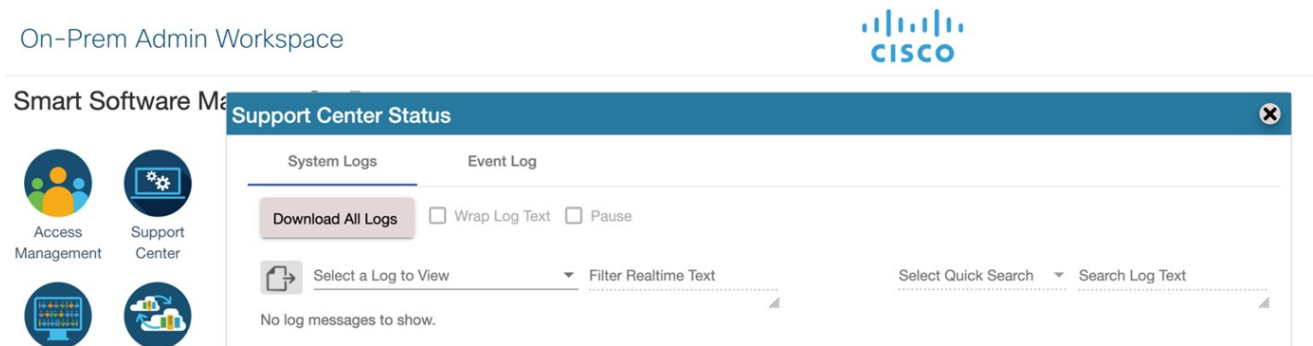
- Connectivity problems. Depending on the implemented topology, this can mean a connectivity problem with CSSM, or CSLU, or SSM On-Prem.
- Delayed communication. There may be a lag between the time that a RUM Report is sent and the RUM acknowledgment (ACK) is available on the product instance. For example, 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 the following 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:

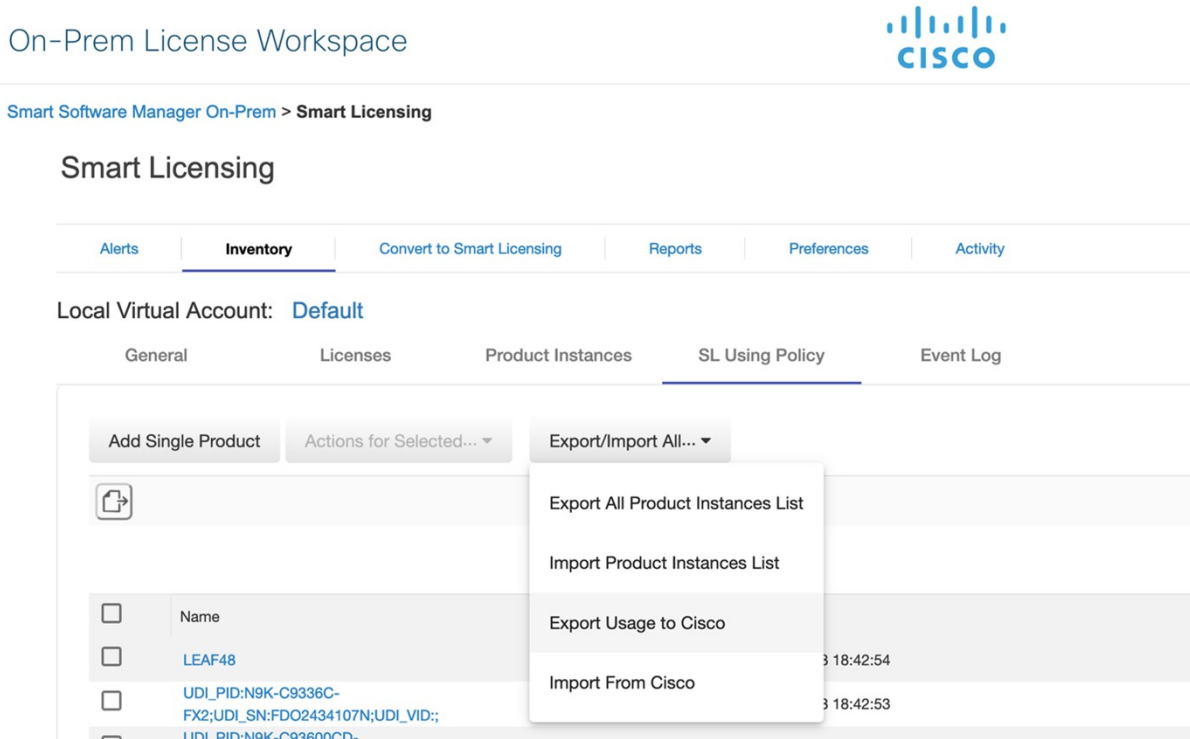
1. Ensure that the trust code is installed.
2. When the trust code is installed, check for **Usage reporting**: in **show license status** to know whether the report is synced or not. The **Next report push** field displays the following information about the synchronization:

```
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
```

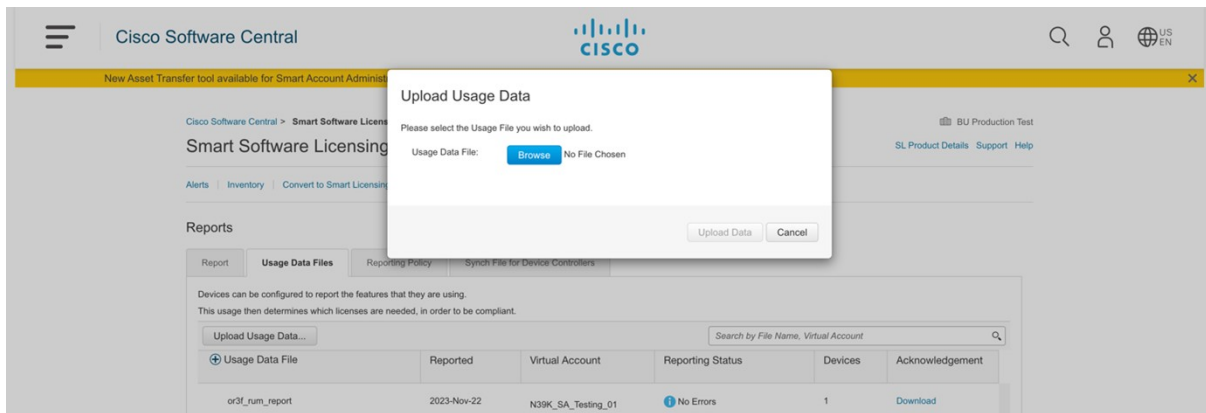
3. If the synchronization does not take place automatically, then initiate an on-demand synchronization based on the implemented topology as follows:
  - For online topologies, use the **license smart sync** command in privileged EXEC mode. If SSM On-Prem is used in topology, then, additionally, sync 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.

Cisco Software Central

Smart Software Licensing

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

Usage Data Files

Devices can be configured to report the features that they are using. This usage then determines which licenses are needed, in order to be compliant.

Upload Usage Data...

Usage Data File	Reported	Virtual Account	Reporting Status	Devices	Acknowledgement
or3f_run_report	2023-Nov-22	N39K_SA_Testing_01	No Errors	1	<a href="#">Download</a>

- 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.



# On-Prem License Workspace

Smart Software Manager On-Prem > Smart Licensing


## Smart Licensing

[Alerts](#)[Inventory](#)[Convert to Smart Licensing](#)[Reports](#)[Preferences](#)

Local Virtual Account: [Default](#)

[General](#)[Licenses](#)[Product Instances](#)[SL Using Policy](#)

Add Single ProductActions for Selected... ▼Export/Import All... ▼



<input type="checkbox"/>	Name
<input type="checkbox"/>	LEAF48
<input type="checkbox"/>	UDI_PID:N9K-C9336C-FX2;UDI_SN:FDO2434107N;UDI_VID;;

Export All Product Instances List

Import Product Instances List

Export Usage to Cisco

Import From Cisco

- 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 the Cisco technical support representative.

## System Message Overview

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. Each system message begins with a percent sign (%) and is structured as follows:

`%FACILITY-SEVERITY-MNEMONIC: Message-text`

### **%FACILITY**

Two or more uppercase letters that show the facility to which the message refers. A facility can be a hardware switch, 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 that are 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)
[hex]	Hexadecimal number

Severity Level	Description
[inet]	Internet address (for example, 10.0.2.16)
[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 that maybe encountered, possible reasons for failure (in case it is a failure message), and recommended action (if action is required).

For all error messages, contact your Cisco technical support representative with the following information if you are unable to resolve it by yourself:

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.

### SMART\_LIC-3-POLICY\_INSTALL\_FAILED

Error Message %SMART\_LIC-3-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 that the system clock on the switch 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.

For example:

```
switch(config)# ntp server 1.1.1.1 prefer
```

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

### SMART\_LIC-3-AUTHORIZATION\_INSTALL\_FAILED

Error Message %SMART\_LIC-3-AUTHORIZATION\_INSTALL\_FAILED: The install of a new licensing authorization code has failed on [chars]: [chars].

#### Explanation

Authorization code installation has failed for enforced license.

### Recommended Action

Use the **license smart authorization request** {add | replace} *port-feature* {local | all} **count** *port-range* command to enable ports or replace the existing authorization code.

### SMART\_LIC-3-COMM\_FAILED

Error Message %SMART\_LIC-3-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 switch initiates the sending of RUM reports (Connected to CSSM Through CSLU: Product Instance Initiated Only, Connected Directly to CSSM, and CSLU Disconnected from CSSM: Product Instance Initiated Only) if this communication failure message coincides with scheduled reporting (**license smart usage interval** *interval\_in\_days*), the switch attempts to send out the RUM report for up to 4 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. After the communication failure is resolved, the system reverts the reporting interval to the value that was 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 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.
2. Check DNS resolution. Verify that the switch can ping [smartreceiver.cisco.com](https://smartreceiver.cisco.com) or the *nslookup* translated IP. The following example shows how to ping the translated IP:

```
switch# ping 171.70.168.183
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 171.70.168.183, 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 to check if the URL is exactly as follows: <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 smart-licensing** command.

```
switch# show callhome smart-licensing
Current smart-licensing transport settings:
Smart-license messages: enabled
```

Profile: xml (status: ACTIVE)

### 3. Check DNS Resolution. Verify that the switch can ping `tools.cisco.com` or the `nslookup` translated IP.

```
switch# ping tools.cisco.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 173.37.145.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 41/41/42 ms
```

If the above resolution does not work, check if the switch's `mgmt0` interface is set with IP address and the management interface is up. To ensure that the network is up, configure the **no shutdown** command.

Check if the switch is subnet masked with a subnet IP and if the DNS IP and default gateway are configured.

### 4. Verify if the IP gateway is set.

Use the **show ip interface** command to display the current configuration.

In case the above resolution 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 the `Last ACK received:` field. If this has a recent timestamp, it means that the switch has connectivity with CSLU. If not, check if the switch can ping `cslu-local`. A successful ping confirms that the switch is reachable.

If the above resolution does not work, configure the name server with an entry where hostname `cslu-local` is mapped to the CSLU IP address (the Windows or Linux host where CSLU is installed). Configure the **ip domain-lookup**, **ip domain-name domain-name**, and **ip name-server server-address** commands. Here the CSLU IP is 192.168.0.1 and name-server creates entry `cslu-local.example.com`.

```
switch(config)# ip domain-name example.com
switch(config)# ip name-server 192.168.2.1
```

- 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 or Linux host where CSLU is installed. 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 not, configure the **license smart transport cslu** and **license smart url cslu http://<cslu\_ip\_or\_host>:8182/cslu/v1/pi** commands.

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

## SMART\_LIC-3-COMM\_RESTORED

Error Message %SMART\_LIC-3-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

Switch communicating with either the CSSM or CSLU is restored.

### Recommended Action

No action required.

### SMART\_LIC-3-POLICY\_REMOVED

Error Message %SMART\_LIC-3-POLICY\_REMOVED: The licensing policy has been removed.

### Explanation

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

Possible reasons for failure include:

If the **license smart factory reset** command is executed in EXEC mode, all licensing information including the policy is removed.



### Note

---

The switch must be reloaded after using the **license smart factory reset** command.

---

### Recommended Action

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

If the policy was removed inadvertently, reapply the policy. Depending on the topology that is implemented, follow the corresponding method to retrieve the policy:

- Connected Directly to CSSM:

Enter the **show license status** command, and check the `Trust Code installed:` field. If trust is established, then CSSM will automatically return the policy. The policy is automatically reinstalled on switches of the corresponding Virtual Account.

If trust has not been established, complete these tasks:

[Generating a New Token for a Trust Code from CSSM](#) and [Installing a Trust Code](#). When these tasks are completed, CSSM will automatically return the policy. The policy is then automatically installed on all switches of that Virtual Account.

- Connected to CSSM Through CSLU:

For switch-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 switch.

- CSLU Disconnected from CSSM

For switch-initiated communication, enter the **license smart sync** command. The synchronization request causes CSLU to push the missing information (a policy or authorization code) to the switch. Then, complete these tasks in the given order:

1. [Export to CSSM](#)
2. [Uploading Usage Data to CSSM and Downloading an ACK](#), and
3. [Import from CSSM](#).

- No Connectivity to CSSM and No CSLU

In an entirely air-gapped network, from a workstation that has connectivity to the Internet and CSSM complete [Downloading a Policy File from CSSM](#).

Then, complete [Installing a File on the Switch](#).

- SSM On-Prem Disconnected from CSSM

For switch-initiated communication, enter the **license smart sync** command in privileged EXEC mode. The synchronization request causes CSLU on SSM On-Prem to push the missing information (a policy or authorization code) to the switch.

## SMART\_LIC-3-TRUST\_CODE\_INSTALL\_FAILED

Error Message %SMART\_LIC-3-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 switch. If the UDI is already registered and you try to install another one, installation fails.
- Smart Account-Virtual Account mismatch: This means that the Smart Account or Virtual Account (for which the token ID was generated) does not include the switch on which the trust code was installed. The token that is generated in CSSM applies at the Smart Account or Virtual Account level and applies only to all switches in that account.
- A signature mismatch: This means that the system clock is not accurate.
- Timestamp mismatch: This means the switch time is not synchronized with CSSM and can cause installation to fail.

### Recommended Action

- A trust code is already installed: To install a trust code despite an existing trust code on the switch, reconfigure the **license smart trust idtoken id\_token\_value {local | all} [force]** command in privileged EXEC mode and ensure to include the **force** keyword. Using 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: Login to the CSSM Web UI at <https://software.cisco.com/software/smart-licensing/alerts>. Click **Inventory** > **Product Instances**.

Check if the switch on which the token is to be generated 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: [Generating a New Token for a Trust Code from CSSM](#) and [Installing a Trust Code](#).

- Timestamp mismatch and signature mismatch: Configure the **ntp server** command. For example:

```
switch(config)# ntp server 1.1.1.1 prefer
```

## SMART\_LIC-4-REPORTING\_NOT\_SUPPORTED

Error Message %SMART\_LIC-4-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

The previous version of SSM On-Prem (formerly known as Cisco Smart Software Manager satellite) is not supported in the SLP environment. The switch will behave as follows:

- Stop sending registration renewals and authorization renewals.
- Start recording usage and saving RUM reports locally. The RUM reports are stored locally at `<CSLU_Working_Directory>/data/default/rum/unsent`.

## Recommended Action

Refer to and implement one of the supported topologies instead. For more information, see *Deploy* section.

### SMART\_LIC-6-POLICY\_INSTALL\_SUCCESS

Error Message %SMART\_LIC-6-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. To know which policy is applied (the policy in-use) and its reporting requirements, enter the **show license all** command.

### SMART\_LIC-6-AUTHORIZATION\_INSTALL\_SUCCESS

Error Message %SMART\_LIC-6-AUTHORIZATION\_INSTALL\_SUCCESS: A new licensing authorization code was successfully installed on: [chars].

## Explanation

A new licensing authorization code was installed.

## Recommended Action

No action is required. To know installed license status, enter the **show license all** command.

### SMART\_LIC-6-AUTHORIZATION\_REMOVED

Error Message %SMART\_LIC-6-AUTHORIZATION\_REMOVED: A licensing authorization code has been removed from [chars]

## Explanation

[chars] is the UDI where the authorization code was removed. This removes the licenses from the switch and may cause a change in the behavior of smart licensing and the features using the licenses.

## Recommended Action

No action is required. To see the current state of the license, enter the **show license all** command.

### SMART\_LIC-6-REPORTING\_REQUIRED

Error Message %SMART\_LIC-6-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 requirement.



## Recommended Action

Ensure that RUM reports are sent within the requested time.

- If the switch is directly connected to CSSM or to CSLU and the switch is configured to initiate communication, wait until the next schedule time (use the **show license all | grep "Next report push:"** command) or manually trigger the sync using **license smart sync** command from EXEC mode.. The switch will automatically send usage information at the scheduled time.

If it is not sent at the scheduled time because of technical difficulties, use the **license smart sync** command in EXEC mode.

- If the switch is connected to CSLU but CSLU is disconnected from CSSM, complete these tasks:

1. [Export to CSSM](#)
2. [Uploading Usage Data to CSSM and Downloading an ACK](#), and
3. [Import from CSSM](#).

- If the switch is disconnected from CSSM and CSLU is not being used either, enter the **license smart save usage** command in EXEC mode to save the required usage information in a file. Then, from a workstation that is connected to CSSM, complete these tasks: [Uploading Usage Data to CSSM and Downloading an ACK](#) > [Installing a File on the Switch](#).

## SMART\_LIC-6-TRUST\_CODE\_INSTALL\_SUCCESS

Error Message %SMART\_LIC-6-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. To verify that the trust code is installed, enter the **show license status** command in EXEC mode. Look for the updated timestamp under the `Trust Code installed:` field in the output.

# Smart Licensing Using Policy FAQs

## Smart Licensing Using Policy FAQs

### 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 / CLIs 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 MDS 9000 Release 9.2(2) onwards and is supported on Cisco MDS 9000 switches. Enforced and Port licenses are supported on Cisco MDS 9000 switches.

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

Smart Licensing Using Policy	Smart Licensing
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. How often is reporting required?

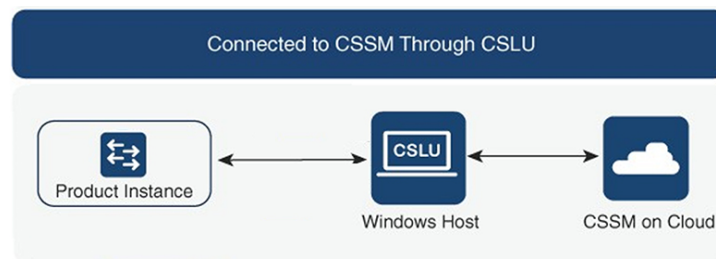
- Report is required within 90 days only when there is a change in software use.
- Ongoing reporting frequency: 365 days.
- Unenforced/Non-Export, first report is required within 90 days.

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

The following are the supported topologies.

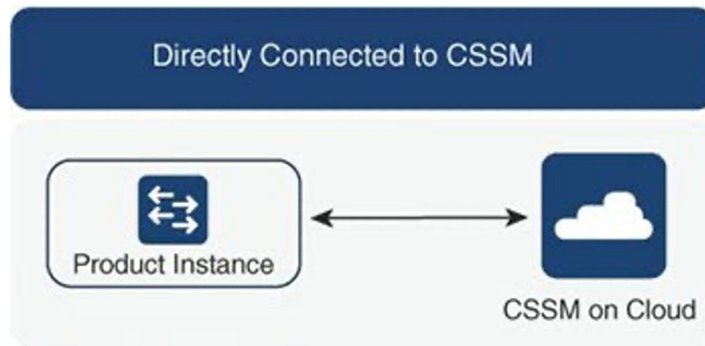
Topology 1: Connected to CSSM Through CSLU

**Figure 1:**



Topology 2: Connected Directly to CSSM

**Figure 2:**

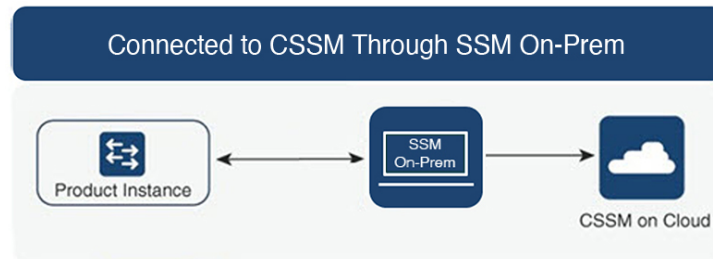


**Note**

A trust token is required only for this topology.

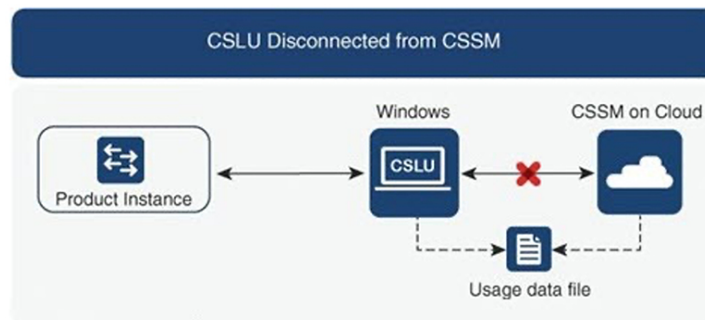
Topology 3: Connected to CSSM Through SSM On-Prem

**Figure 3:**



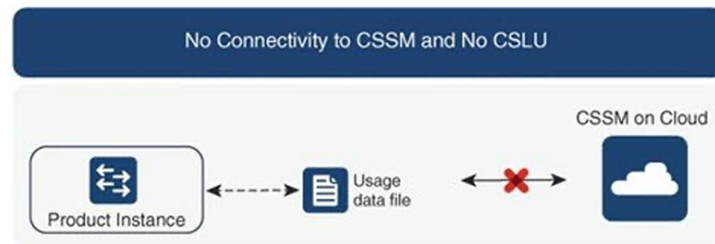
Topology 4: CSLU Disconnected from CSSM

**Figure 4:**



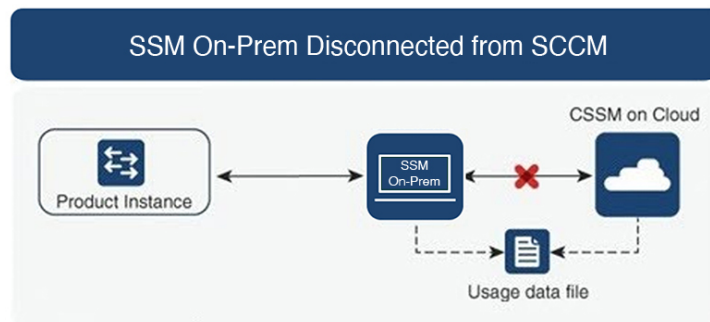
Topology 5: No Connectivity to CSSM and No CSLU

**Figure 5:**



Topology 6: SSM On-Prem Disconnected from CSSM

**Figure 6:**



**6. 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

**7. 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.

**8. 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.

**9. 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.

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

Yes.

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

Yes.

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

Yes.

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

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

14. Does Release 9(2) support only Smart Licensing Using Policy?

Starting with Release 9(2) devices will only support Smart Licensing Using Policy. There is no support for traditional licensing and smart licensing in this release.

15. 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.

16. 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.

17. Is the Policy a hard requirement?

The policy is a requirement from Cisco. It is a soft requirement on device and not an enforcement. Excluding a limited set of advanced VXLAN features, functionality is not disabled by the Nexus due to insufficient licensing.

18. 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).

19. 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

20. 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.

**21.** 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.

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

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

**23.** 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.

<b>UDI</b>	<b>HardwareProduct serial number</b>
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.

<b>SA-VA Level 1</b>	<b>example, Entity (map to a SA)</b>
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)

**24.** 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.

**25.** 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.

**26.** 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.

**27.** 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