Understand Smart Licensing for Catalyst Switching

Contents

Introduction

Purpose

Smart Licensing Using Policy

- Terminology
- Why This Change?
- Available Licenses
  - Base Licenses
  - Add-on Licenses
- The New Components
  - Policy
  - RUM Reports
- Manufacturing Flow for Greenfield Deployment Case
- CSLU

SLP - Direct Connect

- License Reporting
- Direct Connect - Smart Transport
- Direct Connect - Call-Home Transport

SLP - CSLU

- CSLU Installation and Configuration
- CSLU Using PUSH Mode
- CSLU Auto Discovery
- CSLU Using PULL Mode
  - PULL Mode Using RESTAPI
  - CSLU - Procedure to Setup
  - PULL Mode Using RESTCONF
  - CSLU - Procedure to Setup
  - PULL Mode Using NETCONF
  - CSLU - Procedure to Setup
- CSLU Using Disconnected Mode

SLP - Offline Mode

Behavior Changes

Troubleshoot

- Generic Troubleshooting Questionnaire
- Debug PI
- Debug CSLU

Related References

Introduction

This document describes the Smart Licensing feature using Policy on Catalyst Switching Platforms and supported deployment.

Purpose

From versions 17.3.2 and 17.4.1, from the Cisco IOS® XE, all the Catalyst Switching Platforms from the family for Cat9k support a new Licensing Model of SLP (Smart Licensing using Policy). The purpose of this document is to understand the different supported models of implementation and deployment of SLP, primarily for Greenfield deployments.

Smart Licensing Using Policy

With SLP, the device has all licenses 'in use' right out of the box. The earlier concepts, Evaluation mode, Registration, and Reservation go away with SLP. With SLP, it is all about reporting the licenses and their usage. The licenses are still unenforced and licensing levels still remain the same. For Catalyst Switch platforms, there are no export-controlled license levels, apart from the HSECK9 license. The only change is on the infra of reporting of license usage and tracking. This section talks in detail about terminologies, why the changes, the new components that come with SLP, CSLU (Cisco Smart Licensing Utility), and Product Ordering Flow.

Terminology

- CSSM or SSM – Cisco Smart Software Manager
- SA – Smart Account
- VA – Virtual Account
- SL – Smart Licensing
- PLR – Permanent License Reservation
- SLR – Smart License Reservation
- PIDs – Product IDs
- SCH – Smart Call Home
- PI – Product Instances
- CSLU – Cisco Smart Licensing Utility
- RUM – Resource Utilization Measurement
- ACK – Acknowledgement
- UDI – Unique Device Identification – PID + SN
- SLP - Smart Licensing using Policy

Why This Change?

With the introduction of the Smart Licensing model of trust and verify, Cisco has supported various deployment mechanisms to track and report license usage to the CSSM. Yet it was not easily adaptable for all kinds of deployments - there were feedback and requirements from the field, to make Smart Licensing more favorable for adoption. Some of the challenges are:

- With SL Registration - Devices have to be always connected to the Internet to reach CSSM which is a deployment concern.
- On-Prem Satellite servers introduce more cost to deployment and maintenance.
- SLR facilitates only air-gapped networks.
- Any deployments that do not support either of these models have to run their devices in the Unregistered/Eval expired state, even after licenses are purchased.

SLP is introduced to facilitate various such requests from the field. With SLP, you do not have to register

the product to CSSM. All the license levels that are purchased are 'in use' right out of the box. This removes the day-0 friction that was present on the device. SLP also minimizes the workflow of license provisioning and reduces the excess touch points. There is no necessity for the device to be connected to CSSM around the clock. SLP also brings in the ability to use licenses in the disconnected network, report the license usage offline, and report license at intervals determined by customer policies.

Available Licenses

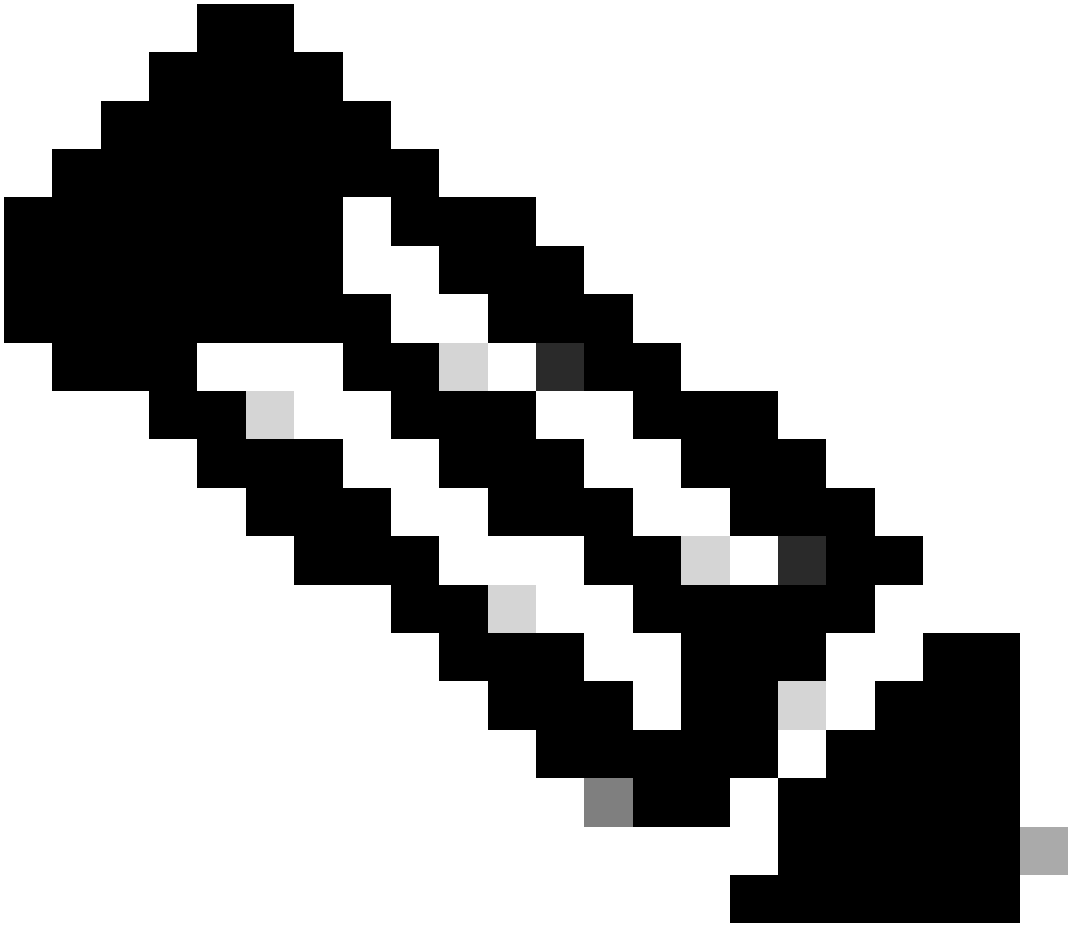
The software features available fall under base or add-on license levels. Base licenses are perpetual licenses and add-on licenses are available in three, five, and seven-year terms.

Base Licenses

- Network Essentials
- Network Advantage
- HSECK9

Add-on Licenses

- DNA Essentials
- DNA Advantage



Note: HSECK9 is an export-controlled license. It requires a SLAC to enable the license and respective feature.

The New Components

Policy

The policy decides what must be the default behavior for the PI. It tells the licensing reporting requirement attributes for different license levels and conditions. The policy also determines whether the ACK message must be sent back to PI, for every report that is sent to CSSM or not. The policy also contains the name of the policy and when the policy is installed. The default policy of Cisco is common and standard for all catalyst products. However, the customer-defined policy is also allowed if you wanted to have different reporting intervals and ACK response omission.

The policy can be installed on a PI on various occasions.

- Default policy present in the software
- Policy installed by Cisco manufacturing
- Policy installed through ACK response

- Policy installed manually through CLI
- Policy pushed using Yang Request

This output shows what a default policy looks like.

```
Policy:

Policy in use: Merged from multiple sources.
Reporting ACK required: yes (CISCO default)
Unenforced/Non-Export Perpetual Attributes:
First report requirement (days): 365 (CISCO default)
Reporting frequency (days): 0 (CISCO default)
Report on change (days): 90 (CISCO default)
Unenforced/Non-Export Subscription Attributes:
First report requirement (days): 90 (CISCO default)
Reporting frequency (days): 90 (CISCO default)
Report on change (days): 90 (CISCO default)
Enforced (Perpetual/Subscription) License Attributes:
First report requirement (days): 0 (CISCO default)
Reporting frequency (days): 0 (CISCO default)
Report on change (days): 0 (CISCO default)
Export (Perpetual/Subscription) License Attributes:
First report requirement (days): 0 (CISCO default)
Reporting frequency (days): 0 (CISCO default)
Report on change (days): 0 (CISCO default)
```

Note: A policy cannot be erased when you erase/modify a system configuration, clear nvram, or format the flash: filesystem. The policy is set to Cisco default, on license **smart factory reset**.

RUM Reports

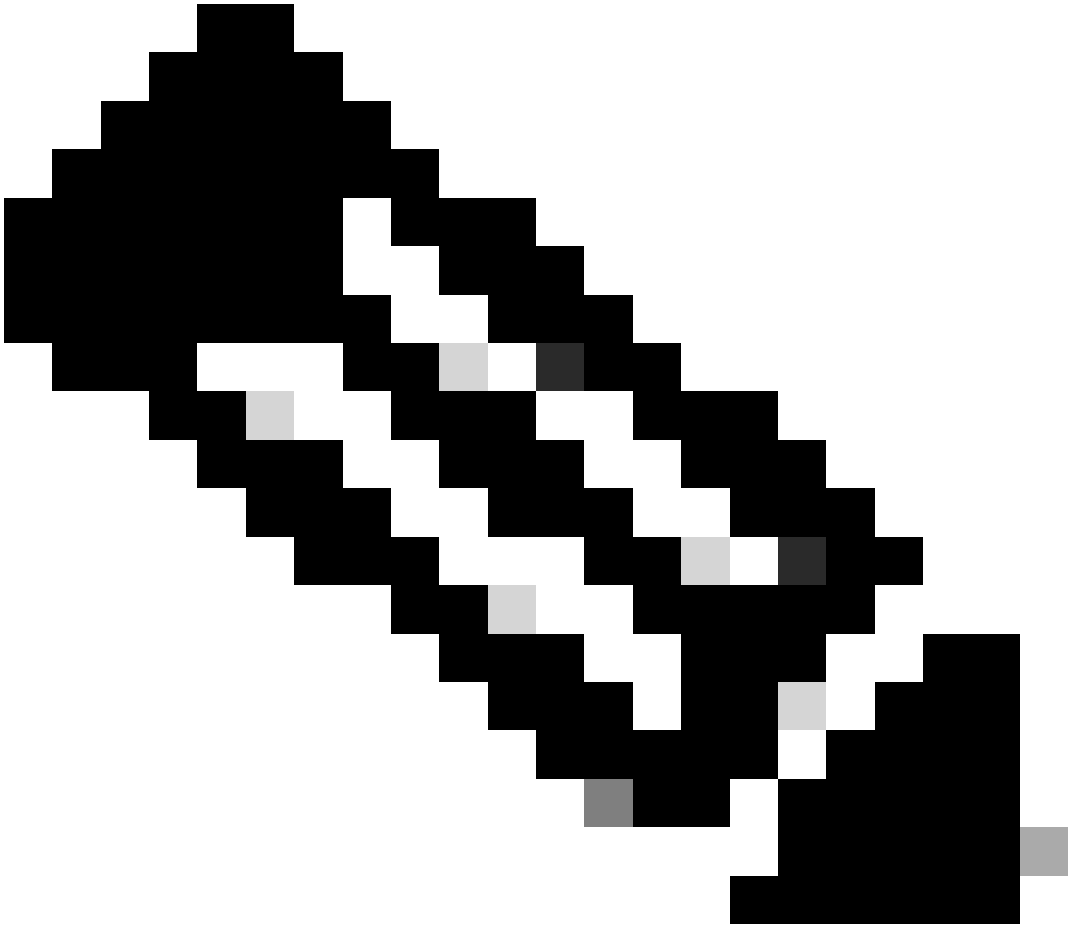
RUM is usage reports generated and stored by the PI. The ISO19770-4 Standard RUM reports are completed for SLP. RUM reports store any and all changes on license usage made in the PI as report files. Usage data for each license level is stored in separate RUM reports. RUM report measurements are collected and stored in PI at regular intervals. Whenever there is a change in the license usage of the PI or a reporting of usage has been triggered or when reports have reached maximum size/samples, new RUM reports for all license levels are generated. In other cases, the RUM reports that exist can be overwritten with a new sample and updated timestamp. The default RUM report utility measurement is every 15 minutes. At every reporting interval, RUM reports are sent to Cisco CSSM.

All the RUM reports are signed by the PI and verified by the CSSM. When CSSM receives the RUM report data from PI, it validates the report, checks the timeline of license usage change, and updates the CSSM data accordingly. CSSM then acknowledges back to the PI through the ACK response message.

RUM reports can be sent to CSSM in several ways:

- PI sends RUM reports to CSSM directly on reporting interval.
- PI pushes the RUM report to CSLU.
- CSLU pulls RUM reports from PI at regular intervals through RESTAPI and YANG models.
- RUM reports are saved manually on the PI through CLI and uploaded manually to CSSM.

Note: RUM reports cannot be erased when you erase/modify a system configuration, clear nvram, or format the flash: filesystem. All RUM reports can be removed from PI, on 'license smart factory reset'.



Note: The default reporting interval is 30 days.

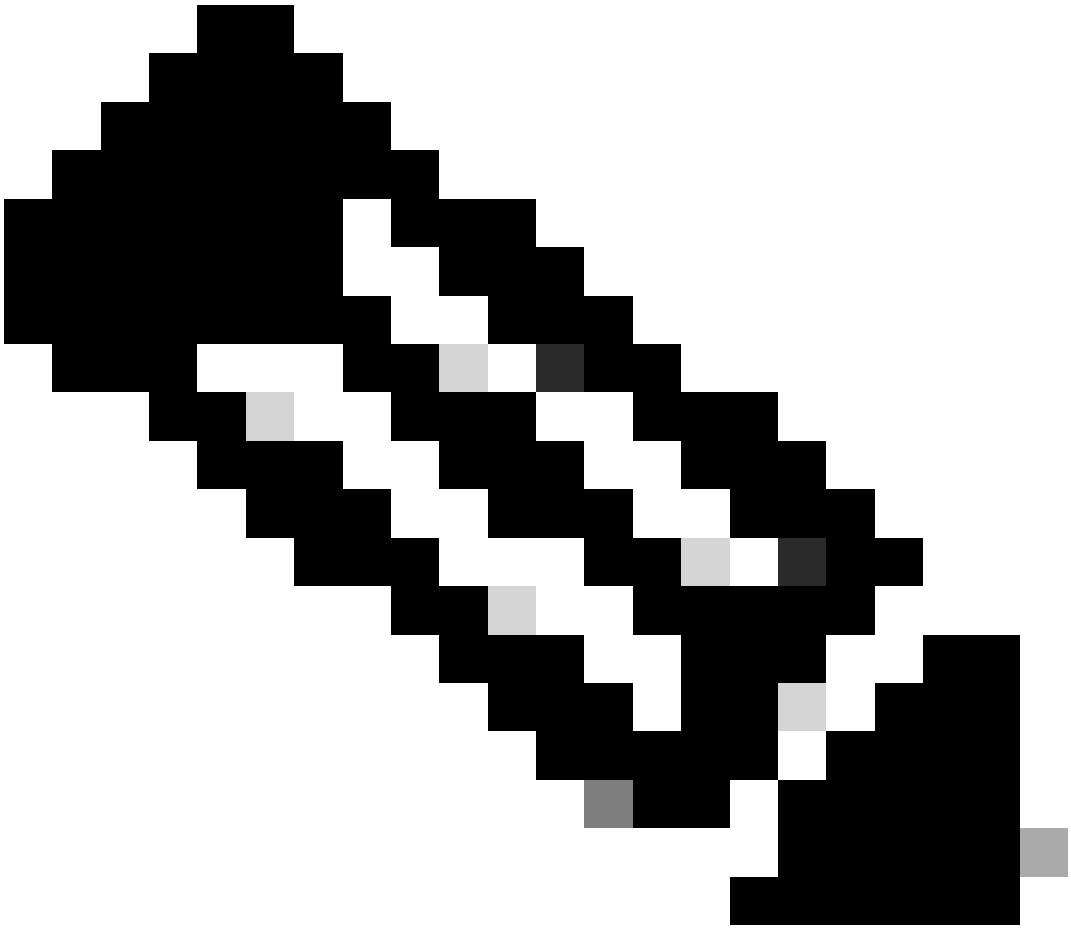
Manufacturing Flow for Greenfield Deployment Case

Once a new product order is placed at Cisco CCW (Cisco Commerce Workspace), the PI goes through the flow of operations done by the manufacturing team. This is to facilitate the secured process of signing RUM reports and remove the day-0 friction in registering the PI. Once the order is placed, any SA/VA that exists or new SA/VA that is created is associated with the product. The Cisco manufacturing team takes care of these operations before it ships the product to you:

- Install the Trust Code on the device. Trust code signature is installed based on device UDI. It is installed on every product.
- Install Purchase Code - Information on what license levels are purchased along with the product. It is installed on every product.
- SLAC - Smart License Auth Code - Not Applicable for Catalyst Platforms.

- Install Policy - Default or Custom Policy based on your input.
- Report the License Usage to CSSM - SA/VA.

Note: With the 17.3.3 release, this flow is followed for all Catalyst switching platforms except for C9200/C9200L.

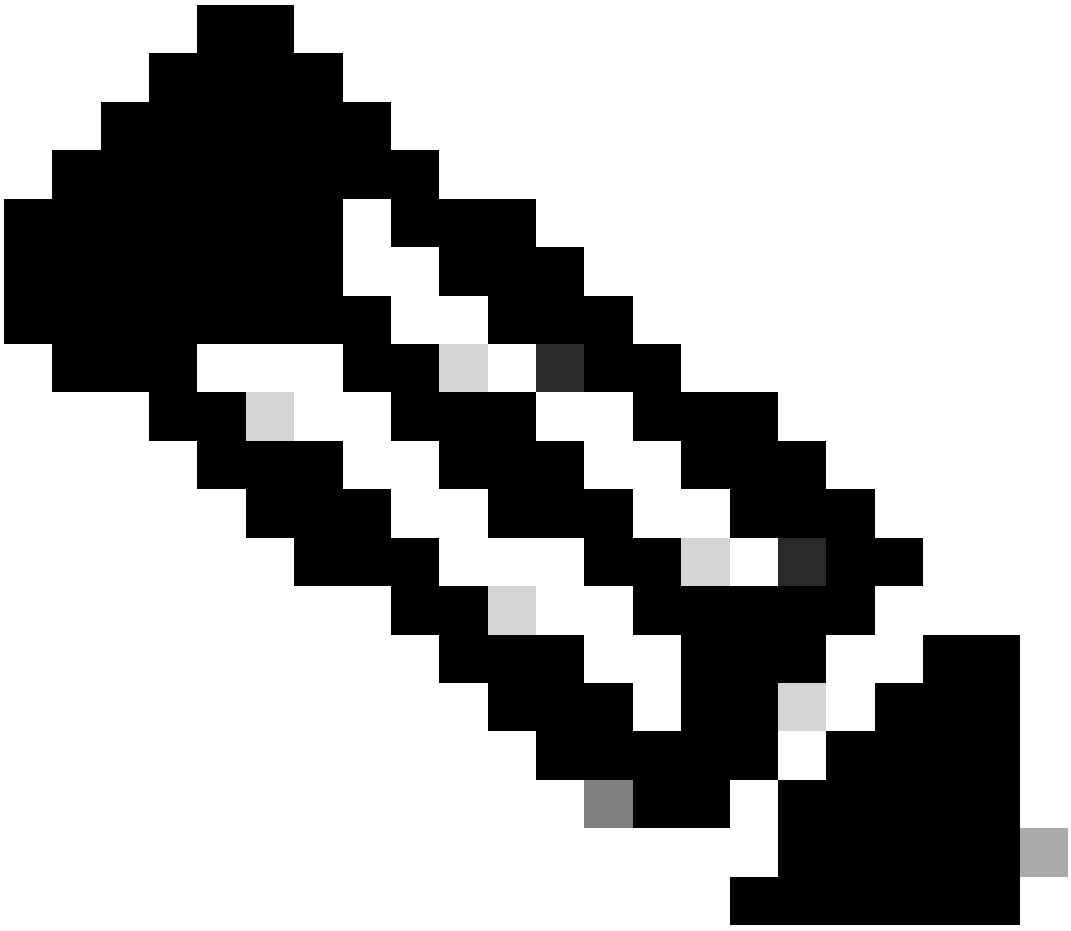


Note: The trust code is installed only in manufacturing with 17.7.1 for all Catalyst switching platforms except C9200/C9200L.

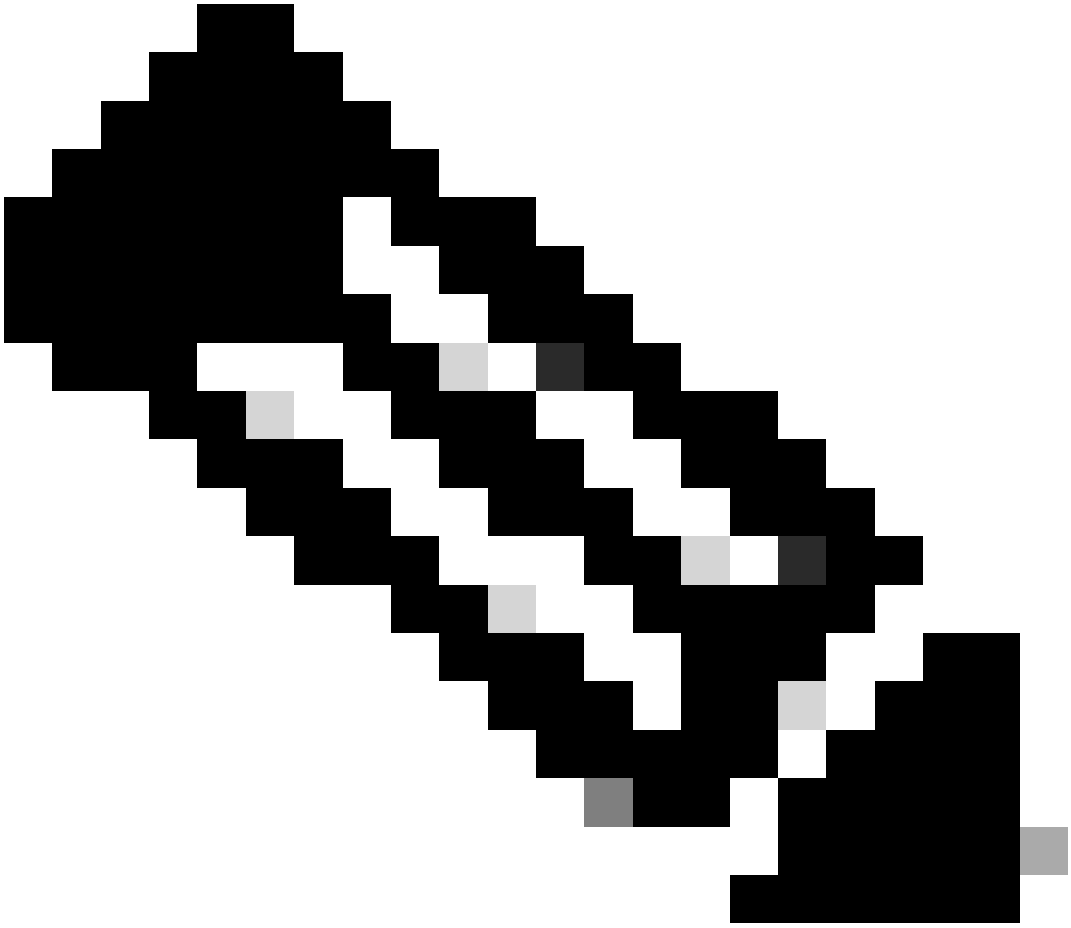
CSLU

SLP brings in a new simple yet powerful tool CSLU. CSLU is a GUI-based tool, that runs on Windows 10 Operating System or Linux version based on RHEL/Debian. CSLU, which can be run on your local private network, is responsible to collect the RUM ports from the PIs associated with CSSM. CSLU must be provisioned in a manner to collect RUM reports on PIs in the local network and also to periodically push the RUM report to CSSM through the Internet. CSLU is a simple tool, that displays only the details of the UDIs of the provisioned devices. All the License Usage data for PIs, Purchased Licenses, and Unused Licenses in the pool are seen only in SA/VA of CSSM, for you to verify. It is powerful because it can collect usage

reports of up to 10K PIs. CSLU is also responsible to push the ACK messages from CSSM back to PI.



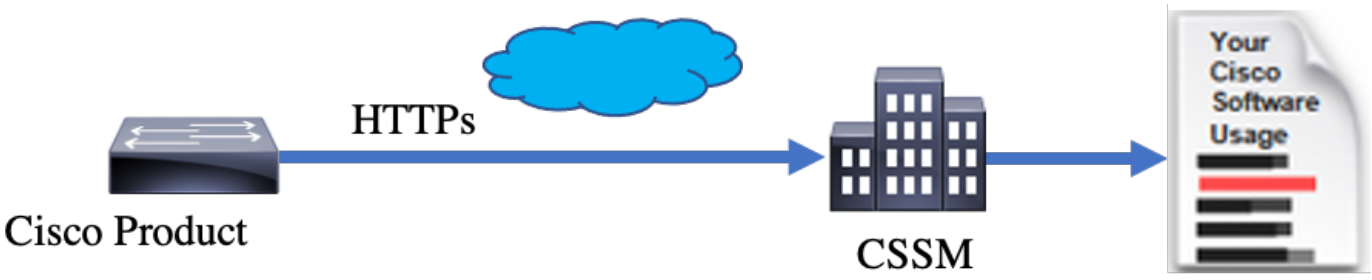
Note: Refer to the section, CSLU-based Topology for detailed configuration and supported modes of Operation of CSLU.

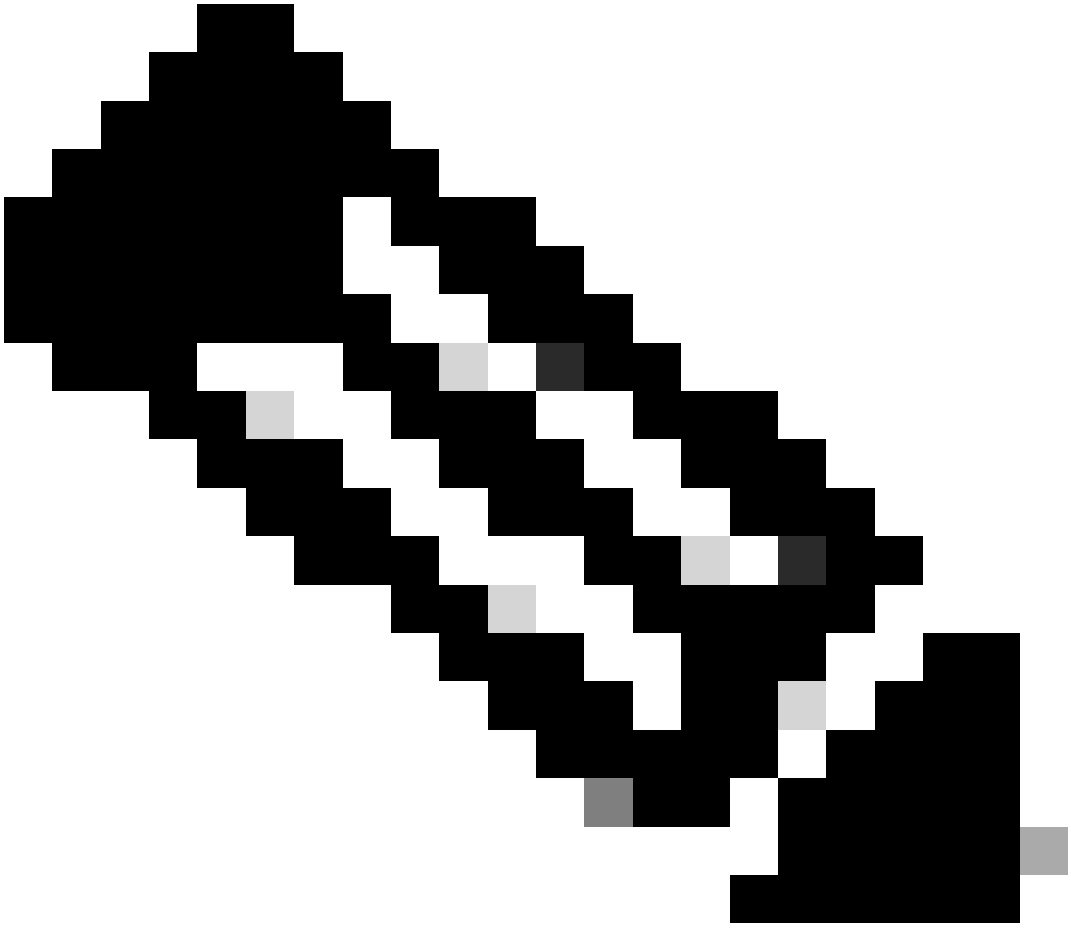


Note: Linux version of CSLU is supported from release 17.7.1.

SLP - Direct Connect

On a factory-shipped product, the default transport mode is configured to CSLU. If you wish to use the Direct Connect method, you must change the transport mode to Call-home or SMART based on the requirement. The basic requirement for the Direct Connect method of topology is to have Internet connectivity for the reachability to CSSM. Additionally, it must be ensured that for the connectivity to CSSM, the required L3 configurations, DNS, and Domain configurations are present in the device.





Note: Smart transport is the recommended transport method when you directly connect to CSSM.

License Reporting

On Direct Connect topology the RUM reports are directly sent to CSSM. License Reports require a successful Trust Code to be installed on the device. The Trust Code is installed by Cisco manufacturing on the Device before it is shipped. You can also install Trust Code on the device.

The Trust Code is a token string taken from CSSM, on Virtual Account - General Page. Trust Code can be installed through the CLI.

```
Switch#license smart trust idtoken < > all/local
```

Note: All the options must be used for HA or Stacking back system. For a Standalone device, the local option can be used.

```
Switch#license smart trust idtoken < > all/local.
```

On Successful installation of policy, the same can be verified through 'show license status' CLI.

```
Switch#show license status

Utility:
Status: DISABLED

Smart Licensing Using Policy:
Status: ENABLED

Data Privacy:
Sending Hostname: yes
Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
Type: Callhome

Policy:
Policy in use: Installed On Nov 07 22:50:04 2020 UTC
Policy name: SLP Policy
Reporting ACK required: yes (Customer Policy)
Unenforced/Non-Export Perpetual Attributes:
First report requirement (days): 60 (Customer Policy)
Reporting frequency (days): 60 (Customer Policy)
Report on change (days): 60 (Customer Policy)
Unenforced/Non-Export Subscription Attributes:
First report requirement (days): 30 (Customer Policy)
Reporting frequency (days): 30 (Customer Policy)
Report on change (days): 30 (Customer Policy)
Enforced (Perpetual/Subscription) License Attributes:
First report requirement (days): 0 (CISCO default)
Reporting frequency (days): 90 (Customer Policy)
Report on change (days): 90 (Customer Policy)
Export (Perpetual/Subscription) License Attributes:
First report requirement (days): 0 (CISCO default)
Reporting frequency (days): 90 (Customer Policy)
Report on change (days): 90 (Customer Policy)

Miscellaneous:
Custom Id: <empty>

Usage Reporting:
Last ACK received: Nov 03 12:57:01 2020 UTC
Next ACK deadline: Dec 03 12:57:01 2020 UTC
Reporting push interval: 30 days
Next ACK push check: <none>
Next report push: Nov 07 22:50:35 2020 UTC
Last report push: Nov 03 12:55:57 2020 UTC
Last report file write: <none>

Trust Code Installed:
Active: PID:C9500-24Y4C,SN:CAT2344L4GH
INSTALLED on Nov 07 22:50:04 2020 UTC
Standby: PID:C9500-24Y4C,SN:CAT2344L4GJ
INSTALLED on Nov 07 22:50:04 2020 UTC
```

Once the Trust Code is installed successfully, the PI can report the usage to CSSM directly. These conditions result in license reporting:

- A successful Trust Code installation
- On every default Reporting Interval
- On-device Reload/Boot-up
- A switchover
- A stack member addition or removal
- Manual trigger of license sync

License reporting to CSSM can be triggered with these CLI:

```
Switch#license smart sync all
```

The Usage Reporting section in the `show license status` tells you the timelines of the last ACK received, the next ACK deadline, the next report push, and the last report push.

```
Usage Reporting:
Last ACK received: Nov 03 12:57:01 2020 UTC
Next ACK deadline: Dec 03 12:57:01 2020 UTC
Reporting push interval: 30 days
Next ACK push check: <none>
Next report push: Nov 07 22:50:35 2020 UTC
Last report push: Nov 03 12:55:57 2020 UTC
Last report file write: <none>
```

Direct Connect - Smart Transport

On a Direct Connect or Direct Cloud Access mode topology, if SMART Transport is used, these are the required configurations on the device.

```
Configure the desired Transport mode using below CLI.

Switch(config)#license smart transport smart

Running config on Smart Transport Mode:
!
license smart url smart https://smartreceiver.cisco.com/licservice/license
license smart transport smart
!
```

Direct Connect - Call-Home Transport

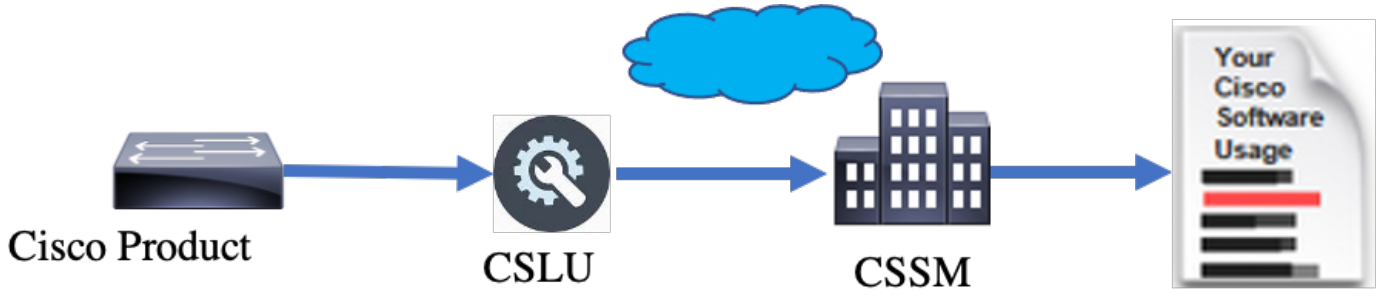
On a Direct Connect or Direct Cloud Access mode topology, if Call-home Transport is used, these are the required configurations on the device.

```
Configure the desired Transport mode using below CLI.

Switch(config)#license smart transport callhome

Running config on Smart Transport Mode:
!
service call-home
!
call-home
contact-email-addr shmandal@cisco.com
no http secure server-identity-check
profile "CiscoTAC-1"
active
reporting smart-licensing-data
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination transport-method http
!
```

Note: By default, the destination address for Call-home is configured to CSSM URL. This can be verified in the `show run all` configuration.

SLP - CSLU

The CSLU mode is the default Transport Mode on the factory shipped devices that run 17.3.2 or later. Also, if you migrate from Eval/Eval expired licenses, the transport mode after you move to SLP is CSLU. In CSLU-based Topology, the CSLU sits in between the PI and CSSM. CSLU avoids users not to have direct network connectivity to Cisco Cloud - CSSM. CSLU can run locally on a private network and download usage reports from all the associated PIs. The Usage Reports are locally saved on the Windows PC before they are sent to the CSSM through the internet. CSLU is a lightweight tool. You can only see the list of PIs associated with it and it can be identified with the use of UDIs. CSLU cannot display or contain the Redundancy Information of PI or License Levels or License Usage.

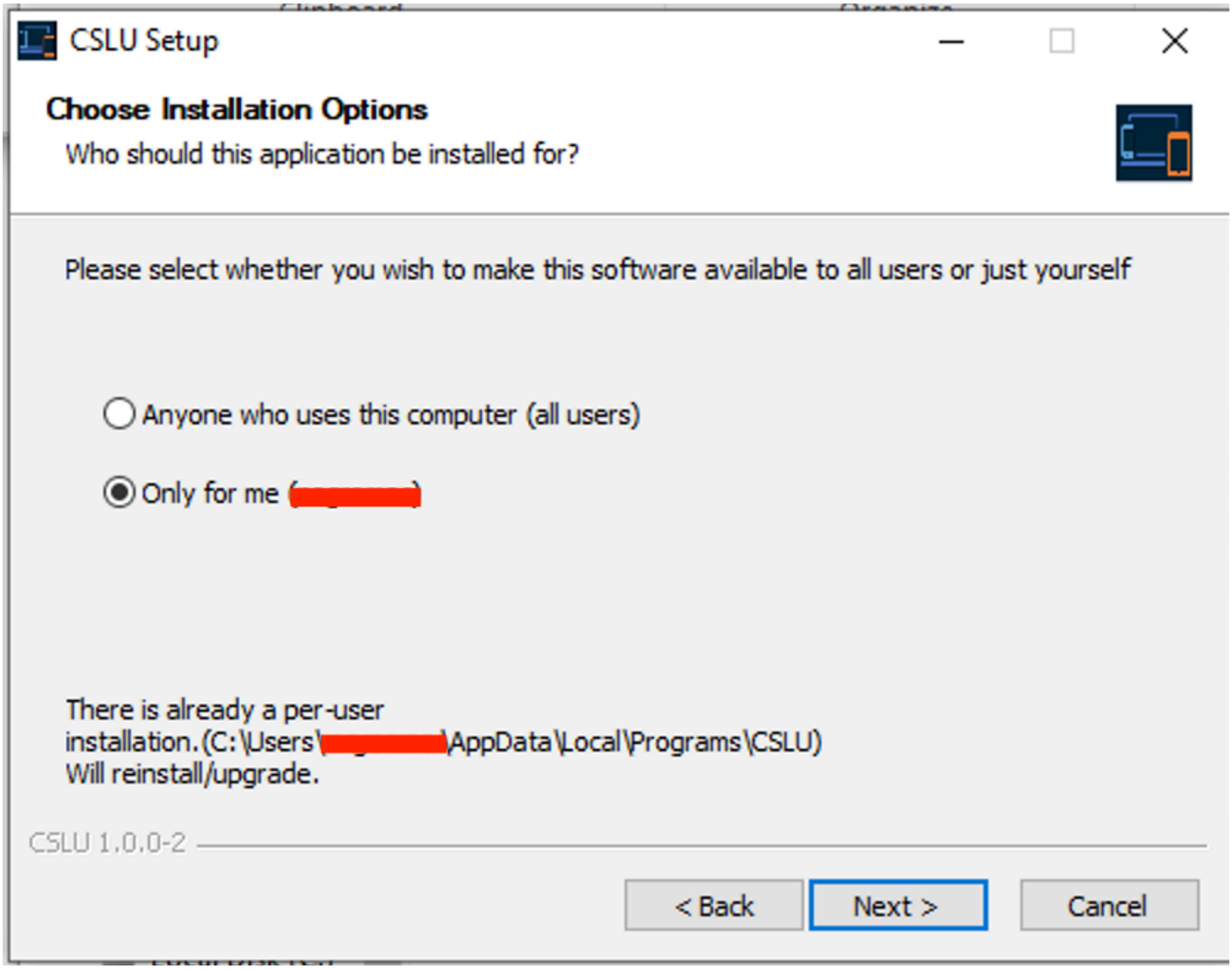


CSLU Installation and Configuration

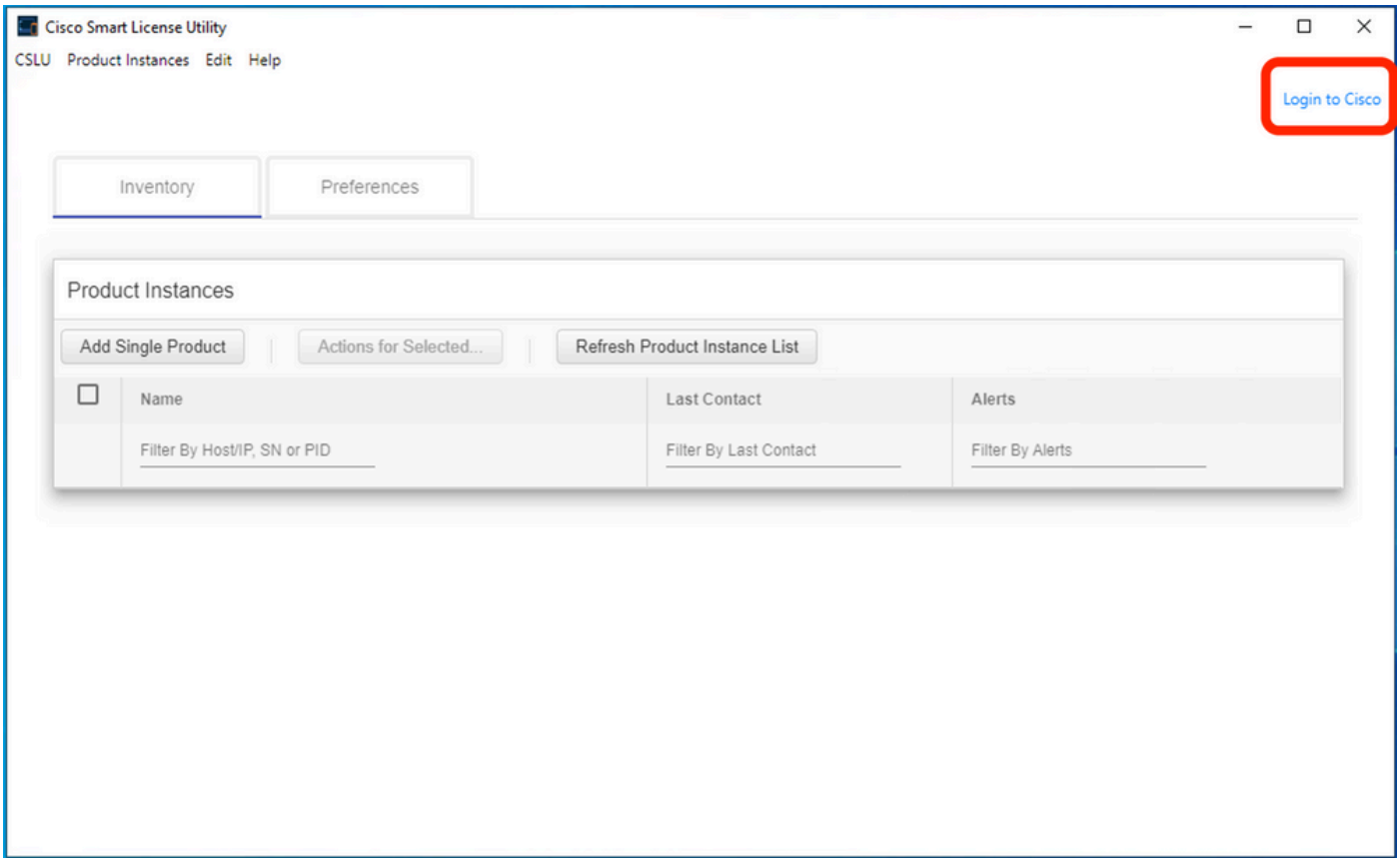
CSLU tool is installed and operated on Windows 10 machines. The software is available in the CCO to download and for usage free of cost. Once the tool is installed, the Quick Start Guide/User Manual can be downloaded from the Help Menu, navigate to Help > Download Help Manual.

CSLU installation requires you to accept the License Agreement.

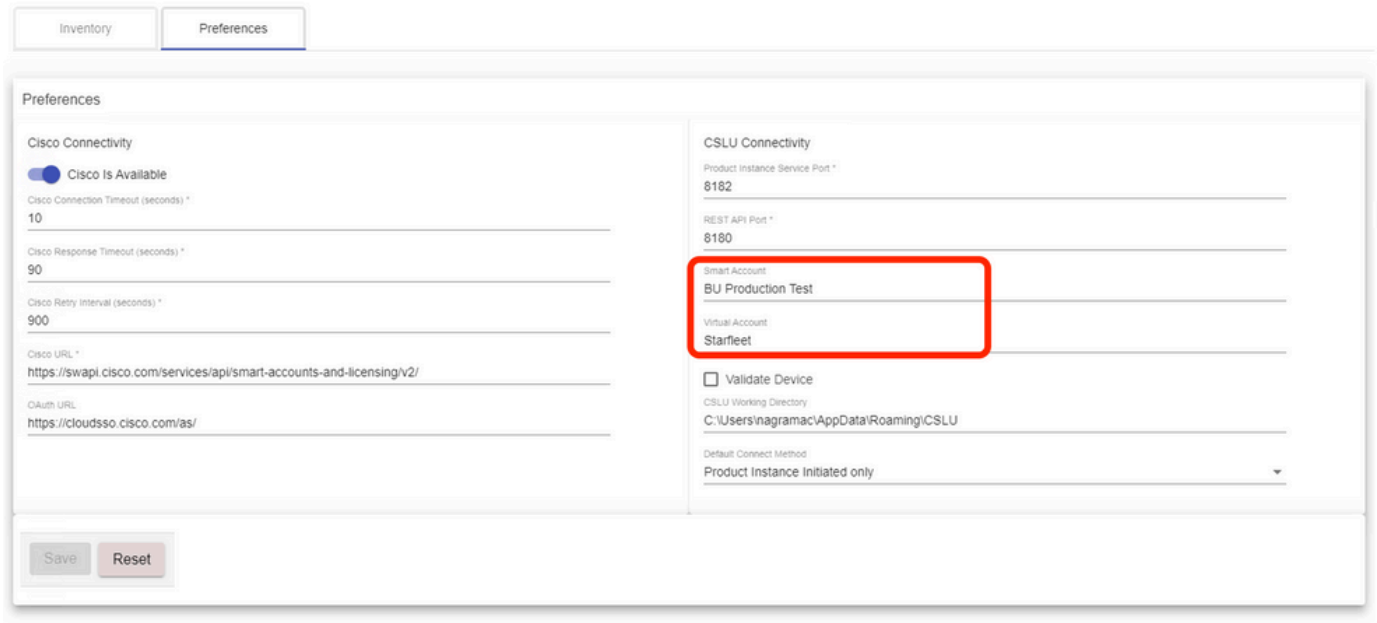
It is recommended that the application is installed only for the current user and not for all users who work on the computer. If an earlier version of CSLU is already present on the PC, it is a good practice to uninstall it beforehand. Nevertheless, the new installation takes care to upgrade the software.



After installation, log in to Cisco, with the use of the login option present in the top right corner of the application. This uses your CEC credentials. And through login, trust is established between CSLU and CSSM.

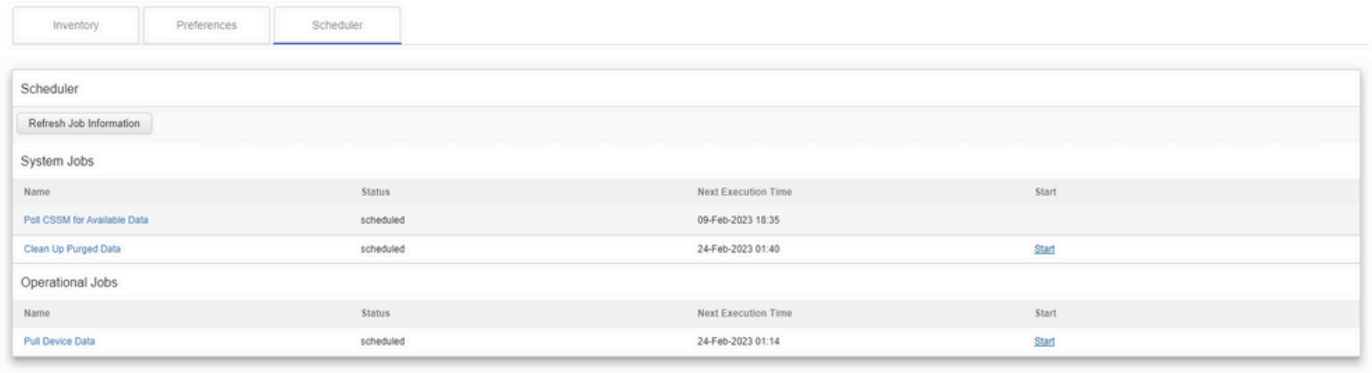


After you log in to Cisco, ensure the SA and VA details are chosen correctly through the drop-down menu, in the Preference Pane of the tool. Ensure to save the configurations.



Schedular Tab on CSLU - Through the schedular tab on CSLU, you can configure these:

- Poll CSSM for available data - Shows the job timings, last pull time, and the next pull time of data from CSSM.
- Clean up purged data - Removes all the purged data from the CSLU datastore. It can be triggered manually as well.
- Pull device data - Triggers the CSLU pull mode.



CSLU Using PUSH Mode

CSLU by default operates in PUSH mode. In PUSH mode, the PI sends the usage reports to CSLU at regular intervals. From the device, you must ensure the L3 network reachability to CSLU is available. For the PI to talk to CSLU, the IP address of the Windows machine that runs CSLU must be configured.

```
Switch(config)#license smart url cslu http://<IP_of_CSLU>:8182/cslu/v1/pi

The same can be verified through 'show license status' CLI

Switch#show license status

Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%

No time source, 20:59:25.156 EDT Sat Nov 7 2020



Utility:

Status: DISABLED



Smart Licensing Using Policy:

Status: ENABLED



Data Privacy:

Sending Hostname: yes

Callhome hostname privacy: DISABLED

Smart Licensing hostname privacy: DISABLED

Version privacy: DISABLED
```

Transport:

Type: cslu

Cslu address: http://<IP_of_CSLU>:8182/cslu/v1/pi

Proxy:

Not Configured

Policy:

Policy in use: Merged from multiple sources.

Reporting ACK required: yes (CISCO default)

Unenforced/Non-Export Perpetual Attributes:

First report requirement (days): 365 (CISCO default)

Reporting frequency (days): 0 (CISCO default)

Report on change (days): 90 (CISCO default)

Unenforced/Non-Export Subscription Attributes:

First report requirement (days): 90 (CISCO default)

Reporting frequency (days): 90 (CISCO default)

Report on change (days): 90 (CISCO default)

Enforced (Perpetual/Subscription) License Attributes:

First report requirement (days): 0 (CISCO default)

Reporting frequency (days): 0 (CISCO default)

Report on change (days): 0 (CISCO default)

Export (Perpetual/Subscription) License Attributes:

First report requirement (days): 0 (CISCO default)

Reporting frequency (days): 0 (CISCO default)

Report on change (days): 0 (CISCO default)

Miscellaneous:

Custom Id: <empty>

```
Usage Reporting:

Last ACK received: <none>

Next ACK deadline: Feb 05 15:32:51 2021 EDT

Reporting push interval: 30 days

Next ACK push check: <none>

Next report push: Nov 07 15:34:51 2020 EDT

Last report push: <none>

Last report file write: <none>

Trust Code Installed: <none>
```

Reports are sent to CSLU from PI on these conditions:

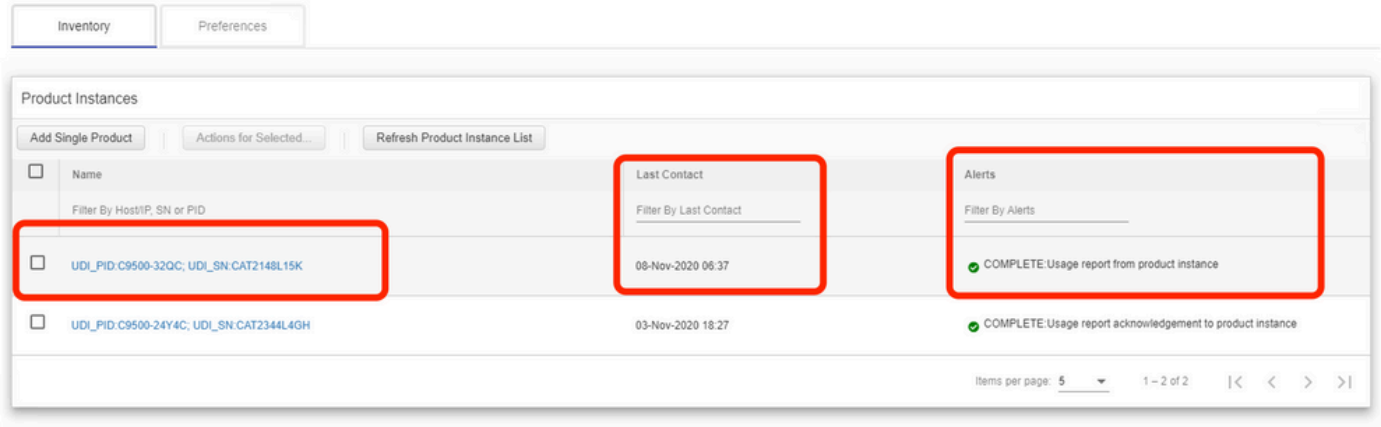
- On every default reporting interval
- On-device Reload/Boot-up
- On Switchover
- On stack member addition or removal
- On manual trigger of License sync

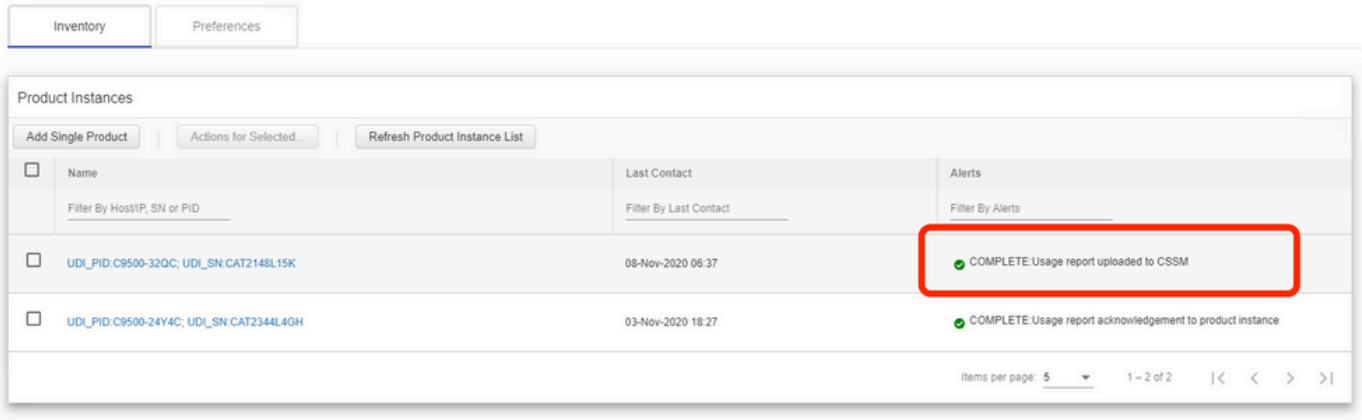
In CSLU, the inventory page lists the devices currently associated with CSLU. The devices in the list can be identified through the UDI. The devices can be filtered based on PID or SN from the list to identify any particular device.

The CSLU inventory page also has two other columns:

- The **Last Contact** column - Shows the latest Time Stamp when the status of reporting has changed.
- The **Alert Column** - Shows the latest reporting status of the PI.

Once the PI sends the report to CSLU, CSLU creates the PI entry in CSSM. The Last Contact TS as well as the Alerts status is updated.





CSSM processes the reports sent by CSLU and adds/updates the product instance on CSSM, based on the license usage. Once the CSSM processes and updates the date, it sends back the ACK message to CSLU. CSLU in turn stores and forwards the message back to PI.

The ACK message consists of:

- Acknowledgment for all the reports sent
- Policy
- Trust Code

If a new policy is available for you in the CSSM, it is now updated to the PI as well. If the policy is unchanged, the same is pushed to PI.

Note: If ACK message reporting is not required as per your policy, the ACK message is not sent.

The alert message column can have one of these statuses:

- Usage report from product instance
- Usage report uploaded to Cisco
- Sync request from product instance
- Sync request uploaded to CSSM
- Acknowledgment received from CSSM
- Usage report acknowledgment to product instance

Note: In CSLU on a HA system, always the entry is seen only for UDI of the Active. Only CSSM has all the UDI for individual devices in the system listed.

CSLU Auto Discovery

To support scale deployments with minimal configurations, auto-discovery of the CSLU is supported. This means you do not have to configure the IP address/URL of the CSLU specifically. In order to achieve this, you only have to add an entry to their DNS server. This lets the device, that has transport mode as CSLU (which is the default), automatically discover CSLU and send reports.

A couple of things to ensure here:

- Create an entry in the DNS server. The IP address of the CSLU must be mapped to the name cslu-local.
- Ensure the name server and DNS configurations are present in the device for reachability.

With this, without any additional configurations, the devices in the network can reach CSLU and send RUM reports at regular intervals.

CSLU Using PULL Mode

PULL mode is where the CSLU initiates the process to fetch the RUM reports from the devices. Here the device details are added to the CSLU and CSLU fetches the data on all the added devices at regular intervals. The PULL from CSLU can also be triggered manually. CSLU in turn sends the RUM report to CSSM, and ACK messages that are received back from CSSM are sent to the PI. PULL mode is supported by three different means - RESTAPI, NETCONF, and RESTCONF.

PULL Mode Using RESTAPI

For PULL mode to work through RESTAPI, the configurations required from the device and CSLU are:

```
Configs on PI:

Ensure the network reachability from PI to CSLU is available and working.

!
 ip http server
 ip http authentication local
 ip http secure-server
!
 aaa new-model
 aaa authentication login default local
 aaa authorization exec default local
 username admin privilege 15 password 0 lab
!
```

Note: The user must have Priv level 15 access.

CSLU - Procedure to Setup

CSLU must be logged in to CSSM for reports to be synced automatically.

Step 1. Choose Add Single Product on the inventory page.

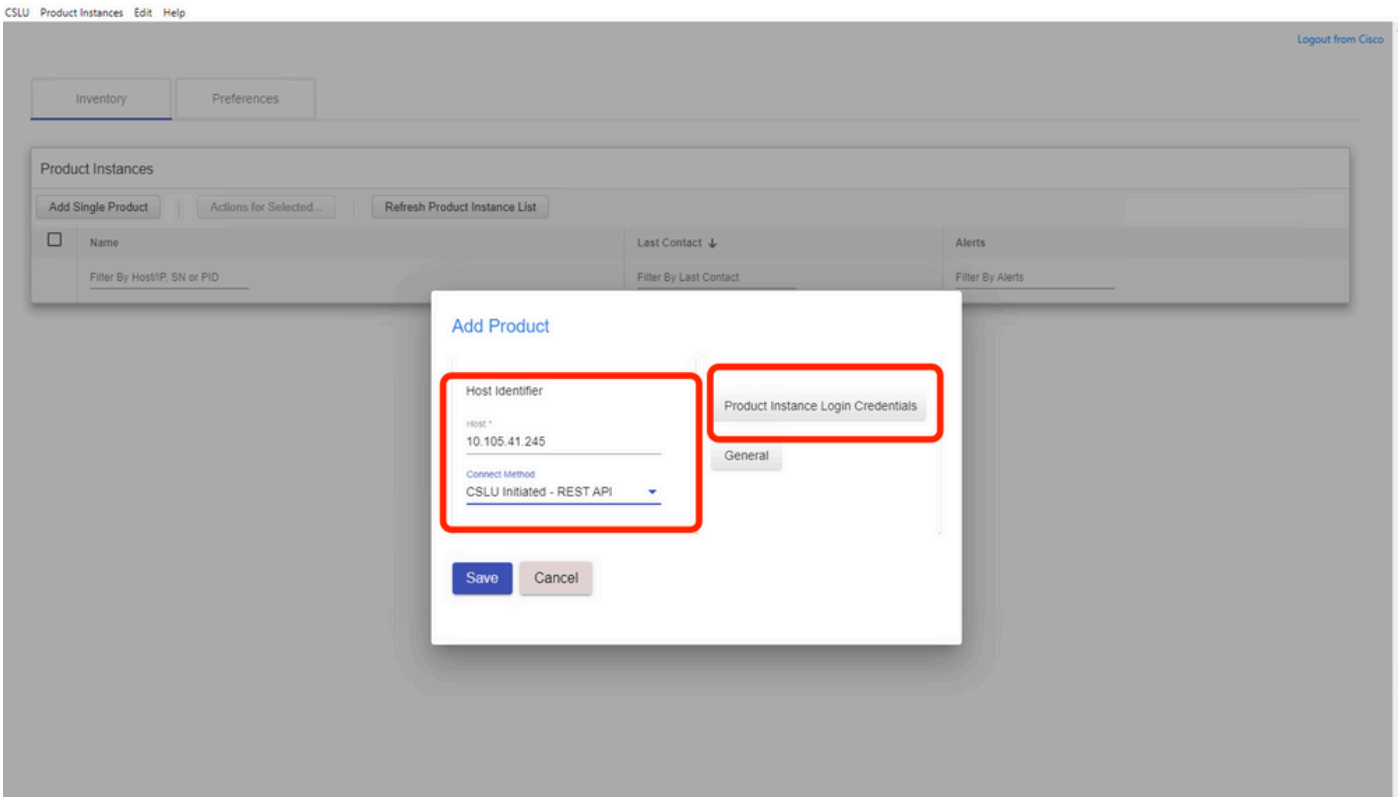
Step 2. Enter the device IP.

Step 3. Choose the connect method as RestAPI.

Step 4. Choose product instance Login Credentials.

Step 5. Enter the user credentials of the user with Priv 15 access.

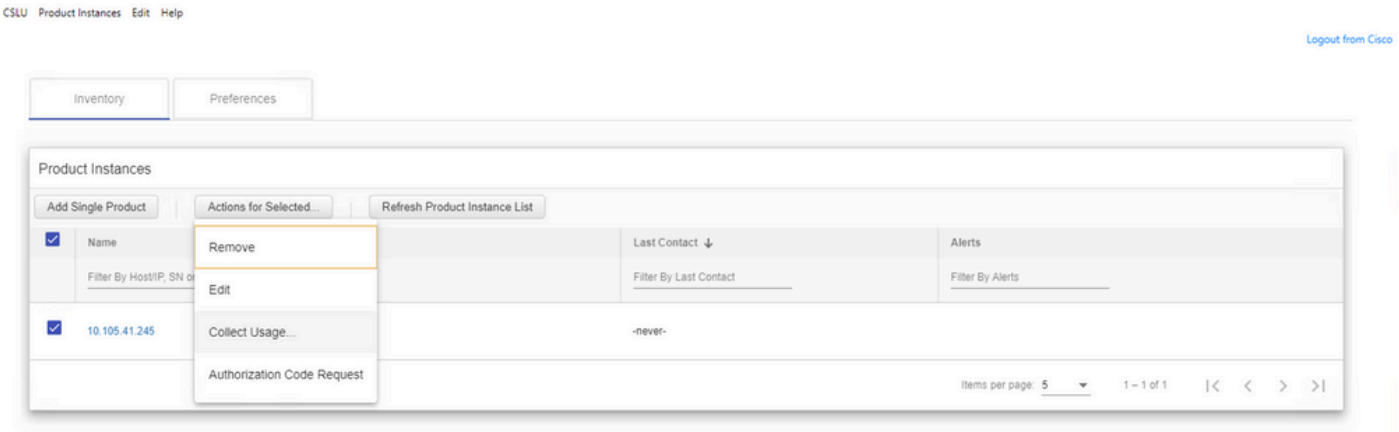
Step 6. Save the configurations.

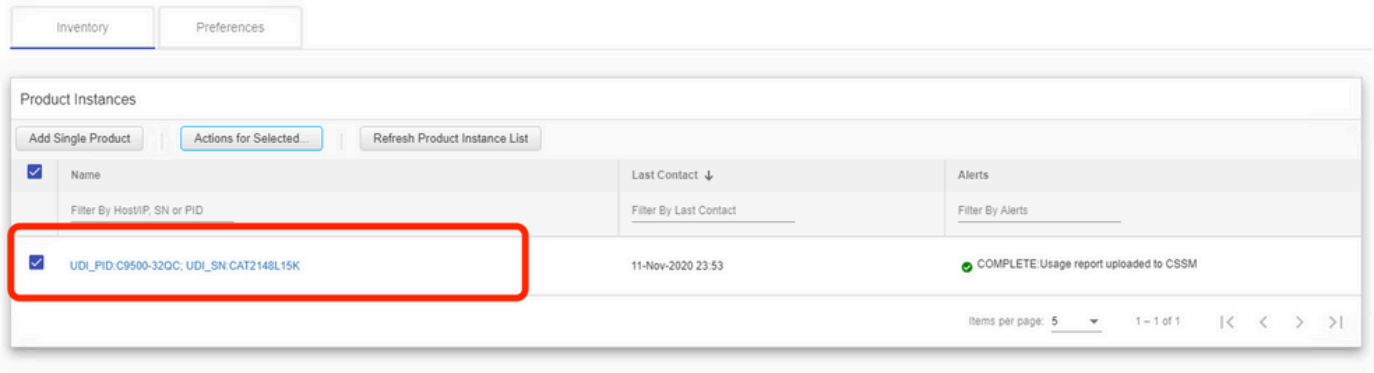


The device is added with an only IP address in the Name field.

Choose the device and navigate to Actions for Selected > Collect Usage.

Once the usage data is successfully collected, the Name field updates to the UDI of the PI, and the timestamp is updated as well. The alert field reflects the latest status.





If the device is still available when the ACK message is received from CSSM, the ACK is sent back to PI. Else, ACK is sent on the next Pull Interval.

PULL Mode Using RESTCONF

For PULL mode to work through RESTCONF , the configurations required from the device and steps from CSLU are:

```
Configs on PI:

!
restconf
!
 ip http secure-server
 ip http authentication local
 ip http client source-interface GigabitEthernet 0/0
!
 username admin privilege 15 password 0 lab
!
```

Note: These configurations are for local authentication. Remote authentication can be also used.

CSLU - Procedure to Setup

CSLU must be logged in to CSSM for reports to be synced automatically. CSLU setup is the same as RESTAPI for RUM report collection and reporting.

Step 1. Choose Add Single Product on the inventory page.

Step 2. Enter the Device IP.

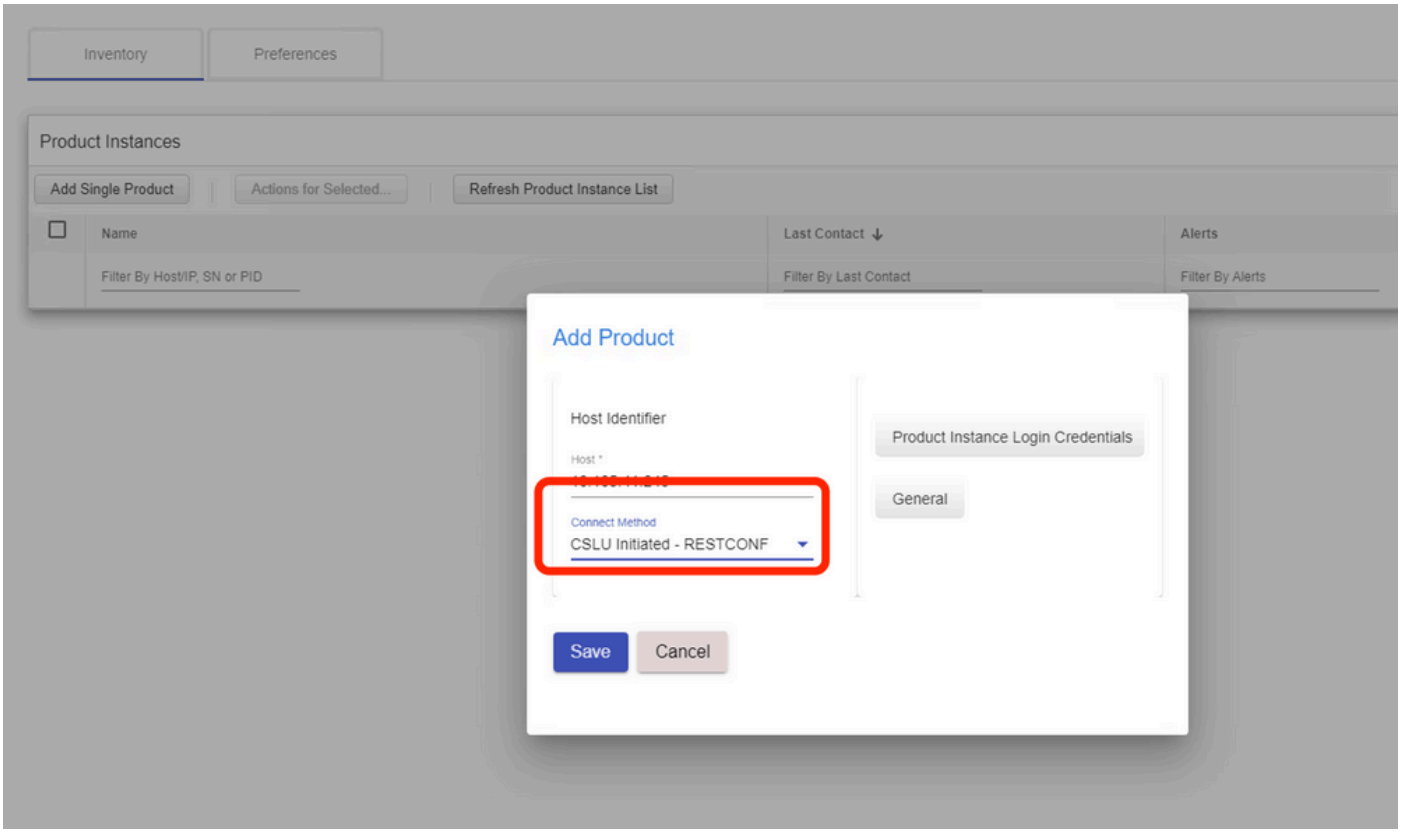
Step 3. Choose the connect method as RESTCONF.

Step 4. Choose product instance Login Credentials.

Step 5. Enter the user credentials of the user with Priv 15 access.

Step 6. Save the configurations.

Step 7. Collect usage data for the selected device.



PULL Mode Using NETCONF

For PULL mode to work through NETCONF, the configurations required from the device and steps from CSLU are:

```
Configs on PI:

!
 ip ssh version
!
 netconf-yang
 netconf ssh
 netconf-yang feature candidate-datastore
!
 username admin privilege 15 password 0 lab
!

To ensure yang process is running, execute the command:

Switch#show platform software yang-management process
confd    : Running
nesd     : Running
syncfd   : Running
ncsshd   : Running
dmiauthd : Running
nginx    : Running
ndbmand  : Running
pubd     : Running
gnmib    : Not Running
```

Note: These configurations are for local authentication. Remote authentication can be also used.

CSLU - Procedure to Setup

CSLU must be logged in to CSSM for reports to be synced automatically. CSLU setup is the same as RESTAPI for RUM report collection and reporting.

Step 1. Choose Add Single Product on the inventory page.

Step 2. Enter the Device IP.

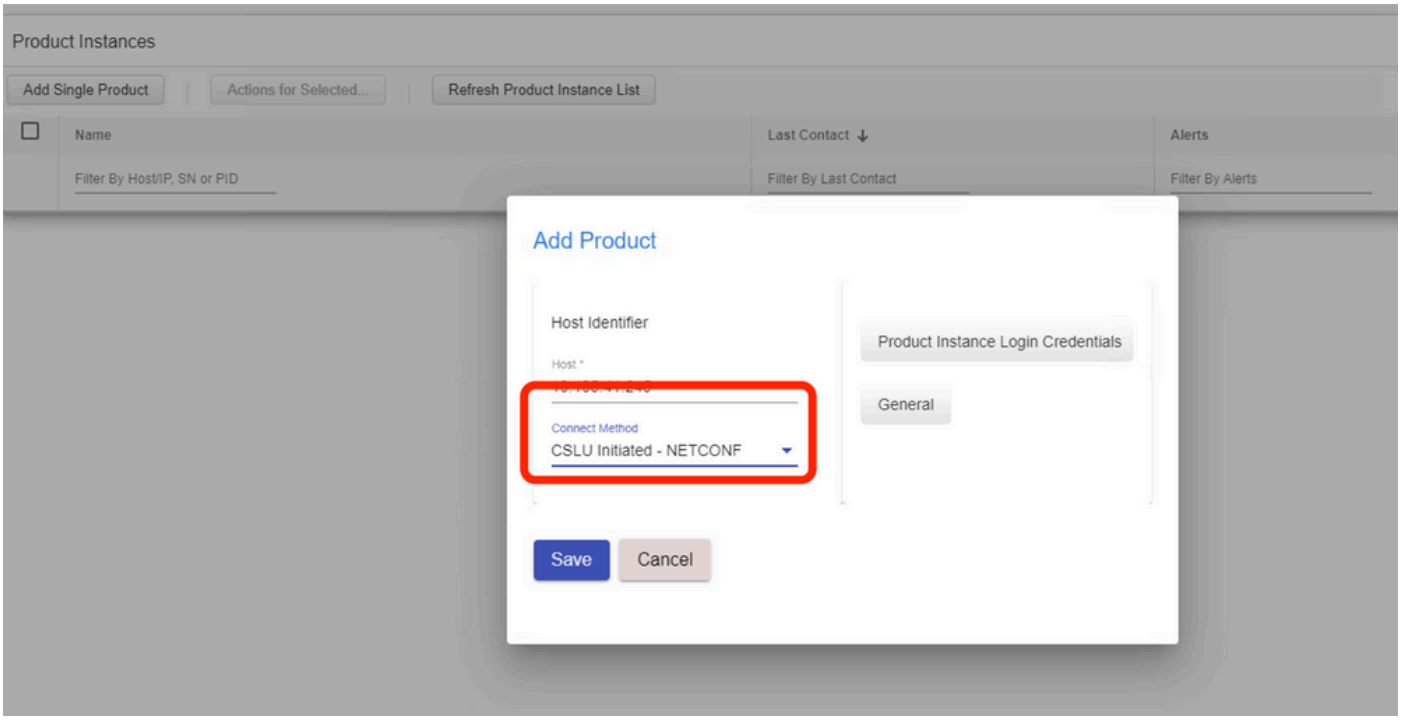
Step 3. Choose the connect method as NETCONF.

Step 4. Choose product instance Login Credentials.

Step 5. Enter the user credentials of the user with Priv 15 access.

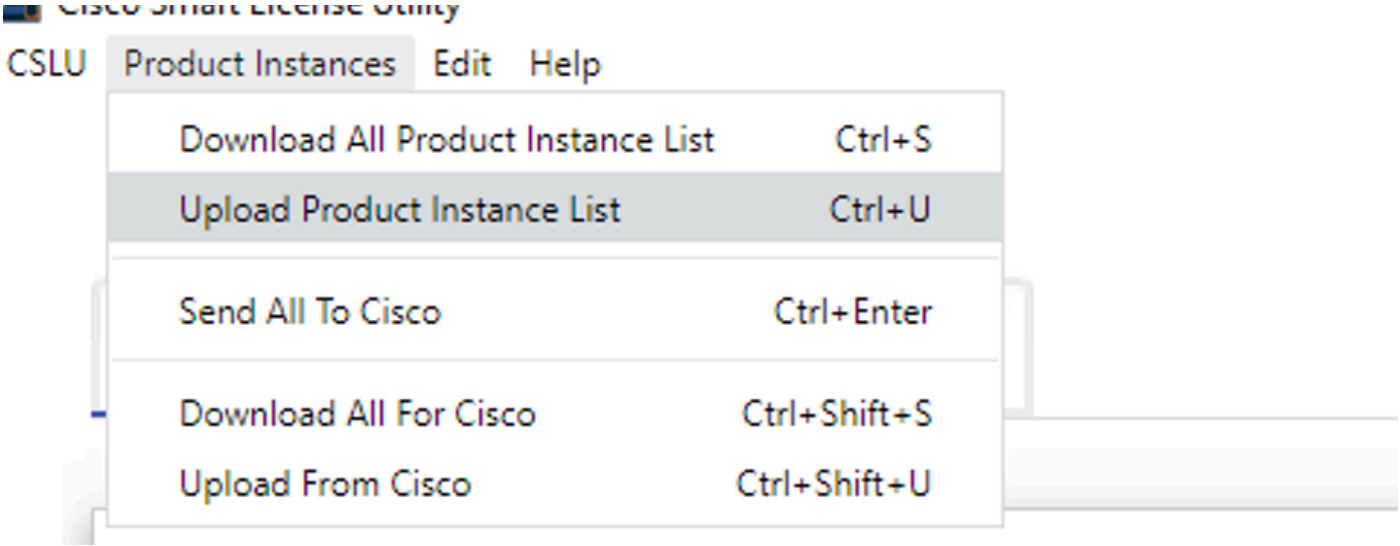
Step 6. Save the configurations.

Step 7. Collect usage data for the selected device.

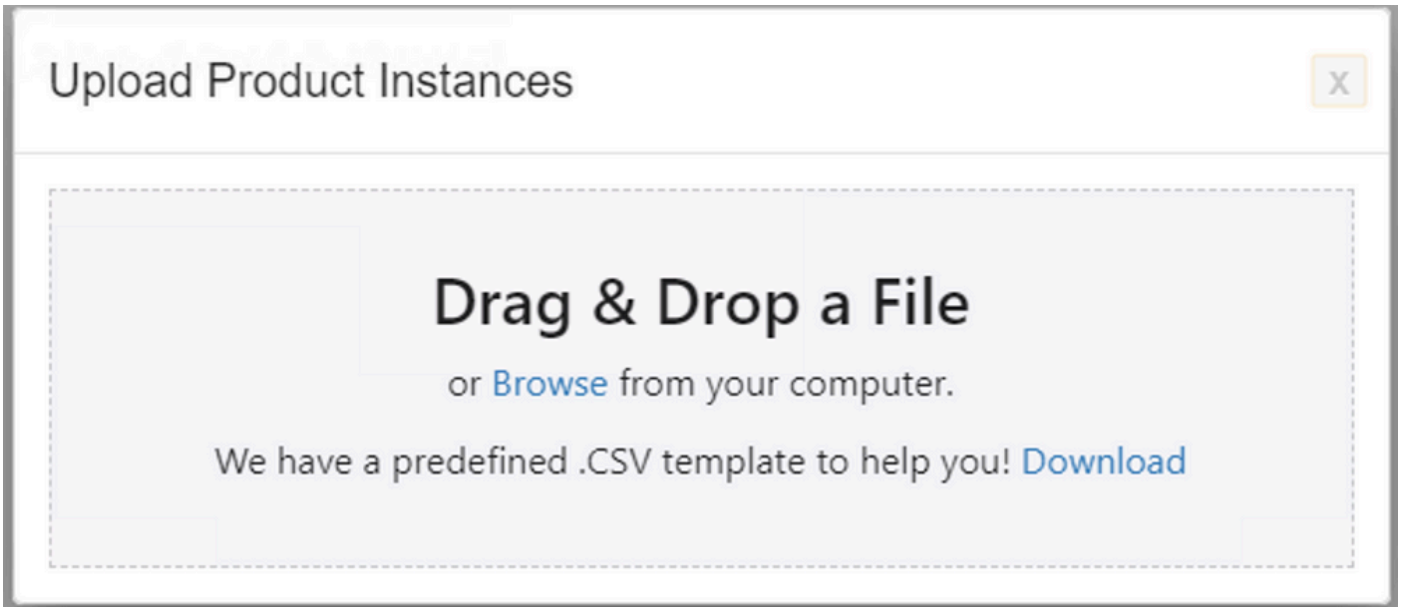


Note: For all models, NETCONF, RESTCONF, and RESTAPI, the device list can be added in bulk.

In order to perform the bulk upload, on the Menu bar, navigate to Product Instance > Upload Product Instance List, as shown in this image.



A new pop-up window opens. The template file can be downloaded from it. In the CSV format file, fill in the device details of the list of devices and upload to CSLU to add multiple devices.



Note: For all the types of CSLU PULL mode, it is recommended to set the transport set to Off on the PI. This can be done with the use of CLI.

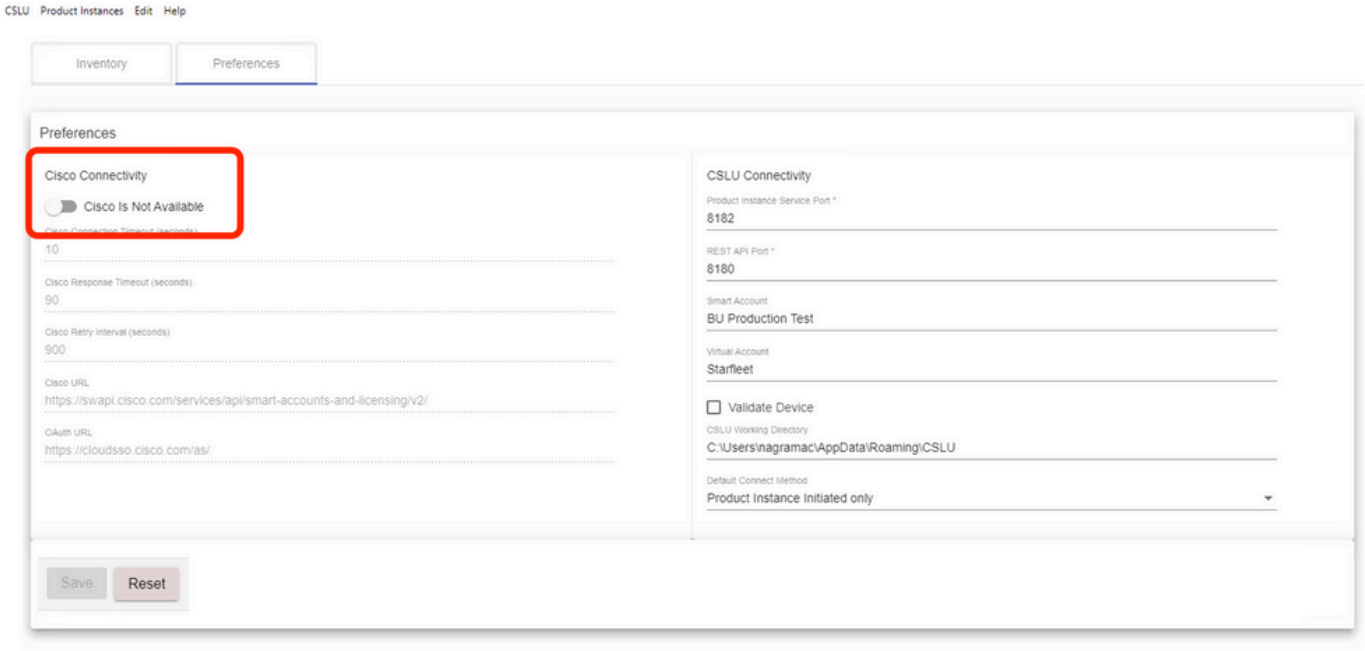
```
Switch(config)#license smart transport off
```

CSLU Using Disconnected Mode

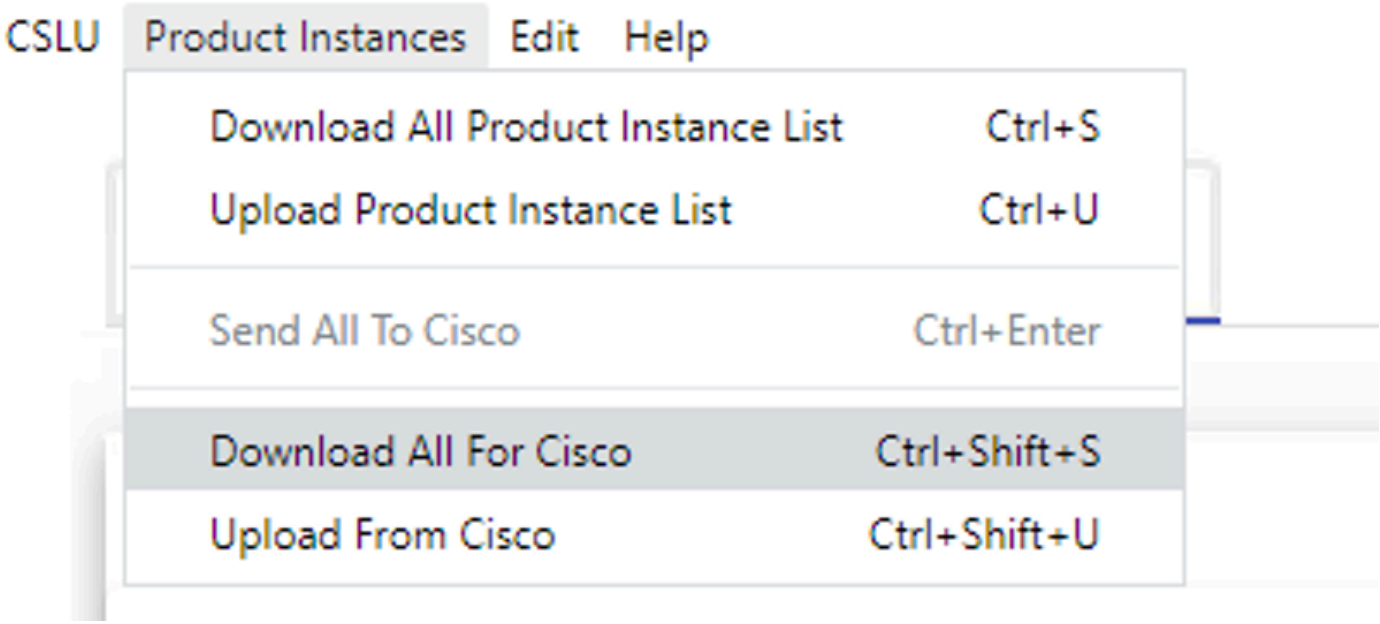
CSLU can operate in disconnected mode from CSSM. This is for any deployments that do not allow the CSLU to be connected to the internet. In the disconnected mode, the reports of all the devices are downloaded manually from CSLU and uploaded to CSSM. In turn, ACK messages are downloaded from CSSM and uploaded to CSLU. CSLU still continues to PULL/PUSH usage dates from PIs and also sends back the ACK message to PI.

Step 1. On CSLU Preference page, turn off the option Cisco Connectivity. This confirms that Cisco is not available.

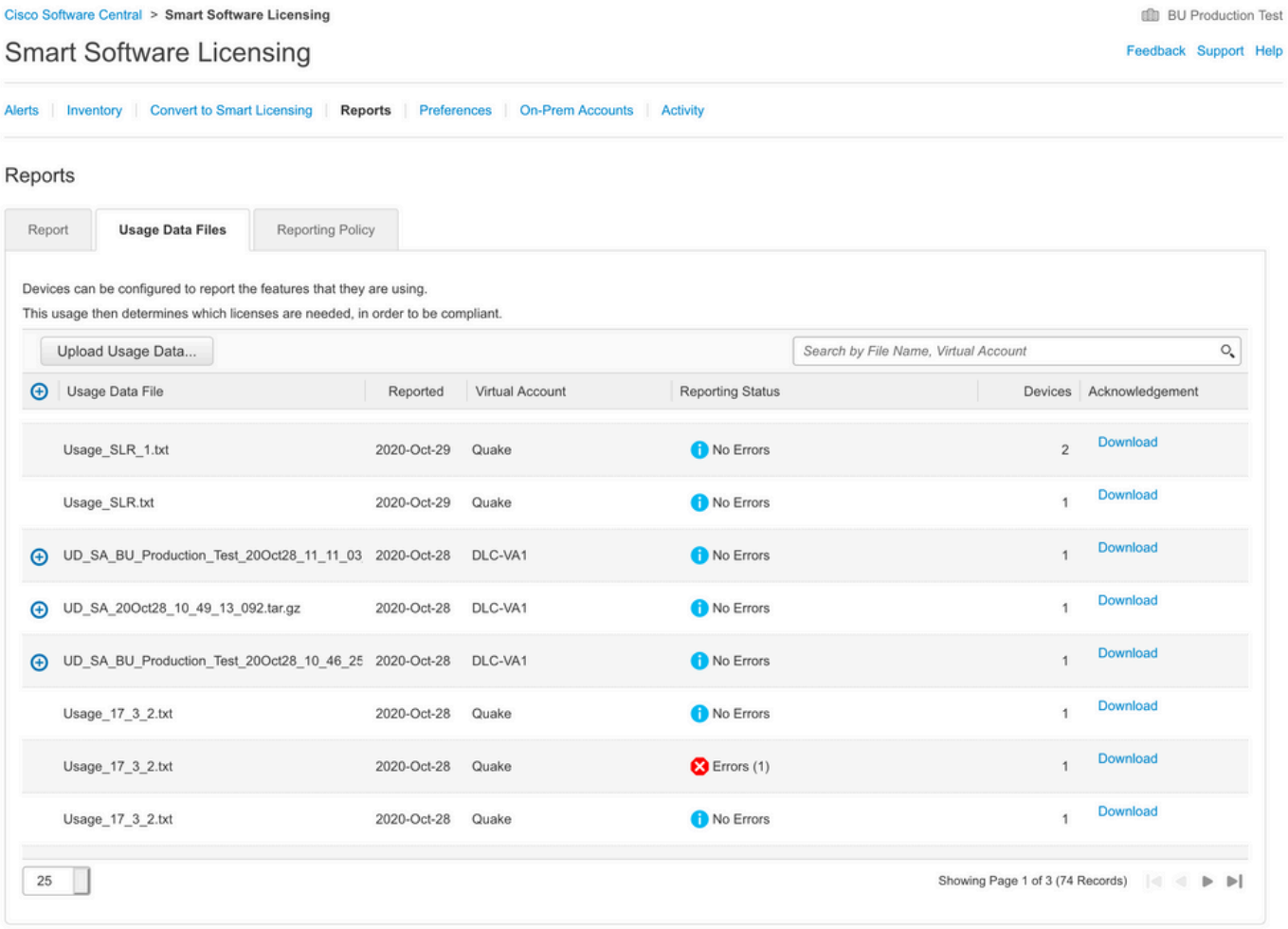
Step 2. Save the settings.

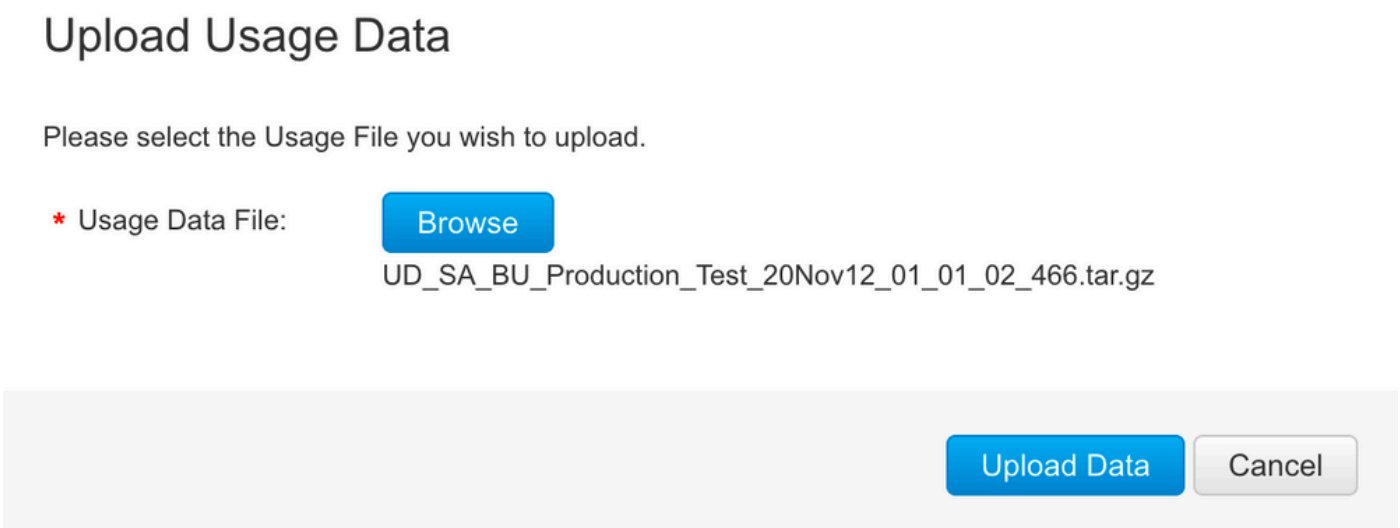


Step 3. In the Menu bar, click Product Instances > Download All for Cisco. This downloads a tar.gz file to the CSLU.

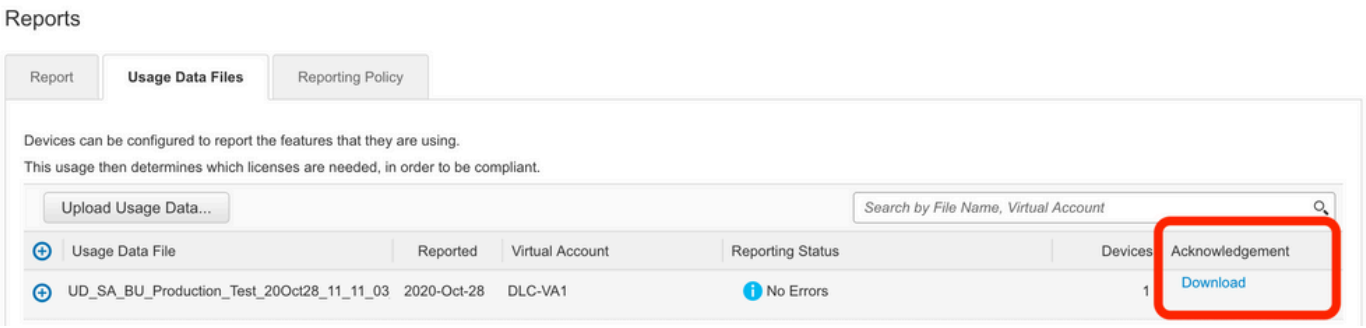


Step 4. Upload the file to CSSM. In the CSSM Smart Account page, navigate to Report > Usage Data Files > Upload usage data. In the pop-up, upload the tar.gz file.

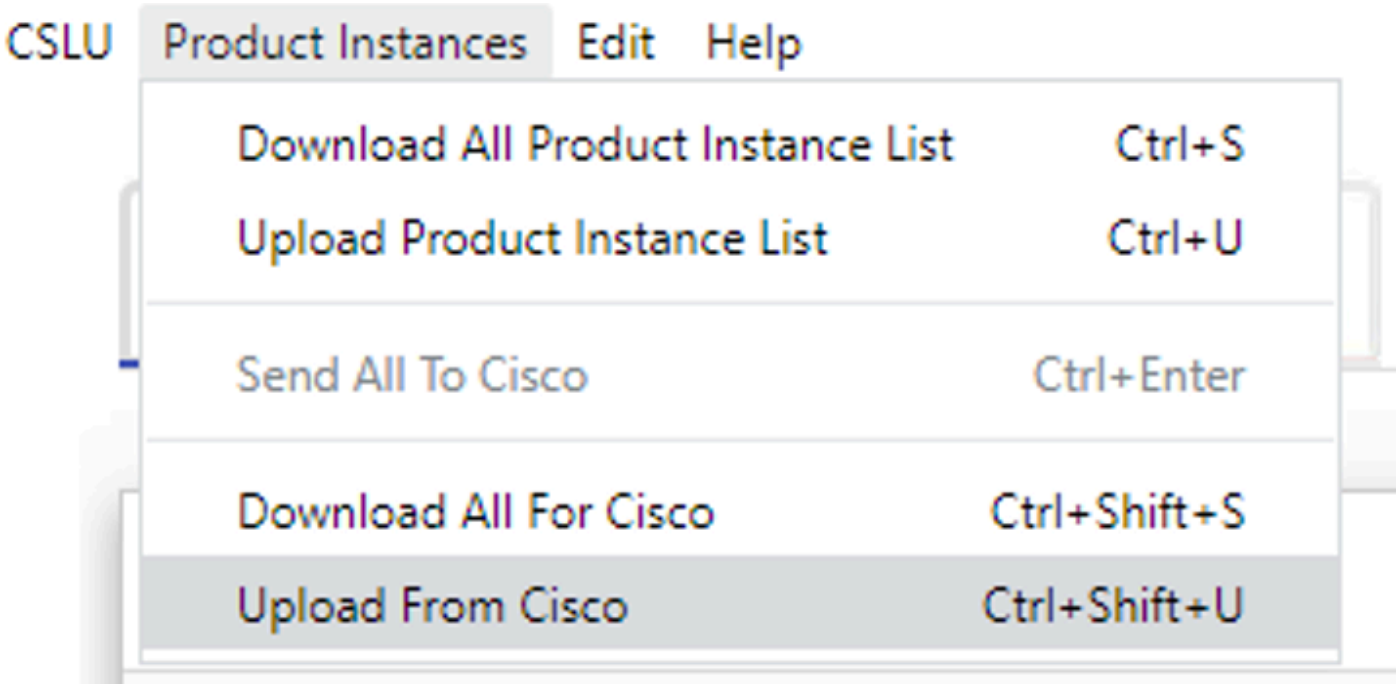




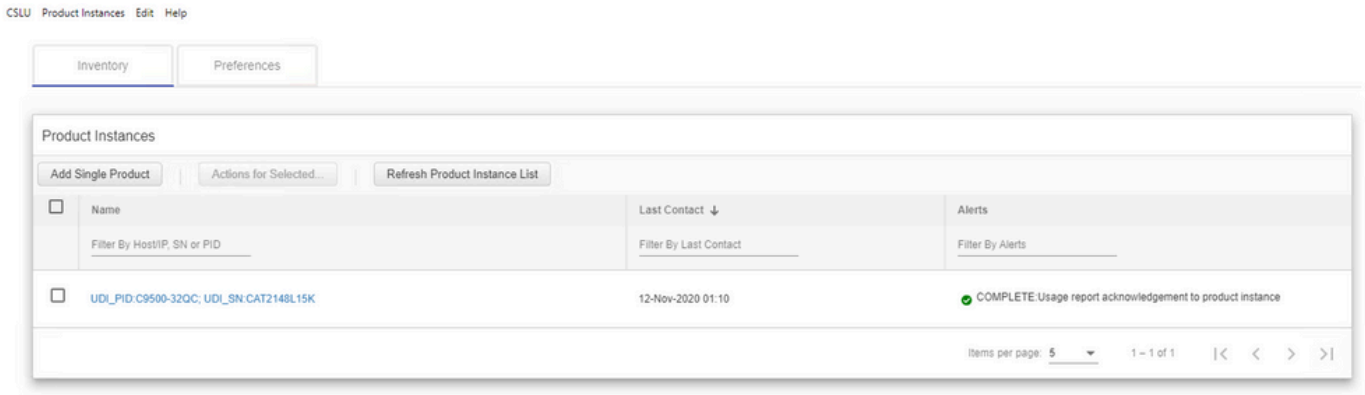
Step 5. Once the data is processed, the Acknowledgment is generated. Download the ACK file and upload it to CSLU.



Step 6. In CSLU, import the ACK file from the Menu bar, and navigate to Product Instances > Upload from Cisco, as shown in this image.



Step 7. Once the ACK is uploaded, the message is sent to the PIs. The same can be verified by the Alerts column.



SLP - Offline Mode

SLP can also work in total Offline Mode. This is mainly for air-gapped networks, that do not prefer internet connectivity and also choose not to use CSLU. In the offline mode, the transport is set to Off.

```
Switch(config)#license smart transport off

Same can be verified through, 'show license status'

Switch#show license status

Utility:
Status: DISABLED

Smart Licensing Using Policy:
Status: ENABLED

Data Privacy:
Sending Hostname: yes
Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
Type: Transport Off

Policy:
Policy in use: Merged from multiple sources.
Reporting ACK required: yes (CISCO default)
Unenforced/Non-Export Perpetual Attributes:
First report requirement (days): 365 (CISCO default)
Reporting frequency (days): 0 (CISCO default)
Report on change (days): 90 (CISCO default)
Unenforced/Non-Export Subscription Attributes:
First report requirement (days): 90 (CISCO default)
Reporting frequency (days): 90 (CISCO default)
Report on change (days): 90 (CISCO default)
Enforced (Perpetual/Subscription) License Attributes:
First report requirement (days): 0 (CISCO default)
Reporting frequency (days): 0 (CISCO default)
Report on change (days): 0 (CISCO default)
Export (Perpetual/Subscription) License Attributes:
First report requirement (days): 0 (CISCO default)
Reporting frequency (days): 0 (CISCO default)
Report on change (days): 0 (CISCO default)



Miscellaneous:
Custom Id: <empty>

Usage Reporting:
Last ACK received: Nov 11 15:41:10 2020 EDT
Next ACK deadline: Dec 11 15:41:10 2020 EDT
Reporting push interval: 30 days
Next ACK push check: <none>
Next report push: Dec 07 21:42:30 2020 EDT
Last report push: Nov 07 21:42:30 2020 EDT
Last report file write: <none>

Trust Code Installed: <none>
```

Whenever you want to report the usage data to CSSM, the usage reports have to be downloaded as a file and manually uploaded to CSSM. In a HA system, active collects usage for standby/member devices.

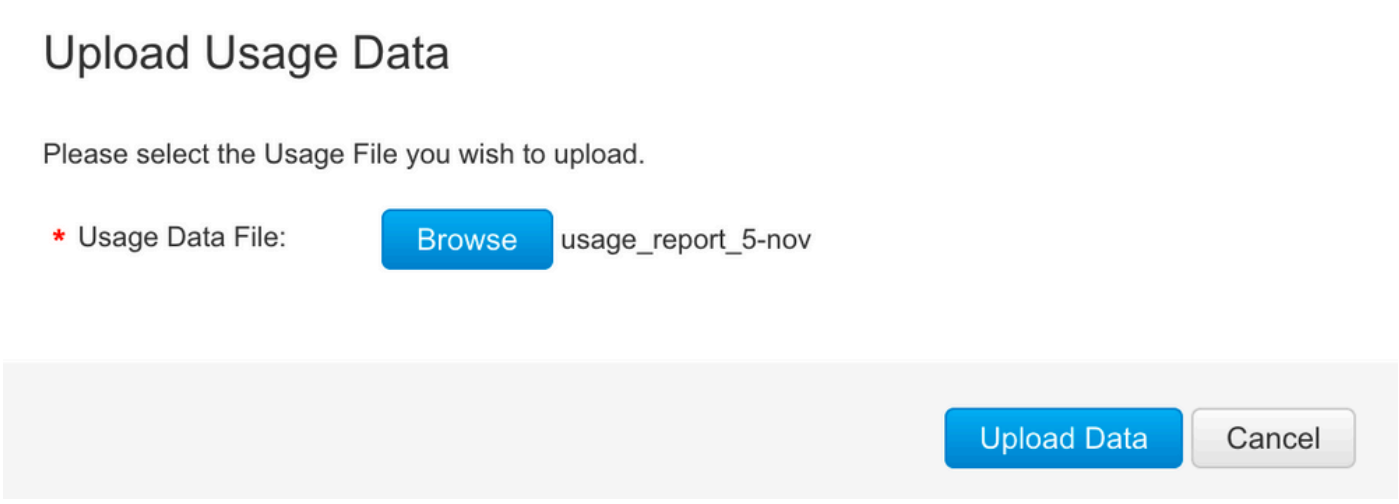
```
To download the usage data from PI -

Switch#license smart save usage unreported file bootflash:<file-name>

Above option 'unreported' is recommended to use. This downloads only the files that are yet to be repor
and discard old usage reports, that were Acknowledged.


However, there are other options available for the amount of data that needs to be reported.
For downloading all the available report use option all,
# of daya can be specified


Switch#license smart save usage ?
all Save all reports
days Save reports from last n days
rum-Id Save an individual RUM report
unreported Save all previously un reported reports
```

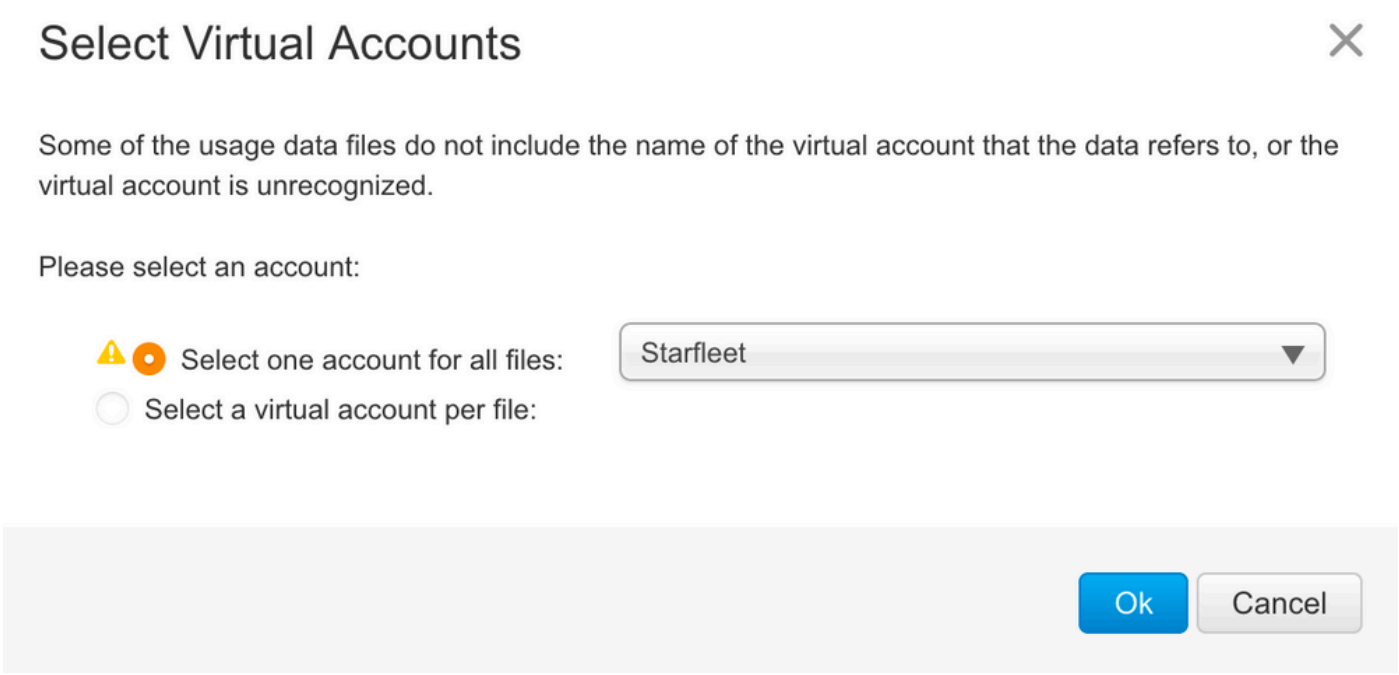
Now, this report has to be manually uploaded to CSSM.

Export the saved usage data from PI to the desktop.

On the CSSM Smart Account page, navigate to Report > Usage Data Files > Upload usage data. In the pop-up window, choose the usage report and click upload.

Once the file is uploaded, you must choose the correct VA with which the device is associated.





Once the data is processed completely and acknowledgment is ready, download the file and load it onto the PI.

```
To import the ACK to PI,
Switch#license smart import bootflash:<file-name>
Import Data Successful

Switch#
Nov 11 20:23:06.783: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy was successfully insta
Switch#

Policy Installed syslog is displayed on console if successful.

Also, the same can be verified using CLI, 'show license all'. The field 'Last ACK received' tells the
last TimeStamp when ACK message was received.


Switch#show license all
Load for five secs: 0%/0%; one minute: 1%; five minutes: 0%
No time source, 16:23:22.294 EDT Wed Nov 11 2020

Smart Licensing Status
======================

Smart Licensing is ENABLED

Export Authorization Key:
Features Authorized:
<none>

Utility:
Status: DISABLED

Smart Licensing Using Policy:
Status: ENABLED

Data Privacy:
```

```
Sending Hostname: yes
Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
Type: Transport Off

Miscellaneous:
Custom Id: <empty>

Policy:
Policy in use: Installed On Nov 11 16:23:06 2020 EDT
Policy name: SLP Policy
Reporting ACK required: yes (Customer Policy)
Unenforced/Non-Export Perpetual Attributes:
First report requirement (days): 60 (Customer Policy)
Reporting frequency (days): 60 (Customer Policy)
Report on change (days): 60 (Customer Policy)
Unenforced/Non-Export Subscription Attributes:
First report requirement (days): 30 (Customer Policy)
Reporting frequency (days): 30 (Customer Policy)
Report on change (days): 30 (Customer Policy)
Enforced (Perpetual/Subscription) License Attributes:
First report requirement (days): 0 (CISCO default)
Reporting frequency (days): 90 (Customer Policy)
Report on change (days): 90 (Customer Policy)
Export (Perpetual/Subscription) License Attributes:
First report requirement (days): 0 (CISCO default)
Reporting frequency (days): 90 (Customer Policy)
Report on change (days): 90 (Customer Policy)

Usage Reporting:
Last ACK received: Nov 11 16:23:06 2020 EDT
Next ACK deadline: Dec 11 16:23:06 2020 EDT
Reporting push interval: 30 days
Next ACK push check: <none>
Next report push: Dec 07 21:42:30 2020 EDT
Last report push: Nov 07 21:42:30 2020 EDT
Last report file write: <none>

Trust Code Installed: <none>

License Usage
=============

network-advantage (C9500 Network Advantage):
Description: network-advantage
Count: 1
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: network-advantage
Feature Description: network-advantage
Enforcement type: NOT ENFORCED
License type: Perpetual

dna-advantage (C9500 32QC DNA Advantage):
Description: C9500-32QC DNA Advantage
Count: 1
Version: 1.0
Status: IN USE
```

```
Export status: NOT RESTRICTED
Feature Name: dna-advantage
Feature Description: C9500-32QC DNA Advantage
Enforcement type: NOT ENFORCED
License type: Subscription

Product Information
===================
UDI: PID:C9500-32QC,SN:CAT2148L15K

Agent Version
=============
Smart Agent for Licensing: 5.0.6_rel/47

License Authorizations
======================
Overall status:
Active: PID:C9500-32QC,SN:CAT2148L15K
Status: NOT INSTALLED

Purchased Licenses:
No Purchase Information Available
```

Behavior Changes

These changes are done on the Smart Licensing feature over releases:

- **Trust Sync** - From 17.7.1, Trust Code is installed on the switch on all supported topologies like CSLU and Offline methods.
- **Privacy Changes** - From 17.7.1, version string and hostname information from 17.9.1 are included in the RUM reports sent to CSSM, if respective privacy settings are disabled.
- **Account Details** - From 17.7.1, the ACK message from CSSM includes the Account information and SA/VA details.
- **RUM Report Throttling** -From 17.9.1, reporting interval of when the PI initiates communication is throttled. The minimum reporting frequency is throttled to one day. This means the product instance does not send RUM reports more than once a day.

Troubleshoot

Generic Troubleshooting Questionnaire

Scenario 1: Some protocols (that is, HSRP) do not work anymore after you upgrade the Cisco IOS XE from a very early release (that is, 16.9.x).

Check the license boot level to see if it is still the same as before you upgrade Cisco IOS XE. It is possible that the license boot level has been reset to Networking-Essentials which possibly does not support the failing protocols (that is, HSRP).

Scenario 2: License status with messages "Failure reason: Fail to send out Call Home HTTP message" or "Last Communication Attempt: PENDING’"

This can be related to basic connectivity issues. To resolve check:

1. Network connectivity to reach CSSM - IP address, Routes, and so on.

2. The ip http client source interface is configured correctly.
3. Time difference. (NTP needs to be configured to provide a correct clock time/zone)
4. If internal Firewall configuration blocks the traffic to CSSM

Scenario 3: What if log error "%SMART_LIC-3-AUTH_RENEW_FAILED: Authorization renewal with the Cisco Smart Software Manager (CSSM) : undefined method 'each' for nil:NilClass" is observed after one year of registration.

Re-register the product. Generate a new Token ID on CSSM and register the product instance again to CSSM**.**

Scenario 4: Error Message "%SMART_LIC-3-COMM_FAILED: Communications failure", when there are no connectivity errors with Cisco.

When there are no connectivity issues to CSSM and if on PI, still the mentioned error is seen, then it can be because the recent server upgrade caused the certificate to be removed. The certificate is required for TLS authentication of the two communicating sides. In that case, configure CLI ip http client secure-trustpoint SLA-TrustPoint on the PI and try again.

Debug PI

In order to troubleshoot any issues, the commands collected from PI are:

```
show license all
show license tech support
show license eventlog
show license history message
show license tech events
show license rum id all


For debugging Trust Installation/Sync -

Switch#show license tech support | s Trust
Trust Establishment:
Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
Last Response: <none>
Failure Reason: <none>
Last Success Time: <none>
Last Failure Time: <none>
Trust Acknowledgement:
Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
Last Response: <none>
Failure Reason: <none>
Last Success Time: <none>
Last Failure Time: <none>
Trust Sync:
Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
Last Response: <none>
Failure Reason: <none>
Last Success Time: <none>
Last Failure Time: <none>
Trusted Store Interface: True
Local Device: No Trust Data
Overall Trust: No ID

For debugging Usage reporting timers/intervals -
```

```
Switch#show license tech support | in Utility
Utility:
Start Utility Measurements: Nov 11 16:46:09 2020 EDT (7 minutes, 34 seconds remaining)
Send Utility RUM reports: Dec 07 21:42:30 2020 EDT (26 days, 5 hours, 3 minutes, 55 seconds remaining)
Process Utility RUM reports: Nov 12 15:32:51 2020 EDT (22 hours, 54 minutes, 16 seconds remaining)
```

```
For Collecting all btrace logs for debugging -

Step 1. Switch#request platform software trace rotate all
Step 2. Switch#show logging process iosrp internal start last boot to-file bootflash:<file-name>
```

```
If there are any failues on PULL mode, ensure server SL_HTTP is Acive
```

```
HTTP server application session modules:
  Session module Name  Handle Status   Secure-status     Description
SL_HTTP                2      Active   Active          HTTP REST IOS-XE Smart License Server
HOME_PAGE              4      Active   Active          IOS Homepage Server
OPENRESTY_PKI          3      Active   Active          IOS OpenResty PKI Server
GSI7FBDE91B27B0-web    8      Active   Active          wsma infra
HTTP_IFS               1      Active   Active          HTTP based IOS File Server
BANNER_PAGE            5      Active   Active          HTTP Banner Page Server
WEB_EXEC               6      Active   Active          HTTP based IOS EXEC Server
GSI7FBDED27A1A8-lic    7      Active   Active          license agent app
GSI7FBDF0BD4CA0-web    9      Active   Active          wsma infra
NG_WEBUI               10     Active   Active          Web GUI
```

Debug CSLU

If any issue on CSLU is debugged, it is important that the log file from this directory on CSLU installed PC is taken.

```
C:\Users\<user-name>\AppData\Roaming\CSLU\var\logs
```

Related References

- Migration to SL using Policy - Migration of legacy SL/SLR/PLR licenses to SL using Policy
- Release Notes: RN-9200, RN-9300, RN-9400, RN-9500, RN-9600
- Configuration Guides: Cat9200-CG, Cat9300-CG, Cat9400-CG, Cat9500-CG, Cat9600-CG
- Command References: Cat9200-CR, Cat9300-CR, Cat9400-CR, Cat9500-CR, Cat9600-CR
- Technical Support & Documentation - Cisco Systems