

了解Catalyst交换的智能许可

目录

[简介](#)

[目的](#)

[使用策略的智能许可](#)

[术语](#)

[为什么会有这种变化？](#)

[可用许可证](#)

[基本许可证](#)

[附加许可证](#)

[新组件](#)

[策略](#)

[RUM报告](#)

[绿地部署案例的制造流程](#)

[CSLU](#)

[SLP -直接连接](#)

[许可证报告](#)

[Direct Connect -智能传输](#)

[直接连接- Call-Home传输](#)

[SLP - CSLU](#)

[CSLU安装和配置](#)

[使用推送模式的CSLU](#)

[CSLU自动发现](#)

[使用拉模式的CSLU](#)

[使用RESTAPI的拉模式](#)

[CSLU -设置步骤](#)

[使用RESTCONF的PULL模式](#)

[CSLU -设置步骤](#)

[使用NETCONF的PULL模式](#)

[CSLU -设置步骤](#)

[使用断开模式的CSLU](#)

[SLP -离线模式](#)

[行为更改](#)

[故障排除](#)

[一般故障排除调查表](#)

[调试PI](#)

[Debug CSLU](#)

[相关参考](#)

简介

本文档介绍使用Catalyst交换平台上的策略和支持的部署的智能许可功能。

目的

在Cisco IOS® XE版本17.3.2和17.4.1中，用于Cat9k的系列中的所有Catalyst交换平台都支持SLP的新许可模式（使用策略的智能许可）。本文档旨在了解SLP实施和部署的不同受支持模式，主要适用于绿地部署。

使用策略的智能许可

使用SLP时，设备开箱即用，所有许可证都处于“使用中”状态。早期的概念、评估模式、注册和预留随着SLP而消失。使用SLP时，一切都涉及到报告许可证及其使用情况。许可证仍未执行，并且许可级别保持不变。对于Catalyst交换机平台，除了HSECK9许可证以外，没有出口管制许可证级别。唯一的更改是在报告许可证使用和跟踪的基础之上。本节详细介绍术语、更改原因、SLP附带的新组件、CSLU（思科智能许可实用程序）以及产品订购流程。

术语

- CSSM或SSM -思科智能软件管理器
- SA -智能帐户
- VA -虚拟帐户
- SL -智能许可
- PLR -永久许可证预留
- SLR -智能许可证预留
- PID -产品ID
- SCH - Smart Call Home
- PI -产品实例
- CSLU -思科智能许可实用程序
- RUM —资源利用率衡量
- ACK —确认
- UDI -唯一设备标识- PID + SN
- SLP -使用策略的智能许可

为什么会有这种变化？

通过引入trust and verify的智能许可模式，思科支持各种部署机制，以跟踪许可证使用情况并向CSSM报告。但是，它不容易适应所有类型的部署-现场有反馈和要求，使智能许可更有利于采用。其中一些挑战是：

- 通过SL注册-设备必须始终连接到互联网才能到达CSSM，这是部署问题。
- 内部部署卫星服务器会增加部署和维护成本。
- SLR仅用于气隙网络。
- 任何不支持这两种模式的部署都必须以Unregistered/Eval expired 状态运行其设备，即使购买了许可证也是如此。

引入SLP是为了方便来自现场的各种此类请求。使用SLP时，您无需向CSSM注册产品。所有购买的许可证级别均开箱即用。这将消除设备上的第0天摩擦。SLP还可以最大限度地减少许可证调配的工作流程，并减少多余的接触点。设备无需全天候连接到CSSM。SLP还能够在断开连接的网络中使用许可证，离线报告许可证使用情况，并按客户策略确定的间隔报告许可证。

可用许可证

可用的软件功能属于基本或附加许可证级别。基本许可证是永久许可证，附加许可证分为三年、五年和七年三个期限。

基本许可证

- 网络基础
- 网络优势
- HSECK9

附加许可证

- DNA要素
- DNA优势



注意：HSECK9是出口管制许可证。它需要SLAC才能启用许可证和相应的功能。

新组件

策略

该策略决定PI的默认行为是什么。它告知不同许可证级别和条件的许可报告要求属性。该策略还确定对于发送到CSSM的每份报告，是否必须将ACK消息发送回PI。策略还包含策略名称以及策略安装时间。思科的默认策略是所有Catalyst产品的通用和标准。但是，如果希望具有不同的报告间隔和ACK响应遗漏，则也允许使用客户定义的策略。


该策略可在各种情况下安装在PI上。

- 软件中存在的默认策略
- 思科制造部门安装的策略
- 通过ACK响应安装的策略
- 通过CLI手动安装策略
- 使用Yang请求推送策略

此输出显示默认策略的外观。

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)

 **注意：**当您清除/修改系统配置、清除nvram或格式化闪存时，无法清除策略：filesystem。在许可证智能工厂重置时，策略被设置为思科默认值。


RUM报告

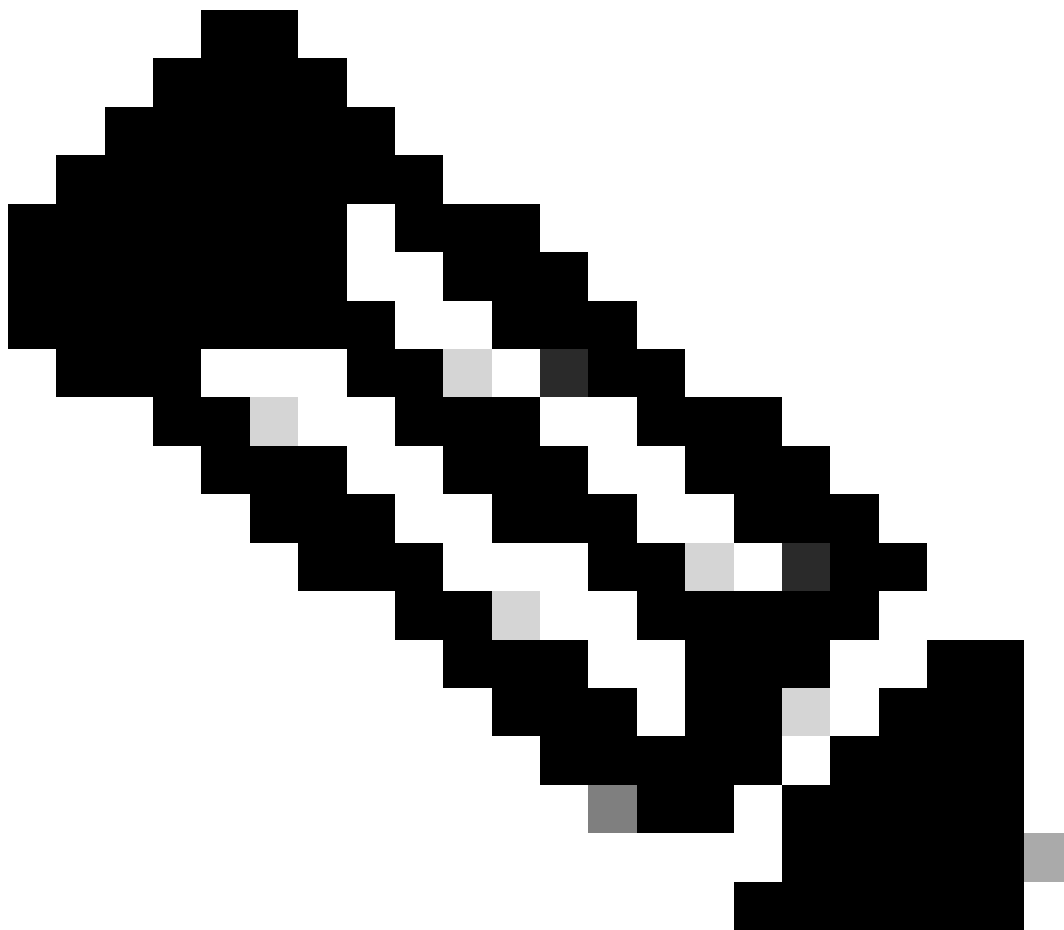
RUM是由PI生成并存储的使用情况报告。针对SLP完成ISO19770-4标准RUM报告。RUM报告将PI中对许可证使用情况所做的所有更改存储为报告文件。每个许可证级别的使用数据存储在单独的RUM报告中。RUM报告测量定期在PI中收集和存储。每当PI的许可证使用情况发生变化或触发使用情况报告时，或当报告达到最大大小/样本时，都会生成所有许可证级别的新RUM报告。在其他情况下，可以使用新的示例和更新的时间戳覆盖现有的RUM报告。默认RUM报告实用程序测量是每15分钟一次。在每个报告间隔，RUM报告发送到Cisco CSSM。

所有RUM报告均由PI签名并由CSSM验证。当CSSM从PI接收RUM报告数据时，它会验证该报告，检查许可证使用更改的时间表，并相应地更新CSSM数据。然后，CSSM通过ACK响应消息向PI确认消息。

RUM报告可通过多种方式发送到CSSM：

- PI在报告时间间隔内将RUM报告直接发送到CSSM。
- PI将RUM报告推送给CSLU。
- CSLU通过RESTAPI和YANG模型定期从PI提取RUM报告。
- RUM报告通过CLI在PI上手动保存，并手动上传到CSSM。

 注：当您清除/修改系统配置、清除nvram或格式化闪存时，无法清除RUM报告：filesystem。在“license smart factory reset”上，所有RUM报告都可以从PI中删除。



注：默认报告间隔为30天。

绿地部署案例的制造流程

在Cisco CCW(Cisco Commerce Workspace)下新产品订单后，PI将经历制造团队完成的操作流程。这是为了便于签署RUM报告的安全流程，并消除PI注册过程中的第0天摩擦。下单后，任何现有的SA/VA或创建的新SA/VA都将与产品关联。思科制造团队在将产品发送给您之前会处理这些操作：

- 在设备上安装信任代码。信任代码签名基于设备UDI安装。它安装在每个产品上。
- 安装购买代码—有关随产品购买的许可证级别的信息。它安装在每个产品上。
- SLAC -智能许可证身份验证代码-不适用于Catalyst平台。
- Install Policy -根据您的输入选择Default或Custom Policy。
- 向CSSM - SA/VA报告许可证使用情况。



注意：对于17.3.3版本，除C9200/C9200L以外的所有Catalyst交换平台均遵循此流程。

注意：信任代码仅在带17.7.1的制造环境中为除C9200/C9200L外的所有Catalyst交换平台安装。

CSLU

SLP引入了一种简单而强大的新工具CSLU。CSLU是基于GUI的工具，运行在Windows 10操作系统或基于RHEL/Debian的Linux版本上。CSLU（可在本地专用网络上运行）负责从与CSSM关联的PI收集RUM端口。CSLU的调配方式必须能够收集有关本地网络中PI的RUM报告，并且定期通过互联网将RUM报告推送到CSSM。CSLU是一个简单的工具，它仅显示已调配设备的UDI的详细信息。池中PI、已购买许可证和未使用许可证的所有许可证使用数据仅在CSSM的SA/VA中可见，供您验证。它功能强大，因为它可以收集多达10K PI的使用报告。CSLU还负责将来自CSSM的ACK消息推送回PI。



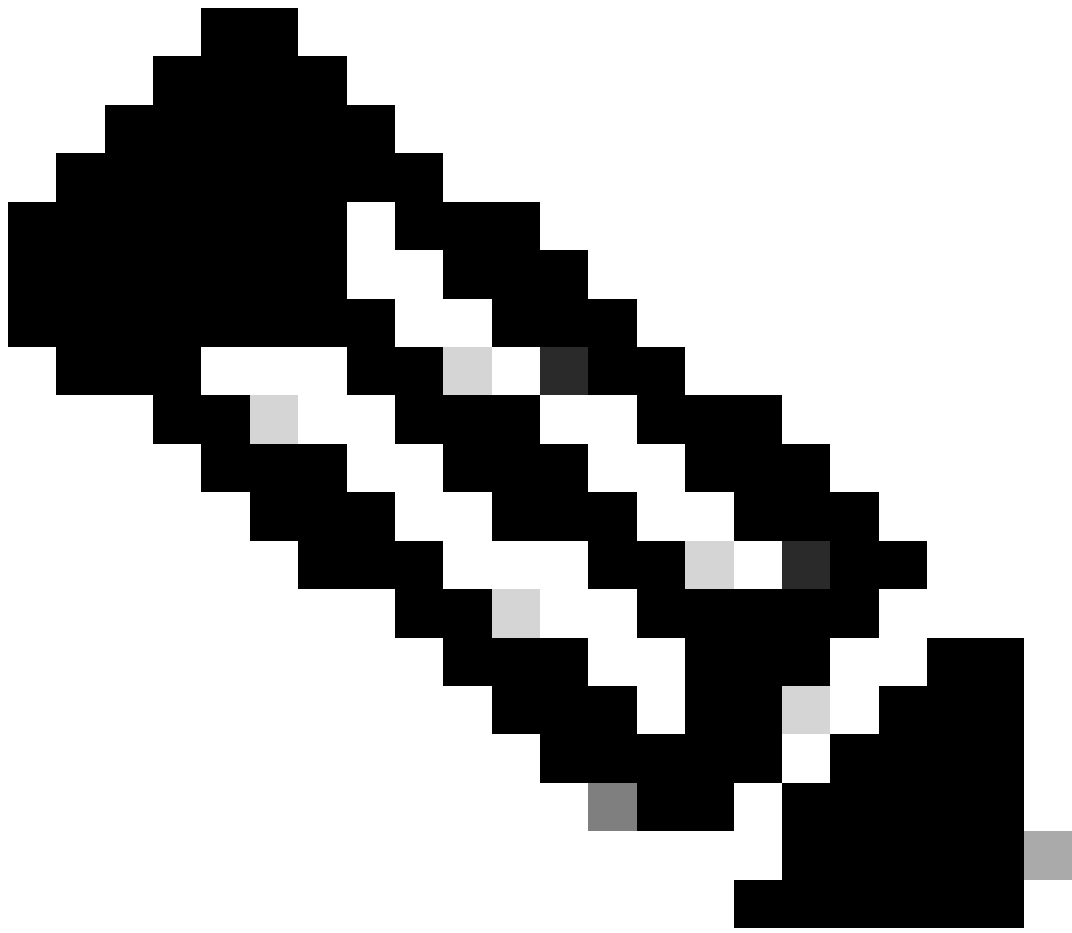
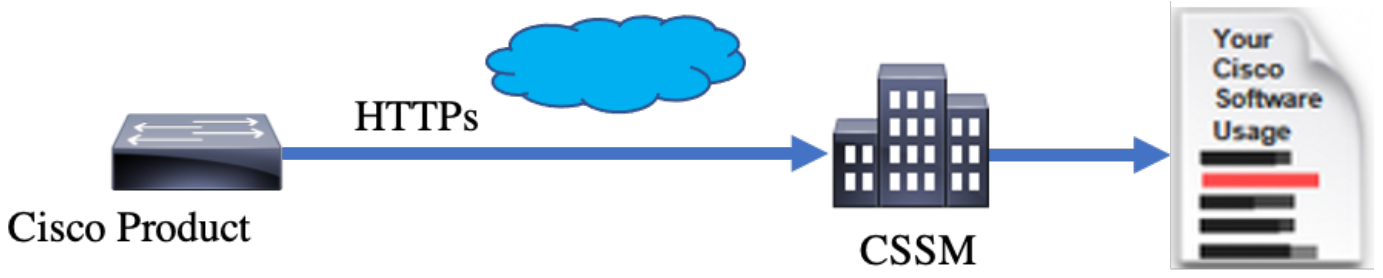
注意：请参阅基于CSLU的拓扑部分，了解CSLU的详细配置和支持的运行模式。



注意：版本17.7.1支持Linux版本的CSLU。

SLP -直接连接

在出厂产品上，默认传输模式配置为CSLU。如果要使用直接连接方法，必须根据需要将传输模式更改为Call-home或SMART。拓扑的直接连接方法的基本要求是具备与CSSM的连通性的Internet连接。此外，必须确保设备中存在所需的L3配置、DNS和域配置，才能连接到CSSM。



注意：当您直接连接到CSSM时，建议使用智能传输方法。

在直接连接拓扑中，RUM报告直接发送到CSSM。许可证报告要求在设备上安装成功的信任代码。信任代码由思科制造商在发货前安装在设备上。您也可以在设备上安装信任代码。

“信任代码”是从“虚拟帐户-常规”页上的CSSM获取的令牌字符串。信任代码可以通过CLI安装。

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



注意：所有选项都必须用于HA或堆叠系统。对于独立设备，可以使用本地选项。

```
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

成功安装信任代码后，PI可以直接向CSSM报告使用情况。这些情况将导致许可证报告：

- 信任代码安装成功
- 在每个默认报告间隔上
- 设备上重新加载/启动
- 切换
- 堆叠部件的添加或移除
- 手动触发许可证同步

可以使用以下CLI触发向CSSM报告的许可证：

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

show license status中的“使用报告”部分将告知您上次收到的ACK、下次ACK截止时间、下次报告推送和最后一次报告推送的时间表。

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 - 智能传输

在直接连接或直接云访问模式拓扑中，如果使用SMART Transport，这些是设备上的必要配置。

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  
!
```

直接连接- Call-Home传输

在直接连接或直接云访问模式拓扑中，如果使用回拨传输，这些是设备上的必要配置。

Configure the desired Transport mode using below CLI.

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

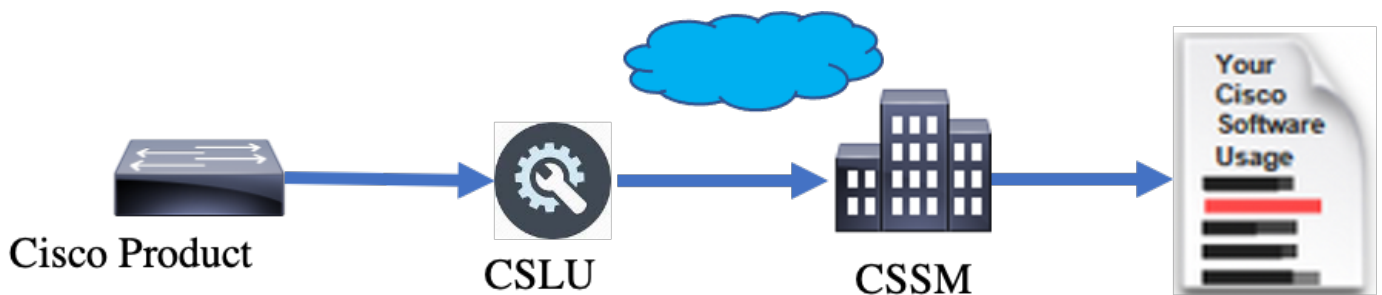
Running config on Smart Transport Mode:

```
!  
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  
!
```

 注意：默认情况下，Call-home的目标地址配置为CSSM URL。这可以在show run all配置中进行验证。

SLP - CSLU

CSLU模式是运行17.3.2或更高版本的出厂设备的默认传输模式。此外，如果从评估/评估到期许可证迁移，则迁移到SLP后的传输模式为CSLU。在基于CSLU的拓扑中，CSLU位于PI和CSSM之间。CSLU可避免用户无法直接连接到思科云-CSSM。CSLU可以在私有网络上本地运行，并从所有关联的PI下载使用情况报告。使用报告在通过互联网发送到CSSM之前，本地保存在Windows PC上。CSLU是一种轻型工具。您只能看到与其关联的PI列表，并且可以通过使用UDI对其进行识别。CSLU无法显示或包含PI的冗余信息、许可证级别或许可证使用情况。

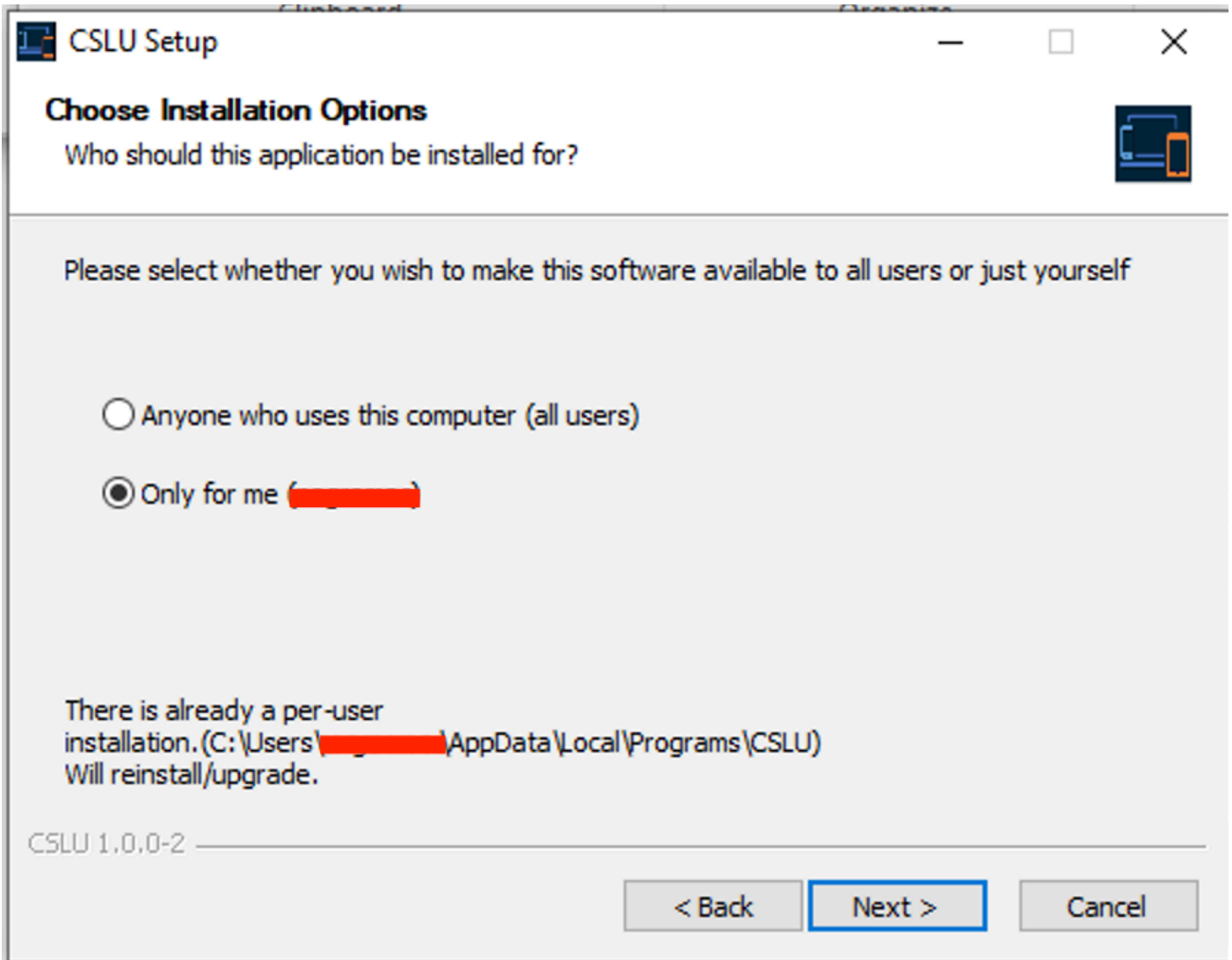


CSLU安装和配置

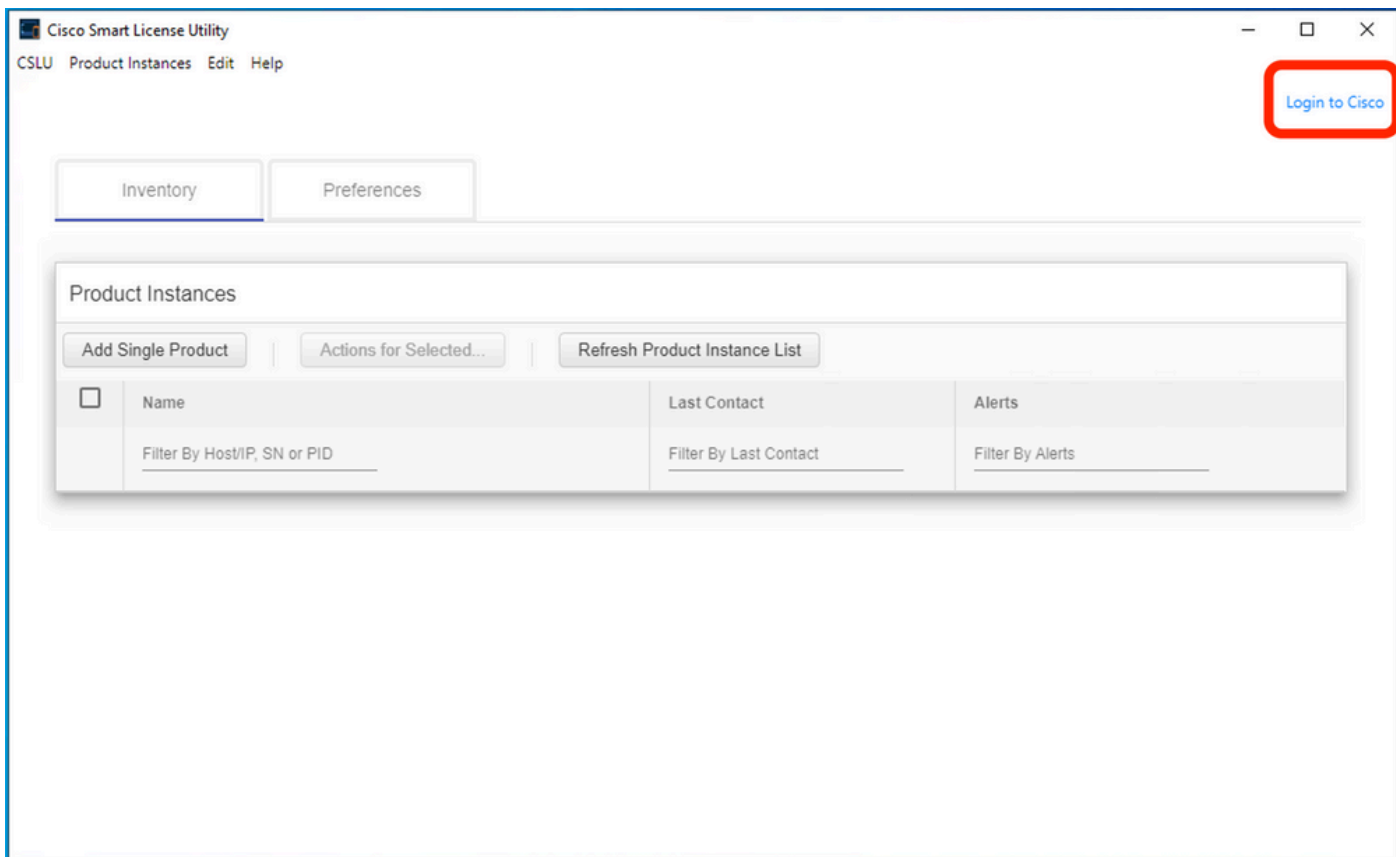
CSLU工具在Windows 10计算机上安装和运行。CCO中可免费下载和使用该软件。安装工具后，可以从“Help”菜单下载“Quick Start Guide/User Manual”，然后导航到Help > Download Help Manual。

CSLU安装要求您接受许可协议。

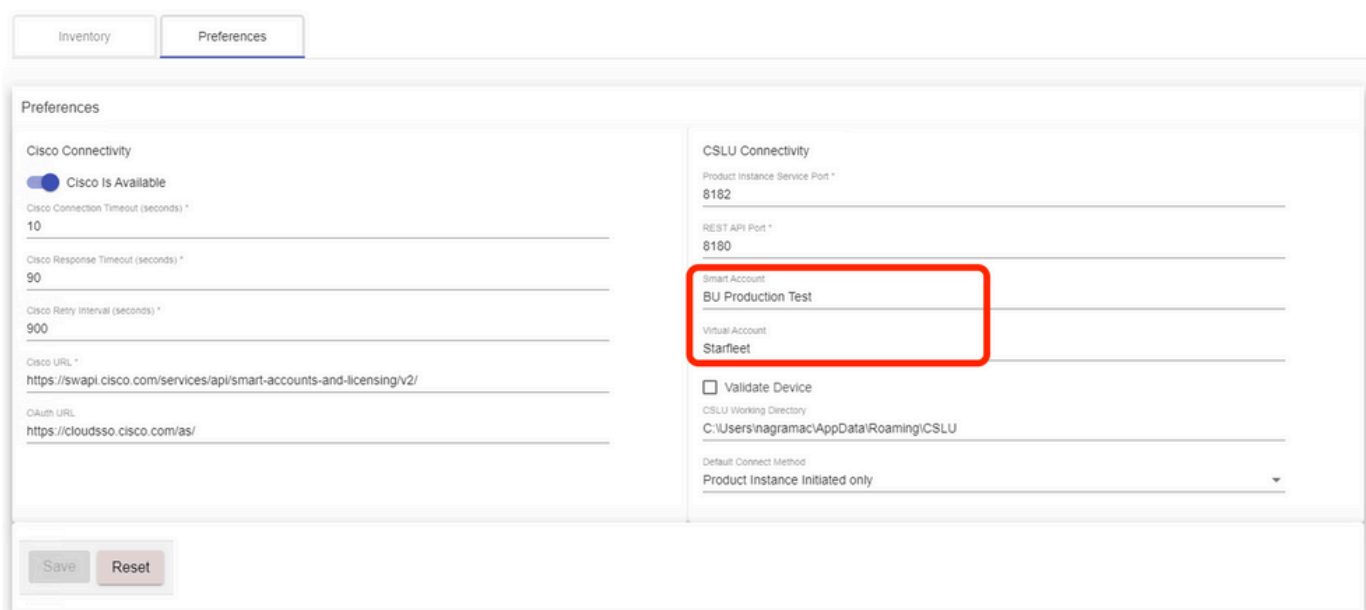
建议仅为当前用户安装该应用程序，而不为在计算机上工作的所有用户安装该应用程序。如果PC上已经存在CSLU的早期版本，则最好提前将其卸载。但是，新安装会注意升级软件。



安装完成后，使用应用程序右上角显示的登录选项登录思科。这将使用您的CEC凭证。通过登录，在CSLU和CSSM之间建立信任。



登录思科后，请确保通过工具的“首选项”窗格中的下拉菜单正确选择SA和VA详细信息。确保保存配置。



CSLU上的Scheduler选项卡-通过CSLU上的Scheduler选项卡，可以配置以下内容：

- Poll CSSM for available data -显示CSSM中数据的作业计时、上次提取时间和下次提取时间。
- 清除已清除的数据-从CSLU数据存储中删除所有已清除的数据。也可以手动触发。
- 拉动设备数据-触发CSLU拉动模式。

Scheduler			
Refresh Job Information			
System Jobs			
Name	Status	Next Execution Time	Start
Poll CSSM for Available Data	scheduled	09-Feb-2023 18:35	
Clean Up Purged Data	scheduled	24-Feb-2023 01:40	Start
Operational Jobs			
Name	Status	Next Execution Time	Start
Pull Device Data	scheduled	24-Feb-2023 01:14	Start

使用推送模式的CSLU

默认情况下，CSLU在PUSH模式下运行。在PUSH模式下，PI定期向CSLU发送使用情况报告。从设备上，您必须确保可与CSLU进行L3网络访问。要使PI与CSLU通信，必须配置运行CSLU的Windows计算机的IP地址。

```
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 CS LU>:8182/cslu/v1/pi](http://<IP_of_CS LU>: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>

从PI向CSLU发送有关以下情况的报告：

- 在每个默认报告间隔上
- 设备上重新加载/启动
- 状态切换
- 堆叠成员添加或移除
- 手动触发许可证同步时

在CSLU中，资产页面列出当前与CSLU关联的设备。列表中的设备可以通过UDI进行识别。可以根据列表中的PID或SN过滤设备，以识别任何特定设备。

CSLU资产页面还有另外两列：

- 上一个联系人列-显示报告状态更改的最新时间戳。
- 风险通告列-显示PI的最新报告状态。

PI向CSLU发送报告后，CSLU将在CSSM中创建PI条目。最后联系人TS和风险通告状态会更新。

Name	Last Contact	Alerts
UDI_PID:C9500-32QC; UDI_SN:CAT2148L15K	08-Nov-2020 06:37	COMPLETE: Usage report from product instance
UDI_PID:C9500-24Y4C; UDI_SN:CAT2344L4GH	03-Nov-2020 18:27	COMPLETE: Usage report acknowledgement to product instance

Name	Last Contact	Alerts
UDI_PID:C9500-32QC; UDI_SN:CAT2148L15K	08-Nov-2020 06:37	COMPLETE: Usage report uploaded to CSSM
UDI_PID:C9500-24Y4C; UDI_SN:CAT2344L4GH	03-Nov-2020 18:27	COMPLETE: Usage report acknowledgement to product instance

CSSM处理CSLU发送的报告，并根据许可证使用情况在CSSM上添加/更新产品实例。CSSM处理并更新日期后，会将ACK消息发送回CSLU。CSLU反过来存储消息并将其转发回PI。

ACK消息包括：

- 确认所有已发送的报告
- 策略
- 信任代码

如果新策略在CSSM中可用，则其现在也会更新到PI。如果策略未更改，则会向PI推送相同的策略。

 **注意：**如果根据策略不需要ACK消息报告，则不会发送ACK消息。

警报消息列可以具有以下状态之一：

- 来自产品实例的使用情况报告

- 使用情况报告已上传到思科
- 从产品实例同步请求
- 同步请求已上载到CSSM
- 从CSSM收到的确认
- 产品实例的使用情况报告确认



注意：在HA系统上的CSLU中，始终只为主用UDI看到条目。只有CSSM才列出系统中各个设备的所有UDI。

CSLU自动发现

为了支持使用最少配置进行扩展部署，支持自动发现CSLU。这意味着您不必专门配置CSLU的IP地址/URL。为此，只需向其DNS服务器添加一个条目。这使传输模式为CSLU（默认值）的设备能够自动发现CSLU并发送报告。

此处需要确保以下几点：

- 在DNS服务器中创建条目。CSLU的IP地址必须映射到名称cslu-local。
- 确保设备中存在名称服务器和DNS配置以实现可访问性。

这样，无需任何额外配置，网络中的设备即可访问CSLU并定期发送RUM报告。

使用拉模式的CSLU

PULL模式是CSLU启动从设备获取RUM报告的过程。此处，设备详细信息会添加到CSLU，CSLU会定期读取所有已添加设备上的数据。也可以手动触发CSLU的PULL。CSLU进而向CSSM发送RUM报告，从CSSM返回的ACK消息发送到PI。PULL模式支持三种不同方式- RESTAPI、NETCONF和RESTCONF。

使用RESTAPI的拉模式


要使PULL模式能通过RESTAPI，设备和CSLU所需的配置如下：

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  
!
```

 **注意：**用户必须具有Priv 15级访问权限。

CSLU -设置步骤

CSLU必须登录到CSSM才能自动同步报告。

步骤1:在“清单”页面上选择Add Single Product。

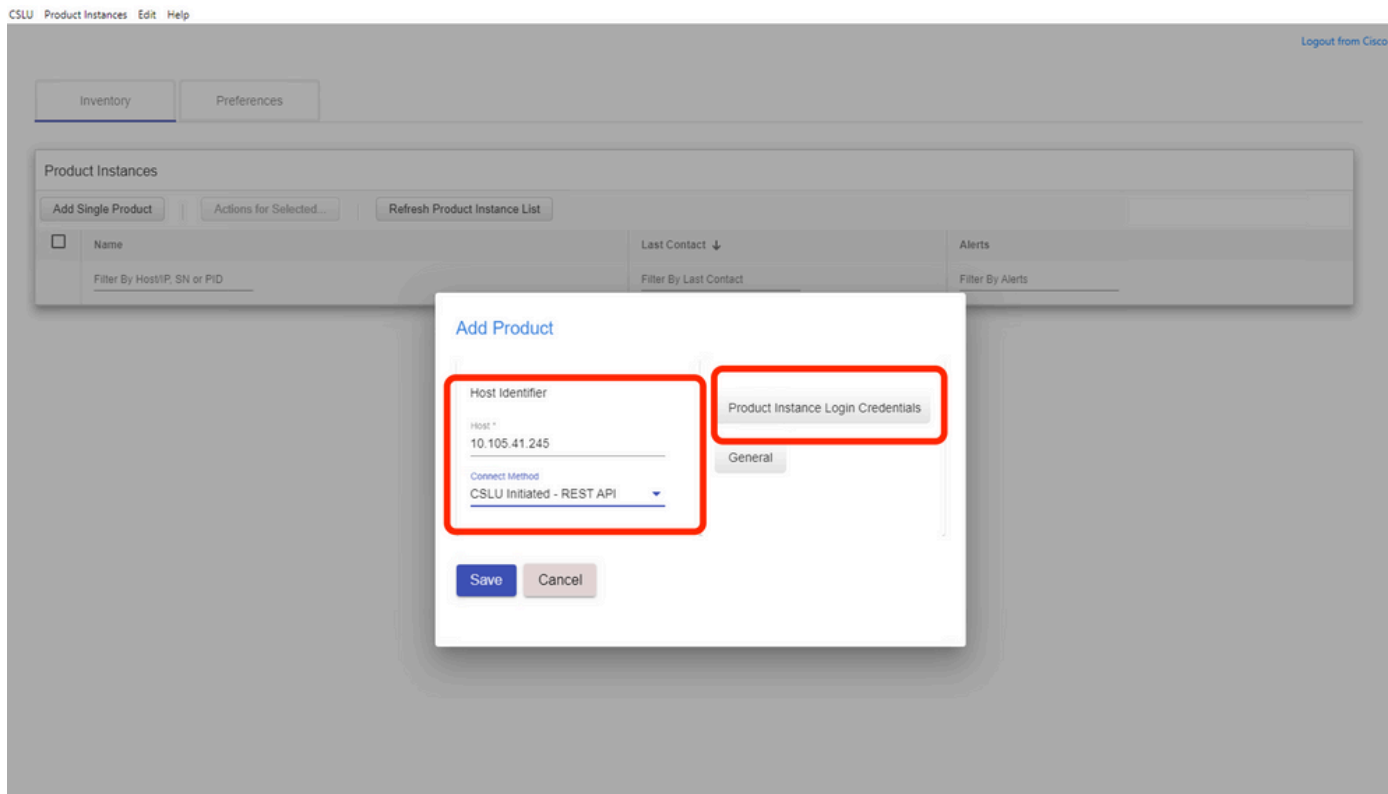
第二步：输入设备IP。

第三步：选择RestAPI作为连接方法。

第四步：选择product instance Login Credentials。

第五步：输入具有Priv 15访问权限的用户的用户凭证。

第六步：保存配置。



CSLU Product Instances Edit Help

Logout from Cisco

Inventory Preferences

Product Instances

Add Single Product Actions for Selected... Refresh Product Instance List

Name	Last Contact ↓	Alerts
Filter By Host/IP, SN or PID	Filter By Last Contact	Filter By Alerts

Add Product

Host Identifier

HOST *

10.105.41.245

Connect Method

CSLU Initiated - REST API

Product Instance Login Credentials

General

Save Cancel

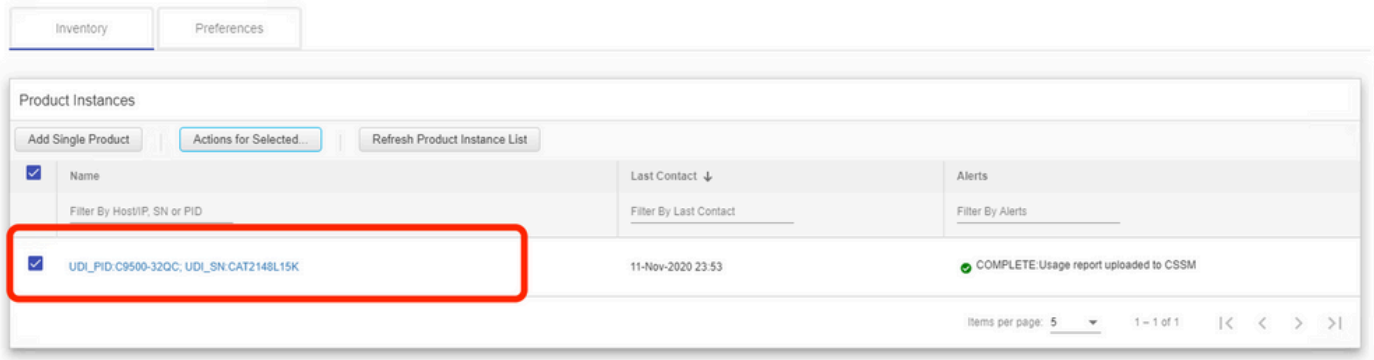
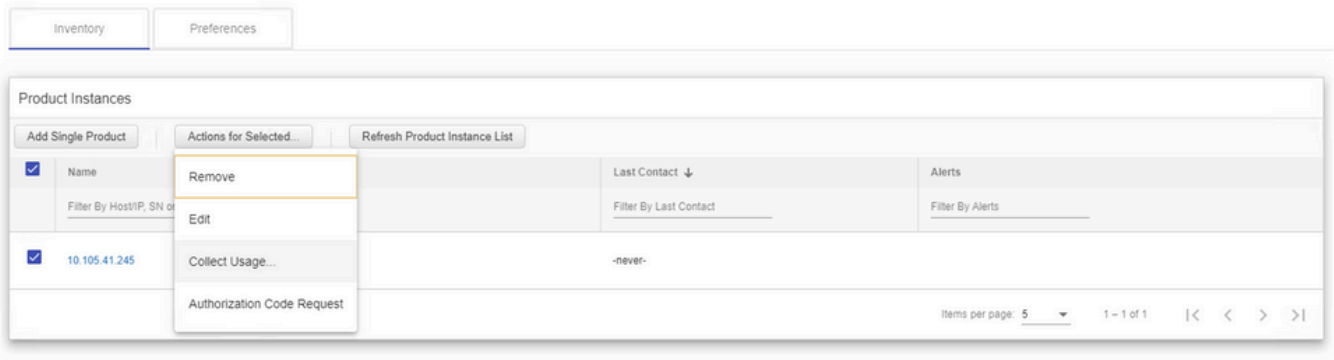
设备会通过Name字段中的唯一IP地址添加。

选择设备并导航至Actions for Selected > Collect Usage。

成功收集使用数据后，“名称”字段将更新到PI的UDI，同时更新时间戳。警报字段反映最新状态。

CSLU Product Instances Edit Help

Logout from Cisco




如果从CSSM收到ACK消息后设备仍然可用，ACK将发送回PI。否则，将在下一个拉取间隔发送ACK。

使用RESTCONF的PULL模式

要使PULL模式通过RESTCONF工作，设备所需的配置以及CSLU的步骤如下：

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  
!
```


 **注意：**这些配置用于本地身份验证。也可以使用远程身份验证。

CSLU -设置步骤

CSLU必须登录到CSSM才能自动同步报告。CSLU设置与RUM报告收集和报告的RESTAPI相同。

步骤1:在“清单”页面上选择Add Single Product。

第二步：输入设备IP。

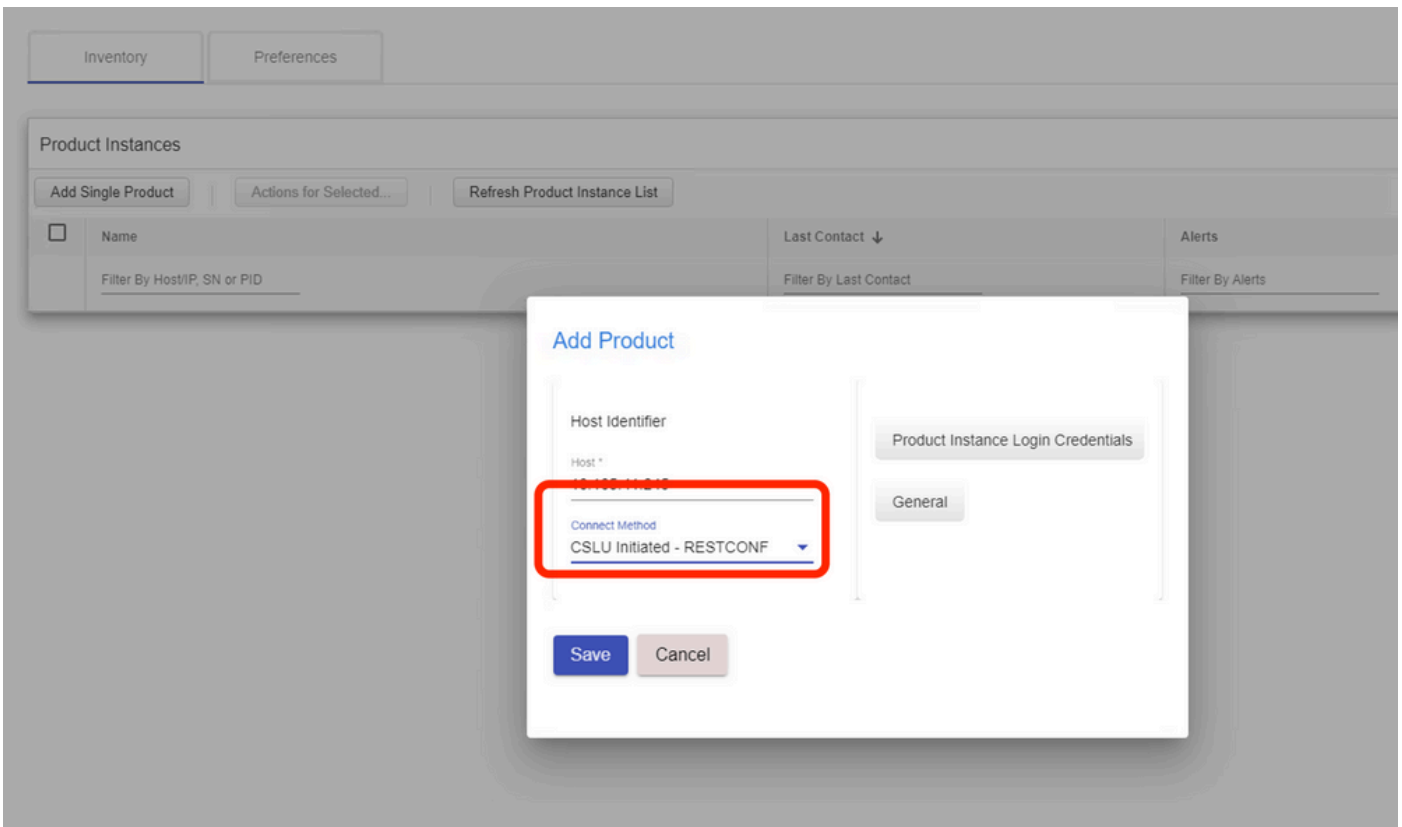
第三步：选择RESTCONF作为连接方法。

第四步：选择product instance Login Credentials。

第五步：输入具有Priv 15访问权限的用户的用户凭证。

第六步：保存配置。

步骤 7.收集所选设备的使用数据。



使用NETCONF的PULL模式

要使PULL模式能通过NETCONF，从设备要求的配置以及CSLU的步骤如下：

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
```



注意：这些配置用于本地身份验证。也可以使用远程身份验证。

CSLU -设置步骤

CSLU必须登录到CSSM才能自动同步报告。CSLU设置与RUM报告收集和报告的RESTAPI相同。

步骤1:在“清单”页面上选择Add Single Product。

第二步：输入设备IP。

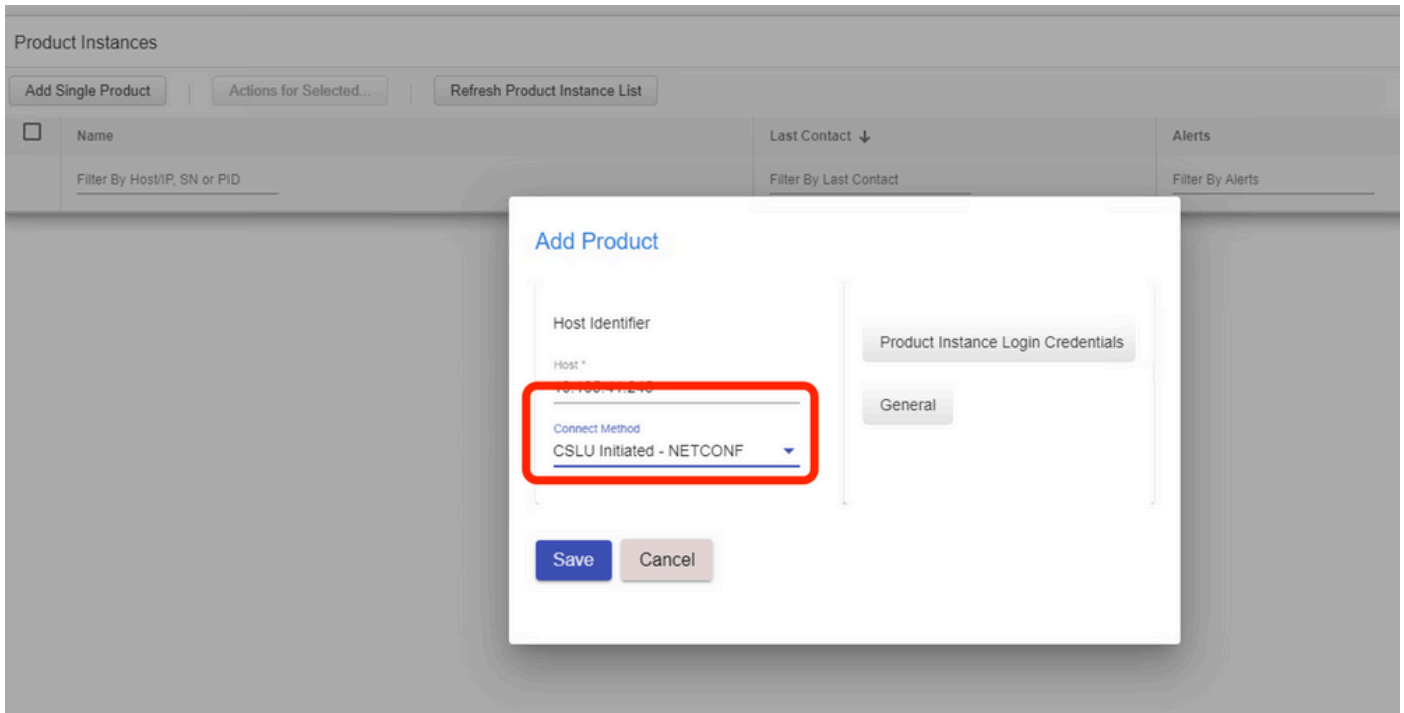
第三步：选择NETCONF作为连接方法。

第四步：选择product instance Login Credentials。

第五步：输入具有Priv 15访问权限的用户的用户凭证。

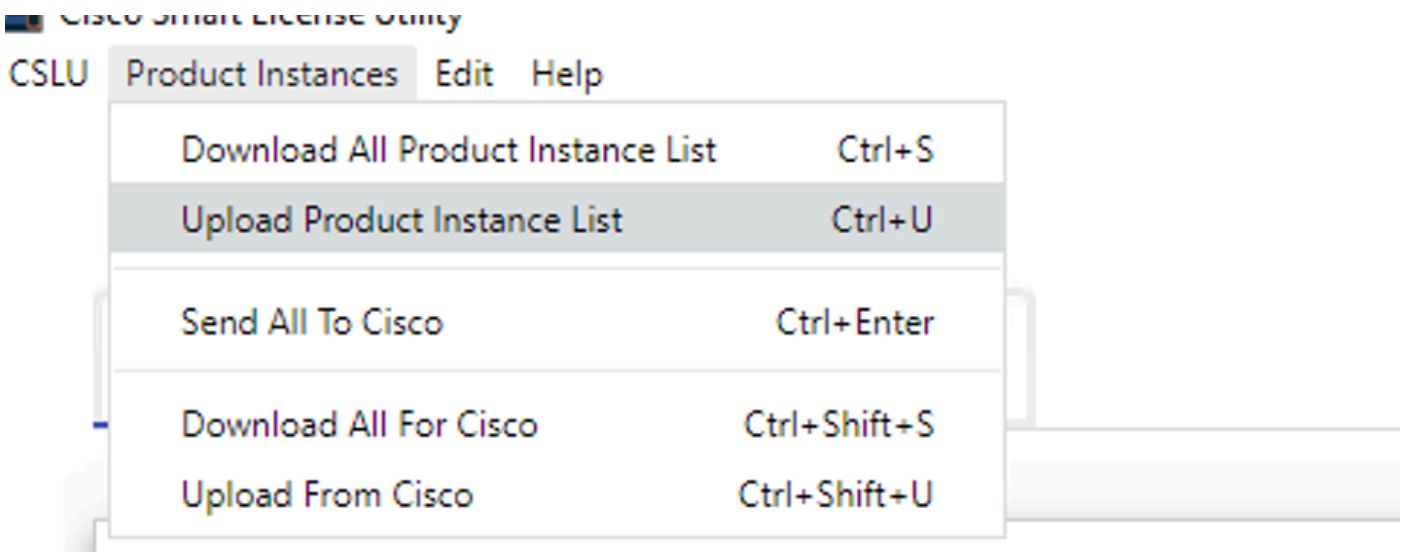
第六步：保存配置。

步骤 7.收集所选设备的使用数据。



 **注意：**对于所有型号、NETCONF、RESTCONF和RESTAPI，都可以批量添加设备列表。

要执行批量上传，请在Menu栏上导航到Product Instance > Upload Product Instance List，如此图中所示。



系统随即会打开一个新的弹出窗口。模板文件可以从其下载。在CSV格式文件中，填写设备列表的设备详细信息，然后上传到CSLU以添加多个设备。

Upload Product Instances



Drag & Drop a File

or [Browse](#) from your computer.

We have a predefined .CSV template to help you! [Download](#)



注意：对于所有类型的CSLU PULL模式，建议将PI上的传输集设置为Off。这可以通过CLI来实现。

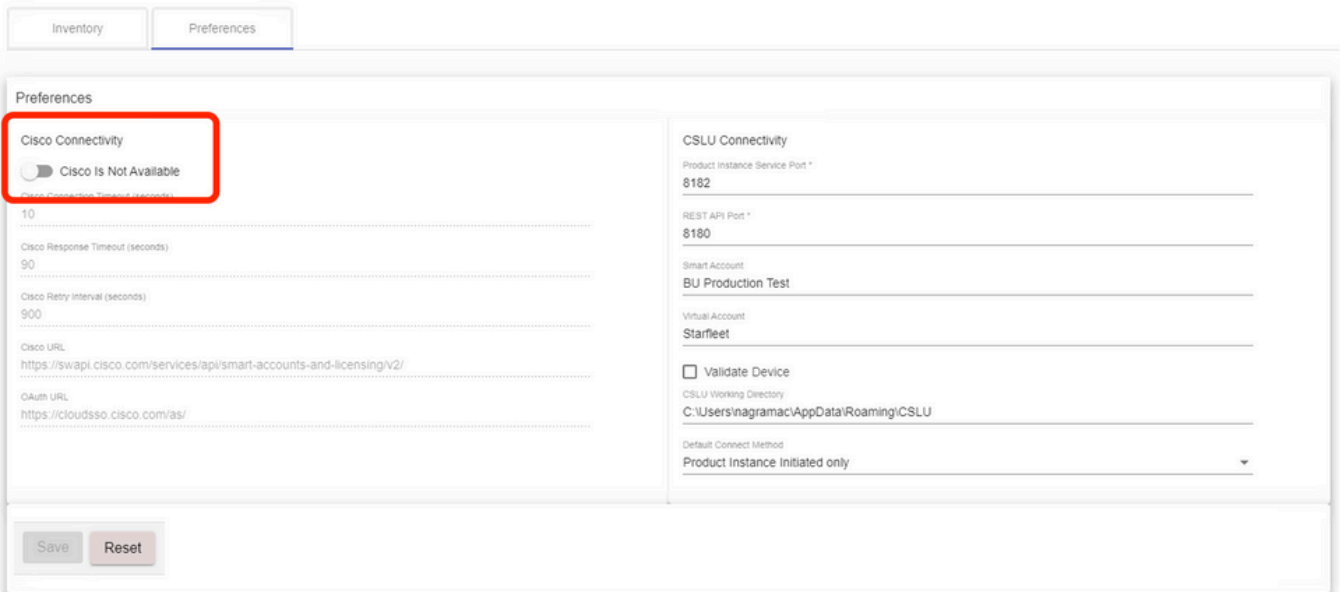
```
Switch(config)#license smart transport off
```

使用断开模式的CSLU

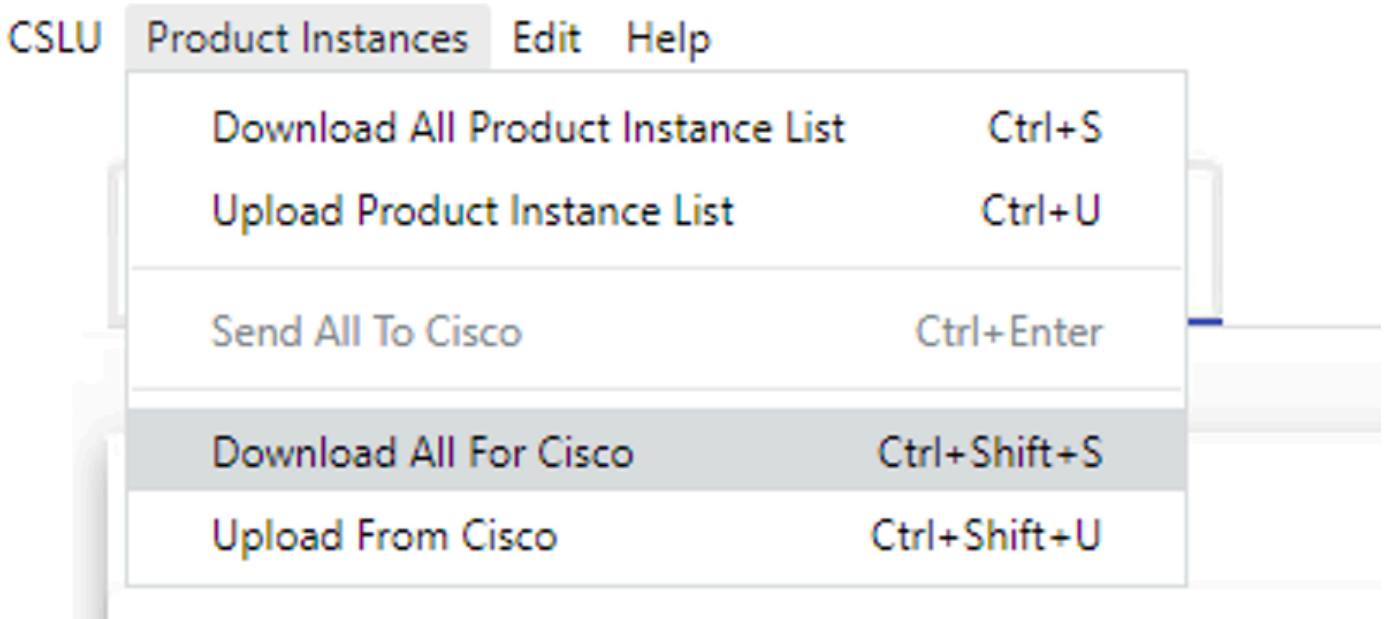
CSLU可在与CSSM断开连接的模式下运行。这适用于不允许CSLU连接到互联网的任何部署。在断开连接模式下，从CSLU手动下载所有设备的报告，并将其上传到CSSM。然后，ACK消息从CSSM下载并上传到CSLU。CSLU仍继续从PI提取/推送使用日期，并将ACK消息发回PI。

步骤1:在CSLU Preference页上，关闭选项Cisco Connectivity。这确认思科不可用。

第二步：保存设置。



第三步：在Menu栏中，单击Product Instances > Download All for Cisco。这会将文件下载tar.gz到CSLU。



第四步：将文件上传到CSSM。在CSSM智能帐户页面，导航至Report > Usage Data Files > Upload usage data。在弹出窗口中，上传tar.gz文件。

Smart Software Licensing

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

Reports

Report	Usage Data Files	Reporting Policy			
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.					
<input type="button" value="Upload Usage Data..."/>		<input type="text" value="Search by File Name, Virtual Account"/>			
Usage Data File	Reported	Virtual Account	Reporting Status	Devices	Acknowledgement
Usage_SLR_1.txt	2020-Oct-29	Quake	i No Errors	2	Download
Usage_SLR.txt	2020-Oct-29	Quake	i No Errors	1	Download
+ UD_SA_BU_Production_Test_20Oct28_11_11_03	2020-Oct-28	DLC-VA1	i No Errors	1	Download
+ UD_SA_20Oct28_10_49_13_092.tar.gz	2020-Oct-28	DLC-VA1	i No Errors	1	Download
+ UD_SA_BU_Production_Test_20Oct28_10_46_25	2020-Oct-28	DLC-VA1	i No Errors	1	Download
Usage_17_3_2.txt	2020-Oct-28	Quake	i No Errors	1	Download
Usage_17_3_2.txt	2020-Oct-28	Quake	x Errors (1)	1	Download
Usage_17_3_2.txt	2020-Oct-28	Quake	i No Errors	1	Download

25 | Showing Page 1 of 3 (74 Records) | << >>

Upload Usage Data

Please select the Usage File you wish to upload.

* Usage Data File:

UD_SA_BU_Production_Test_20Nov12_01_01_02_466.tar.gz

第五步：处理完数据后，即会生成确认。下载ACK文件并将其上传到CSLU。

Reports

Report | **Usage Data Files** | Reporting Policy

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... Search by File Name, Virtual Account

Usage Data File	Reported	Virtual Account	Reporting Status	Devices	Acknowledgement
UD_SA_BU_Production_Test_20Oct28_11_11_03	2020-Oct-28	DLC-VA1	No Errors	1	Download

第六步：在CSLU中，从菜单栏导入ACK文件，然后导航到Product Instances > Upload from Cisco，如此图所示。

CSLU Product Instances Edit Help

- Download All Product Instance List Ctrl+S
- Upload Product Instance List Ctrl+U
- Send All To Cisco Ctrl+Enter
- Download All For Cisco Ctrl+Shift+S
- Upload From Cisco Ctrl+Shift+U

步骤 7.一旦上传ACK，消息就会发送到PI。也可以通过“警报”列进行验证。

CSLU Product Instances Edit Help

Inventory Preferences

Product Instances

Add Single Product | Actions for Selected... | Refresh Product Instance List

Name	Last Contact ↓	Alerts
UDI_PID_C9500-320C; UDI_SN_CAT2148L15K	12-Nov-2020 01:10	COMPLETE: Usage report acknowledgement to product instance

Items per page: 5 1 - 1 of 1 |< < > >|

SLP - 离线模式

SLP也可以在完全脱机模式下工作。这主要适用于气隙网络，这些网络不喜欢Internet连接，也不选择使用CSLU。在脱机模式下，传输设置为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>

每当需要向CSSM报告使用情况数据时，必须将使用情况报告下载为文件并手动上传到CSSM。在HA系统中，主用收集备用/成员设备的使用量。

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 reported 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
```

现在，必须手动将此报告上传到CSSM。

将保存的使用数据从PI导出到桌面。

在CSSM智能帐户页面，导航至Report > Usage Data Files > Upload usage data。在弹出窗口中，选择使用情况报告并单击upload。

上传文件后，您必须选择与设备关联的正确VA。

Upload Usage Data

Please select the Usage File you wish to upload.

* Usage Data File:

Browse

usage_report_5-nov

Upload Data

Cancel

Select Virtual Accounts



Some of the usage data files do not include the name of the virtual account that the data refers to, or the virtual account is unrecognized.

Please select an account:

Select one account for all files:

Select a virtual account per file:

Ok

Cancel

一旦数据完全处理完毕并且确认准备就绪，请下载文件并将其加载到PI上。

```
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 installed  
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

行为更改

这些更改在版本上针对智能许可功能完成：

- **信任同步** -从17.7.1开始，信任代码安装在交换机上所有受支持的拓扑（如CSLU和脱机方法）上。
- **隐私更改** -如果从17.7.1禁用各自的隐私设置，则从17.9.1发送至CSSM的RUM报告中会包括版本字符串和主机名信息。
- **帐户详情** -从17.7.1开始，CSSM中的ACK消息包括帐户信息和SA/VA详情。
- **RUM报告限制** -从17.9.1开始，PI启动通信的时间的报告间隔被限制。最小报告频率限制为一天。这意味着产品实例每天不会多次发送RUM报告。

故障排除

一般故障排除调查表

场景1：从非常早期的版本（即16.9.x）升级Cisco IOS XE后，某些协议（即HSRP）不再有效。

检查许可证引导级别，查看其是否仍然与升级Cisco IOS XE之前相同。许可证引导级别可能重置为Networking-Essentials，它可能不支持失败的协议（即HSRP）。

方案2：许可证状态显示消息“故障原因：无法发送Call Home HTTP消息”或“上次通信尝试：待定”

这可能与基本连接问题有关。要解决检查，请执行以下操作：

- 连接CSSM的网络连接- IP地址、路由等。
ip http client source interface
- 的配置正确。
- 时间差异。(需要配置NTP以提供正确的时钟时间/时区)
- 如果内部防火墙配置阻止到CSSM的流量

方案3：如果在一年的注册后发现日志错误“%SMART_LIC-3-AUTH_RENEW_FAILED：使用思科智能软件管理器(CSSM)进行授权续订：未定义方法“each”表示nil：NilClass，情况会怎样？

重新注册产品。在CSSM上生成新的令牌ID，并将产品实例重新注册到CSSM。

方案4：当与思科之间没有连接错误时，显示错误消息“%SMART_LIC-3-COMM_FAILED：通信失败”。

当没有到CSSM的连接问题，并且如果在PI上，仍然出现上述错误，则可能是由于最近的服务器升级导致证书被删除。通信双方的TLS身份验证需要该证书。在这种情况下，请在PI上配置CLI ip http client secure-trustpoint SLA-TrustPoint，然后重试。

调试PI

为了排除任何问题，从PI收集的命令包括：

```
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 failures on PULL mode, ensure server SL_HTTP is Active

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
SSI7FBDE91B27B0-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
SSI7FBDED27A1A8-lic	7	Active	Active	license agent app
SSI7FBDF0BD4CA0-web	9	Active	Active	wsma infra
NG_WEBUI	10	Active	Active	Web GUI

Debug CSLU

如果调试了CSLU上的任何问题，则必须从安装了CSLU的PC上的此目录获取日志文件。

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

相关参考

- 使用策略迁移至SL - [使用策略将传统SL/SLR/PLR许可证迁移至SL](#)
- 发行版本注释：[RN-9200](#)、[RN-9300](#)、[RN-9400](#)、[RN-9500](#)、[RN-9600](#)

- 配置指南：[Cat9200-CG](#)、[Cat9300-CG](#)、[Cat9400-CG](#)、[Cat9500-CG](#)、[Cat9600-CG](#)
- 命令参考：[Cat9200-CR](#)、[Cat9300-CR](#)、[Cat9400-CR](#)、[Cat9500-CR](#)、[Cat9600-CR](#)
- [技术支持和文档 - Cisco Systems](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。