

Entender o Smart Licensing para switches Catalyst

Contents

[Introdução](#)

[Propósito](#)

[Licenciamento inteligente usando política](#)

[Terminologia](#)

[Por que essa mudança?](#)

[Licenças disponíveis](#)

[Licenças básicas](#)

[Licenças complementares](#)

[Os novos componentes](#)

[Política](#)

[Relatórios RUM](#)

[Fluxo de fabricação para caso de implantação inicial](#)

[CSLU](#)

[SLP - Conexão direta](#)

[Relatórios de licença](#)

[Conexão direta - Transporte inteligente](#)

[Direct Connect - Transporte Call-Home](#)

[SLP - CSLU](#)

[Instalação e configuração do CSLU](#)

[CSLU usando o modo PUSH](#)

[Descoberta automática de CSLU](#)

[CSLU usando o modo PULL](#)

[Modo PULL usando RESTAPI](#)

[CSLU - Procedimento para configuração](#)

[Modo PULL usando RESTCONF](#)

[CSLU - Procedimento para configuração](#)

[Modo PULL usando NETCONF](#)

[CSLU - Procedimento para configuração](#)

[CSLU usando o modo desconectado](#)

[SLP - Modo Offline](#)

[Alterações de comportamento](#)

[Troubleshooting](#)

[Questionário genérico de solução de problemas](#)

[Depurar PI](#)

[Depurar CSLU](#)

[Referências relacionadas](#)

Introdução

Este documento descreve o recurso Smart Licensing usando a Política nas plataformas de switching Catalyst e a implantação suportada.

Propósito

Nas versões 17.3.2 e 17.4.1, do Cisco IOS® XE, todas as plataformas de switching Catalyst da família para Cat9k suportam um novo modelo de licenciamento de SLP (Smart Licensing using Policy). A finalidade deste documento é entender os diferentes modelos suportados de implementação e implantação do SLP, principalmente para implantações iniciantes.

Licenciamento inteligente usando política

Com o SLP, o dispositivo tem todas as licenças 'em uso' prontas para uso. Os conceitos anteriores, Modo de avaliação, Registro e Reserva desaparecem com o SLP. Com o SLP, tudo gira em torno de informar as licenças e seu uso. As licenças ainda não foram aplicadas e os níveis de licenciamento continuam os mesmos. Para plataformas de Switch Catalyst, não há níveis de licença de exportação controlada, exceto a licença HSECK9. A única alteração está na infra de relatórios de uso e rastreamento de licenças. Esta seção fala em detalhes sobre terminologias, por que as alterações, os novos componentes que acompanham o SLP, o CSLU (Cisco Smart Licensing Utility) e o fluxo de pedidos de produtos.

Terminologia

- CSSM ou SSM - Cisco Smart Software Manager
- SA - Conta inteligente
- VA - Conta virtual
- NS - Smart Licensing
- PLR - Reserva de Licença Permanente
- SLR - Reserva de Smart License
- PIDs - IDs de produto
- SCH - Smart Call Home
- PI - Instâncias de Produto
- CSLU - Utilitário Cisco Smart Licensing
- RUM - Medição de Utilização de Recursos
- ACK - Confirmação
- UDI - Identificação exclusiva do dispositivo - PID + SN
- SLP - Licenciamento inteligente usando política

Por que essa mudança?

Com a introdução do modelo Smart Licensing de trust and verify, a Cisco tem suportado vários mecanismos de implantação para rastrear e relatar o uso da licença para o CSSM. No entanto, não era facilmente adaptável para todos os tipos de implantações - havia feedback e requisitos em campo para tornar o Smart Licensing mais favorável para adoção. Alguns dos desafios são:

- Com o registro SL - Os dispositivos precisam estar sempre conectados à Internet para acessar o CSSM, que é uma preocupação de implantação.
- Os servidores de satélite no local apresentam mais custo de implantação e manutenção.
- O SLR facilita apenas redes com isolamento de ar.
- As implantações que não suportam nenhum desses modelos precisam executar seus dispositivos no Unregistered/Eval expired estado, mesmo após a compra das licenças.

O SLP é introduzido para facilitar vários pedidos desse tipo no campo. Com o SLP, você não precisa registrar o produto no CSSM. Todos os níveis de licença adquiridos são "em uso" prontos para uso. Isso remove o atrito de dia 0 que estava presente no dispositivo. O SLP também minimiza o fluxo de trabalho de provisionamento de licenças e reduz o excesso de pontos de contato. Não há necessidade de o dispositivo estar conectado ao CSSM o tempo todo. O SLP também oferece a capacidade de usar licenças na rede desconectada, relatar o uso da licença off-line e relatar a licença em intervalos determinados pelas políticas do cliente.

Licenças disponíveis

Os recursos de software disponíveis se enquadram nos níveis de licença básica ou complementar. As licenças básicas são licenças perpétuas e as licenças complementares estão disponíveis por três, cinco e sete anos.

Licenças básicas

- Conceitos Essenciais de Rede
- Vantagem da rede
- HSECK9

Licenças complementares

- Fundamentos do DNA
- Vantagem do DNA

Observação: HSECK9 é uma licença de exportação controlada. Requer um SLAC para ativar a licença e o respectivo recurso.

Os novos componentes

Política

A política decide qual deve ser o comportamento padrão para o PI. Ele informa os atributos de requisitos de relatórios de licenciamento para diferentes níveis e condições de licença. A política também determina se a mensagem ACK deve ser enviada de volta ao PI, para cada relatório enviado ao CSSM ou não. A diretiva também contém o nome da diretiva e quando ela é instalada. A política padrão da Cisco é comum e padrão para todos os produtos catalyst. No entanto, a política definida pelo cliente também é permitida se você quiser ter intervalos de relatório e omissão de resposta ACK diferentes.


A política pode ser instalada em um PI em várias ocasiões.

- Política padrão presente no software
- Política instalada pela indústria da Cisco
- Política instalada através da resposta ACK
- Política instalada manualmente por meio da CLI
- Política enviada usando a Solicitação Yang

Esta saída mostra a aparência de uma política padrão.

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)

 **Observação:** uma política não pode ser apagada quando você apaga/modifica uma configuração de sistema, limpa a nvram ou formata a flash: filesystem. A política é definida como padrão da Cisco, na **redefinição de fábrica inteligente da licença**.

Relatórios RUM


RUM são relatórios de uso gerados e armazenados pelo PI. Os relatórios de RUM padrão ISO19770-4 estão concluídos para o SLP. Os relatórios RUM armazenam todas e quaisquer alterações no uso da licença feitas no PI como arquivos de relatório. Os dados de uso para cada nível de licença são armazenados em relatórios RUM separados. As medições do relatório RUM são coletadas e armazenadas em PI em intervalos regulares. Sempre que houver uma alteração no uso da licença do PI ou um relatório de uso tiver sido disparado ou quando os relatórios tiverem atingido o tamanho/amostras máximos, novos relatórios de RUM para todos os níveis de licença serão gerados. Em outros casos, os relatórios de RUM existentes podem ser substituídos por uma nova amostra e um carimbo de data/hora atualizado. A medição do utilitário de relatório RUM

padrão é a cada 15 minutos. A cada intervalo de relatório, os relatórios RUM são enviados ao Cisco CSSM.

Todos os relatórios RUM são assinados pelo PI e verificados pelo CSSM. Quando o CSSM recebe os dados de relatório RUM do PI, ele valida o relatório, verifica o cronograma de alteração de uso da licença e atualiza os dados do CSSM de acordo. O CSSM então confirma para o PI através da mensagem de resposta ACK.

Os relatórios RUM podem ser enviados ao CSSM de várias maneiras:

- O PI envia relatórios de RUM ao CSSM diretamente no intervalo de relatório.
- O PI envia o relatório RUM para a CSLU.
- A CSLU obtém relatórios de RUM do PI em intervalos regulares através de modelos RESTAPI e YANG.
- Os relatórios de RUM são salvos manualmente no PI por meio da CLI e carregados manualmente no CSSM.

 **Observação:** os relatórios RUM não podem ser apagados quando você apaga/modifica uma configuração do sistema, limpa a nvram ou formata a flash: filesystem. Todos os relatórios de RUM podem ser removidos do PI em 'license smart factory reset'.




Observação: o intervalo de relatório padrão é de 30 dias.

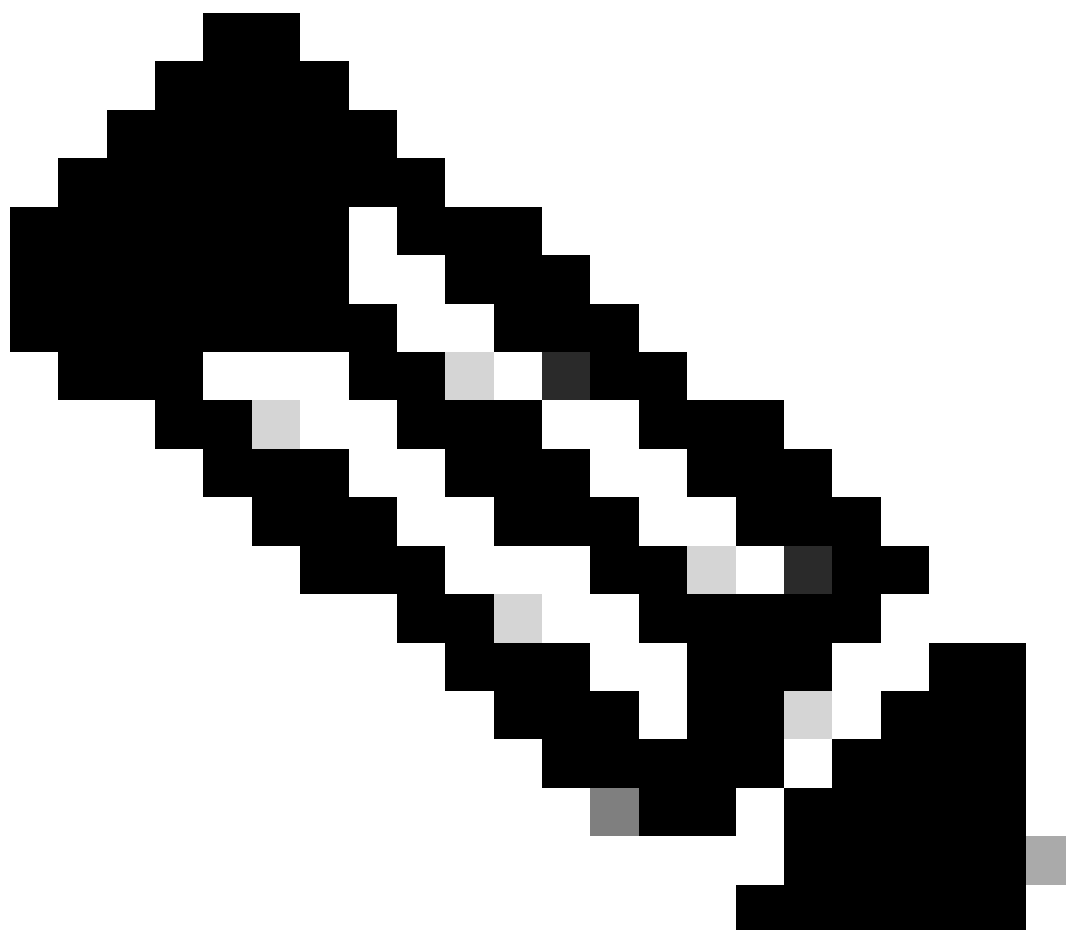
Fluxo de fabricação para caso de implantação inicial

Depois que um novo pedido de produto é feito no Cisco CCW (Cisco Commerce Workspace), o PI passa pelo fluxo de operações feito pela equipe de fabricação. Isso é para facilitar o processo seguro de assinatura de relatórios RUM e remover o atrito de dia 0 no registro do PI. Uma vez feito o pedido, qualquer SA/VA existente ou novo SA/VA criado é associado ao produto. A equipe de fabricação da Cisco cuida dessas operações antes de enviar o produto para você:

- Instale o Código de Confiança no dispositivo. A assinatura do código de confiança é instalada com base na UDI do dispositivo. Ele é instalado em todos os produtos.

- Instalar código de compra - Informações sobre quais níveis de licença são comprados junto com o produto. Ele é instalado em todos os produtos.
- SLAC - Código de Autenticação de Licença Inteligente - Não Aplicável a Plataformas Catalyst.
- Política de instalação - Política padrão ou personalizada com base em sua entrada.
- Relate o uso da licença para CSSM - SA/VA.

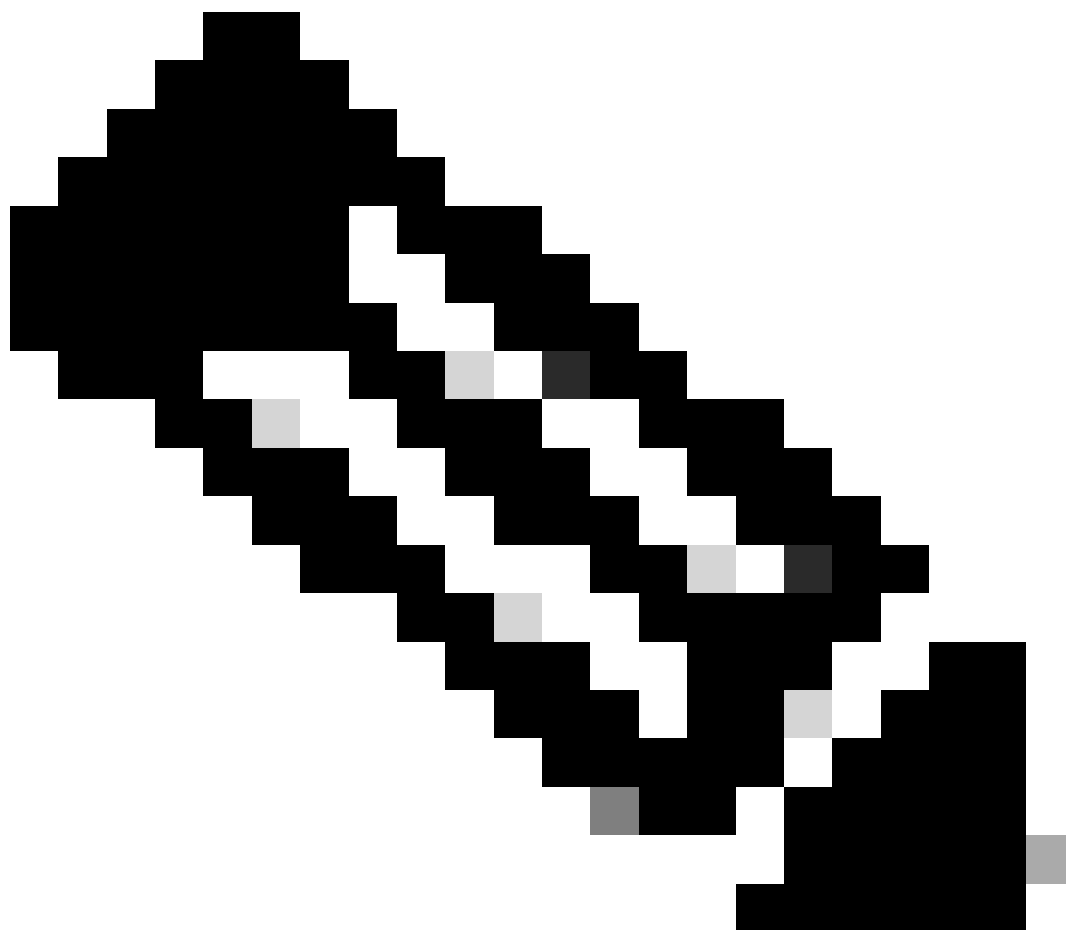
 **Observação:** com a versão 17.3.3, esse fluxo é seguido para todas as plataformas de switching Catalyst, exceto para C9200/C9200L.



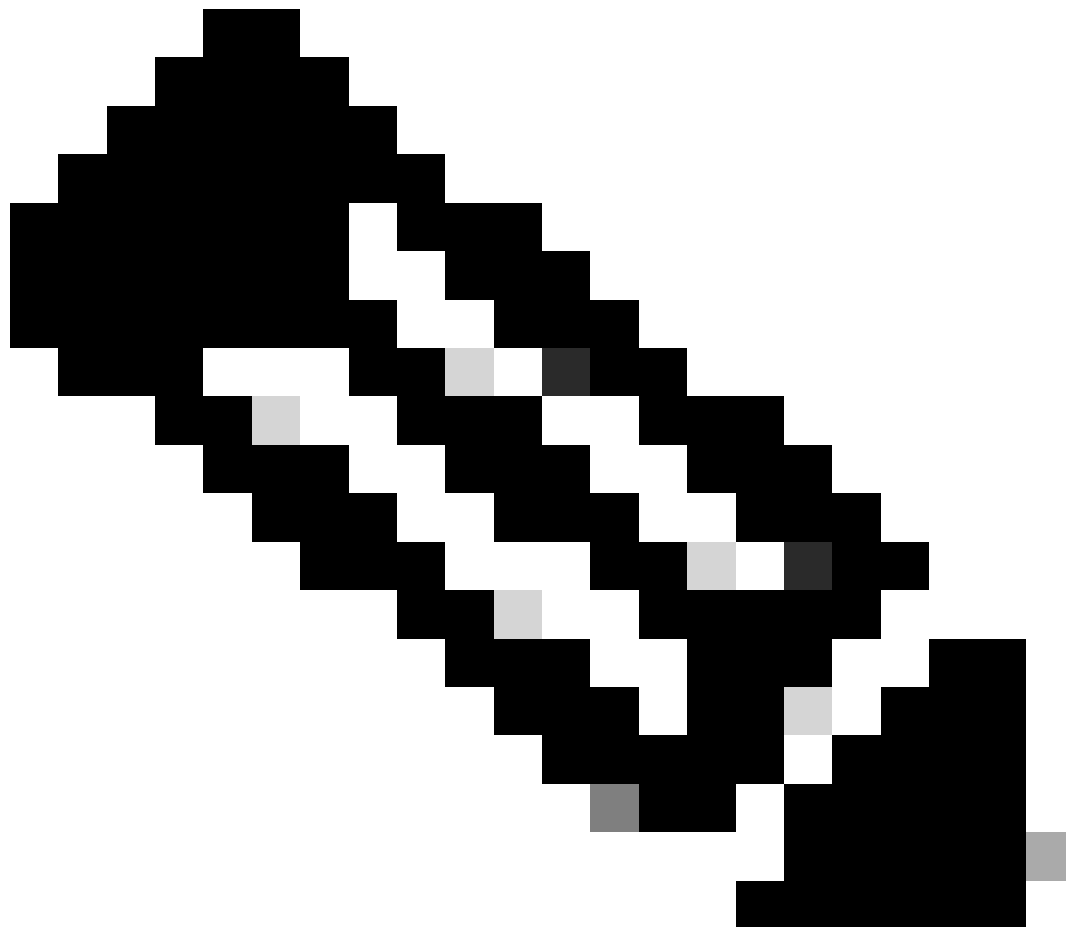
Observação: o código de confiança é instalado somente na fabricação com 17.7.1 para todas as plataformas de switching Catalyst, exceto C9200/C9200L.

CSLU

O SLP traz uma nova ferramenta simples, porém poderosa, o CSLU. CSLU é uma ferramenta baseada em GUI, que roda no sistema operacional Windows 10 ou versão Linux baseada em RHEL/Debian. O CSLU, que pode ser executado na sua rede privada local, é responsável por coletar as portas RUM dos PIs associados ao CSSM. A CSLU deve ser provisionada de forma a coletar relatórios de RUM sobre PIs na rede local e também para enviar periodicamente o relatório de RUM ao CSSM pela Internet. A CSLU é uma ferramenta simples, que exibe apenas os detalhes dos UDIs dos dispositivos provisionados. Todos os dados de Uso de Licença para PIs, Licenças Compradas e Licenças Não Utilizadas no pool são vistos apenas no SA/VA do CSSM, para que você verifique. Ele é eficiente porque pode coletar relatórios de uso de até 10.000 PIs. O CSLU também é responsável por enviar as mensagens ACK do CSSM de volta ao PI.



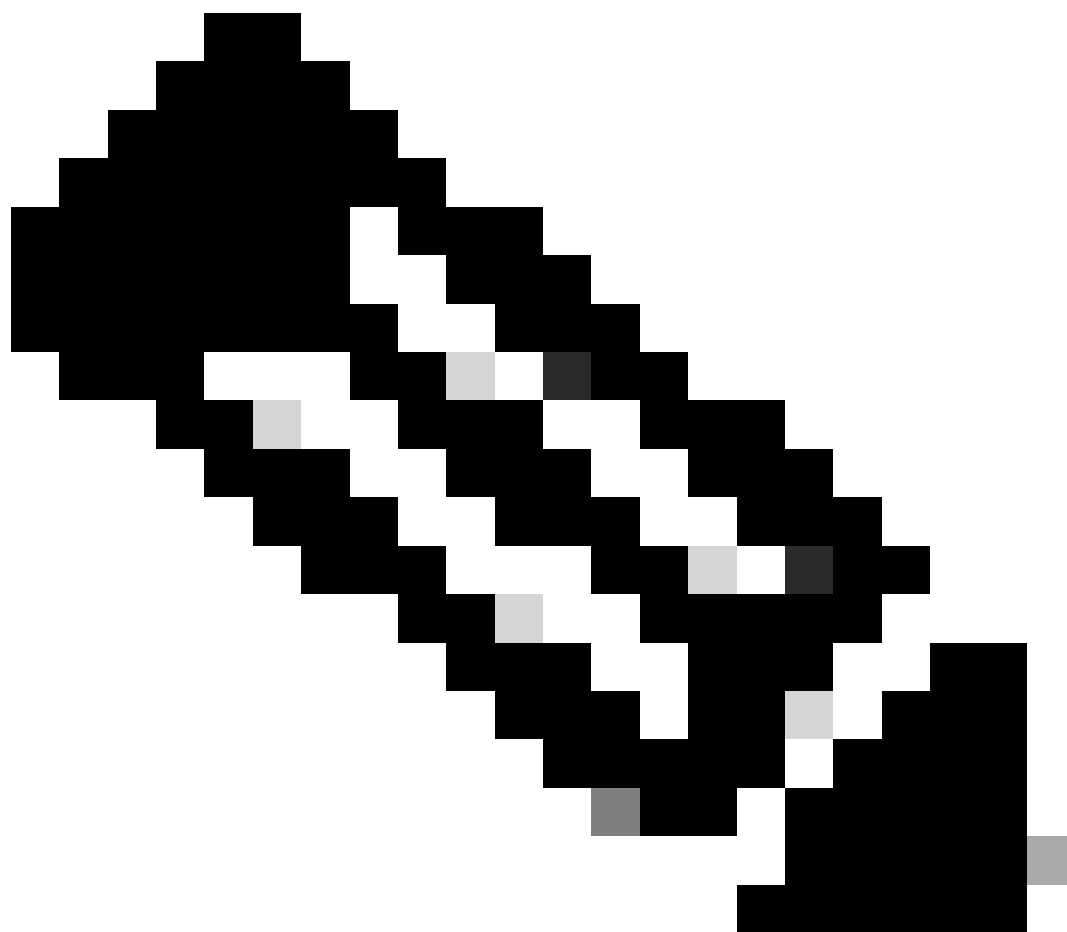
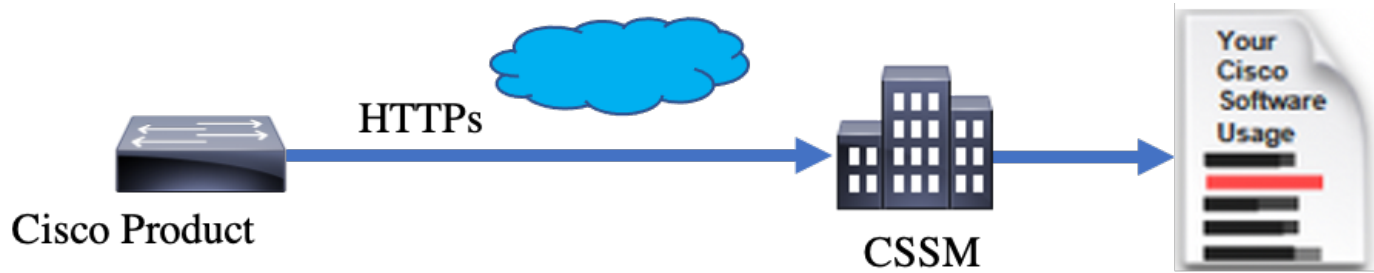
Observação: consulte a seção Topologia baseada em CSLU para obter a configuração detalhada e os modos suportados de Operação de CSLU.



Observação: a versão Linux do CSLU é suportada a partir da versão 17.7.1.

SLP - Conexão direta

Em um produto enviado de fábrica, o modo de transporte padrão é configurado como CSLU. Se quiser usar o método Direct Connect, você deve alterar o modo de transporte para Call-home ou SMART com base no requisito. O requisito básico para o método de conexão direta da topologia é ter conectividade com a Internet para o acesso ao CSSM. Além disso, deve-se garantir que, para a conectividade ao CSSM, as configurações de L3 necessárias, DNS e Domínio estejam presentes no dispositivo.




Observação: o transporte inteligente é o método de transporte recomendado quando você se conecta diretamente ao CSSM.

Na topologia de conexão direta, os relatórios de RUM são enviados diretamente ao CSSM. Os Relatórios de Licença exigem que um Código de Confiança seja instalado com êxito no dispositivo. O Código de Confiança é instalado pela fabricação da Cisco no Dispositivo antes de ser enviado. Você também pode instalar o Trust Code no dispositivo.

O Código de Confiança é uma string de token extraída do CSSM, na Virtual Account - Página Geral. O Trust Code pode ser instalado por meio da CLI.

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

 **Observação:** todas as opções devem ser usadas para o sistema HA ou Stacking back. Para um dispositivo autônomo, a opção local pode ser usada.

```
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

Depois que o Código de Confiança for instalado com êxito, o PI poderá relatar o uso diretamente ao CSSM. Essas condições resultam em relatórios de licença:

- Uma instalação de Código de Confiança bem-sucedida
- Em todos os intervalos de relatório padrão
- Recarga/inicialização no dispositivo
- Um switchover
- Adição ou remoção de um membro da pilha
- Acionamento manual de sincronização de licença

O relatório de licença para CSSM pode ser acionado com estas CLI:

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

A seção Relatório de uso no show license status informa os cronogramas do último ACK recebido, o próximo prazo ACK, o próximo envio de relatório e o último envio de relatório.

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>

Conexão direta - Transporte inteligente

Em uma topologia de modo Direct Connect ou Direct Cloud Access, se o Transporte INTELIGENTE for usado, essas serão as configurações necessárias no dispositivo.

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 - Transporte Call-Home

Em uma topologia de modo Direct Connect ou Direct Cloud Access, se o Transporte Call-home for usado, essas serão as configurações necessárias no dispositivo.

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
```

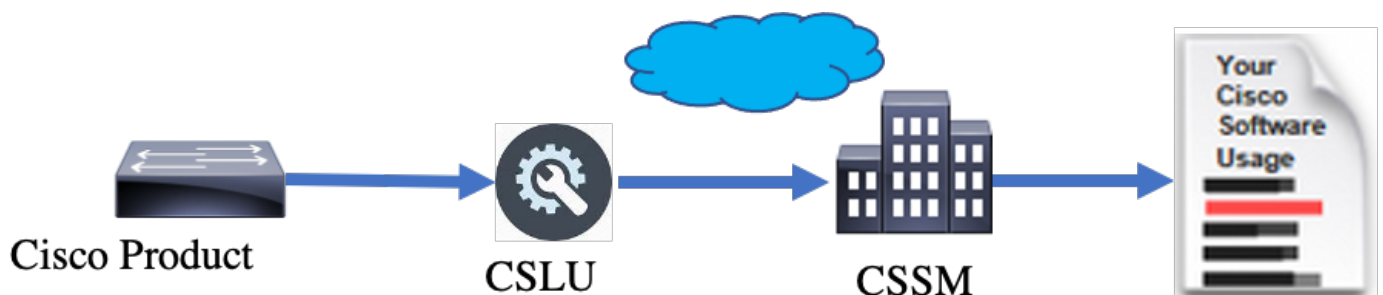
```
contact-email-addr shmandal@cisco.com
```

```
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
!
```

 **Observação:** por padrão, o endereço de destino do Call-home é configurado para o URL do CSSM. Isso pode ser verificado na configuração `doshow run all`.

SLP - CSLU

O modo CSLU é o modo de transporte padrão nos dispositivos enviados de fábrica que executam a versão 17.3.2 ou posterior. Além disso, se você migrar de licenças expiradas de avaliação/avaliação, o modo de transporte após a mudança para o SLP será CSLU. Na topologia baseada em CSLU, a CSLU fica entre o PI e o CSSM. O CSLU evita que os usuários não tenham conectividade de rede direta com o Cisco Cloud - CSSM. A CSLU pode ser executada localmente em uma rede privada e baixar relatórios de uso de todos os PIs associados. Os relatórios de uso são salvos localmente no PC com Windows antes de serem enviados ao CSSM pela Internet. CSLU é uma ferramenta leve. Você pode ver apenas a lista de PIs associados a ele e ele pode ser identificado com o uso de UDIs. A CSLU não pode exibir ou conter as Informações de Redundância de PI ou Níveis de Licença ou Uso de Licença.

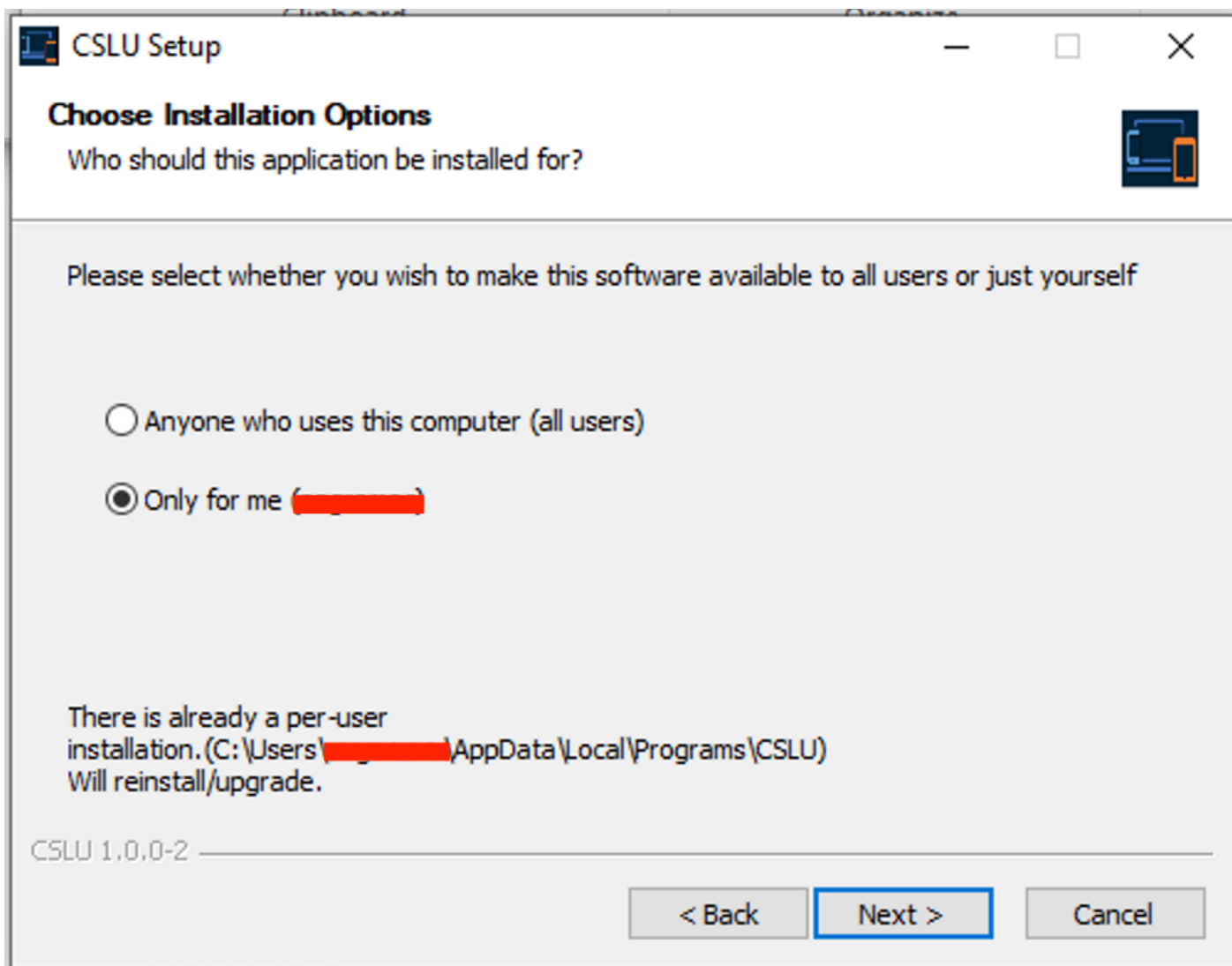


Instalação e configuração do CSLU

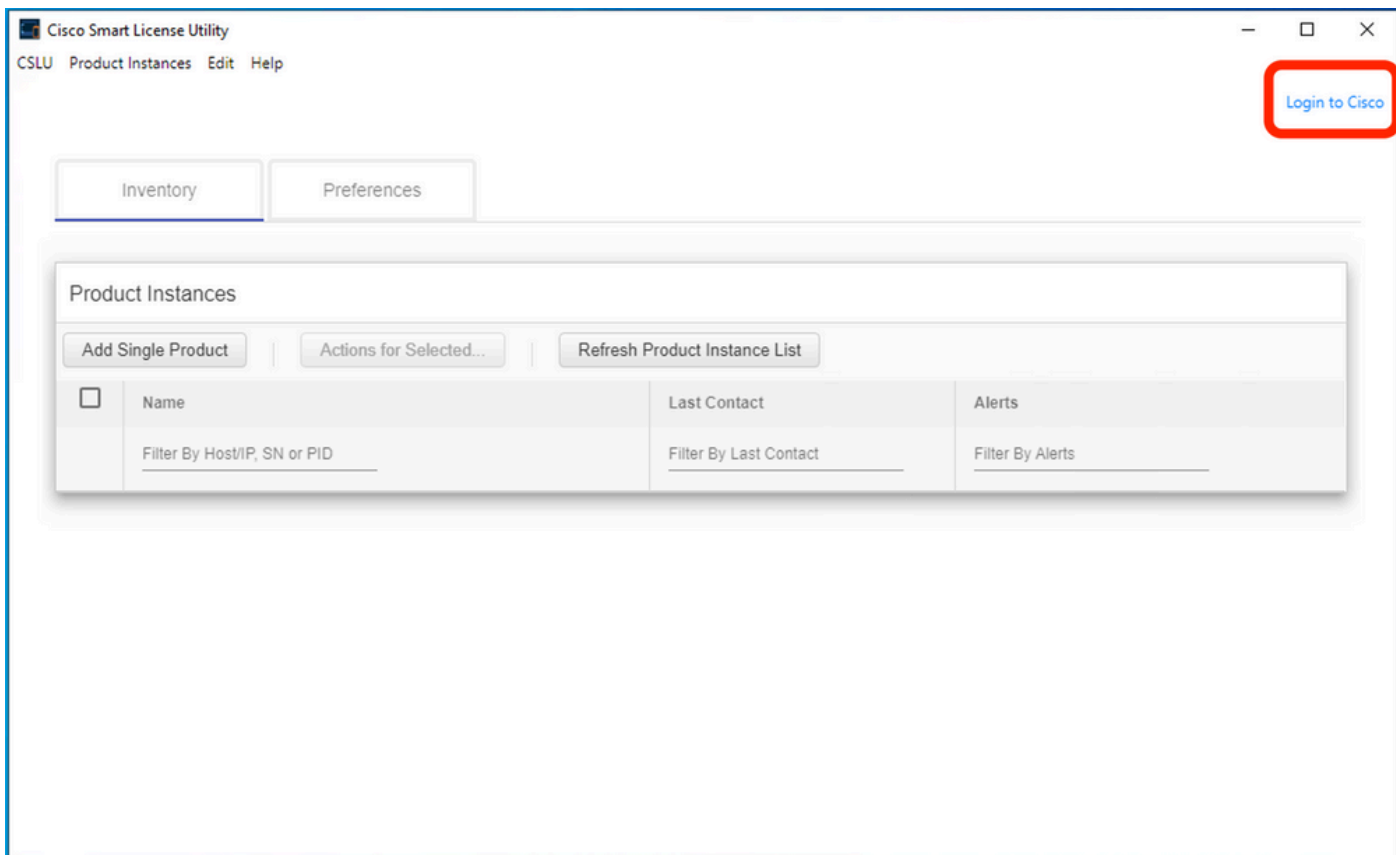
A ferramenta CSLU é instalada e operada em máquinas com Windows 10. O software está disponível no CCO para download e para uso gratuito. Quando a ferramenta estiver instalada, o Manual de usuário/Guia de início rápido poderá ser baixado no menu Ajuda e navegue até Help > Download Help Manual.

A instalação do CSLU exige que você aceite o Contrato de licença.

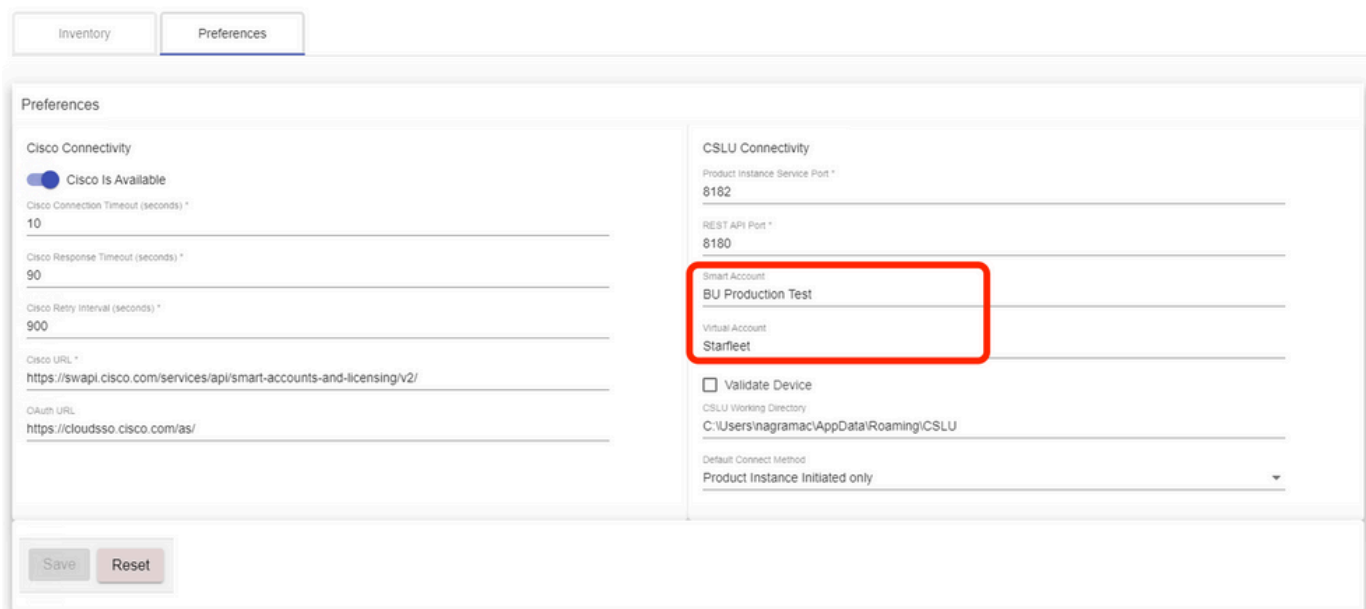
É recomendável que o aplicativo seja instalado apenas para o usuário atual e não para todos os usuários que trabalham no computador. Se uma versão anterior do CSLU já estiver presente no PC, é recomendável desinstalá-la com antecedência. No entanto, a nova instalação tem o cuidado de atualizar o software.



Após a instalação, faça login na Cisco, com o uso da opção de login presente no canto superior direito do aplicativo. Ele usa suas credenciais CEC. E através do login, a confiança é estabelecida entre CSLU e CSSM.



Depois de fazer login na Cisco, verifique se os detalhes de SA e VA foram escolhidos corretamente no menu suspenso, no painel Preferências da ferramenta. Salve as configurações.

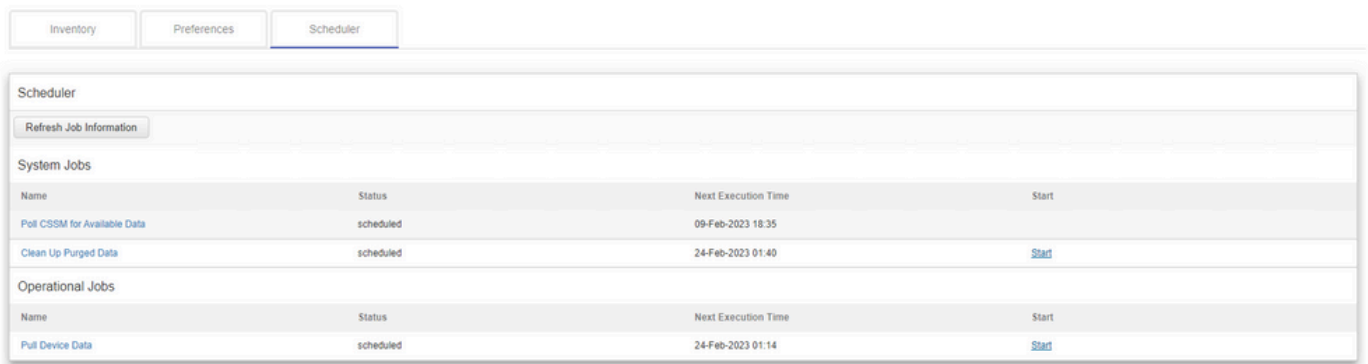


Guia Agendamento no CSLU - Através da guia agendamento no CSLU, você pode configurar:

- Sondar o CSSM quanto aos dados disponíveis - Mostra os tempos de trabalho, o último tempo de recebimento e o próximo tempo de recebimento de dados do CSSM.
- Limpar dados limpos - Remove todos os dados limpos do armazenamento de dados da CSLU. Ele também pode ser acionado

manualmente.

- Dados do dispositivo de recebimento - Aciona o modo de recebimento da CSLU.



The screenshot shows a web interface with three tabs: 'Inventory', 'Preferences', and 'Scheduler'. The 'Scheduler' tab is active. Below the tabs is a 'Refresh Job Information' button. The main content is divided into two sections: 'System Jobs' and 'Operational Jobs'. Each section contains a table with columns for Name, Status, Next Execution Time, and Start.

System Jobs			
Name	Status	Next Execution Time	Start
Poll CSRM 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

CSLU usando o modo PUSH

Por padrão, a CSLU opera no modo PUSH. No modo PUSH, o PI envia os relatórios de uso ao CSLU em intervalos regulares. A partir do dispositivo, você deve garantir que o alcance da rede L3 para CSLU esteja disponível. Para que o PI se comunique com a CSLU, o endereço IP da máquina Windows que executa a CSLU deve ser configurado.

```
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>

Os relatórios são enviados ao CSLU pelo PI nas seguintes condições:

- Em cada intervalo de relatório padrão
- Recarga/inicialização no dispositivo
- Ao Alternar
- Adição ou remoção de membro na pilha
- Ao disparar manualmente a sincronização de Licenças

No CSLU, a página de inventário lista os dispositivos atualmente associados ao CSLU. Os dispositivos na lista podem ser identificados através do UDI. Os dispositivos podem ser filtrados com base em PID ou SN da lista para identificar qualquer dispositivo em particular.

A página de inventário do CSLU também tem duas outras colunas:

- A coluna **Último Contato** - Mostra o Carimbo de Data/Hora mais recente quando o status do relatório foi alterado.

- A **Coluna Alerta** - Mostra o status de relatório mais recente do PI.

Depois que o PI envia o relatório ao CSLU, o CSLU cria a entrada de PI no CSSM. O status do TS do Último Contato e dos Alertas é atualizado.

Name	Last Contact	Alerts
<input type="checkbox"/> UDI_PID:C9500-320C; UDI_SN:CAT2148L15K <small>Filter By HostIP, SN or PID</small>	<small>Filter By Last Contact</small> 08-Nov-2020 06:37	<small>Filter By Alerts</small> COMPLETE: Usage report from product instance
<input type="checkbox"/> UDI_PID:C9500-24Y4C; UDI_SN:CAT2344L4GH	03-Nov-2020 18:27	COMPLETE: Usage report acknowledgement to product instance

Name	Last Contact	Alerts
<input type="checkbox"/> UDI_PID:C9500-320C; UDI_SN:CAT2148L15K <small>Filter By HostIP, SN or PID</small>	08-Nov-2020 06:37	COMPLETE: Usage report uploaded to CSSM
<input type="checkbox"/> UDI_PID:C9500-24Y4C; UDI_SN:CAT2344L4GH	03-Nov-2020 18:27	COMPLETE: Usage report acknowledgement to product instance

O CSSM processa os relatórios enviados pelo CSLU e adiciona/atualiza a instância do produto no CSSM, com base no uso da licença. Depois que o CSSM processa e atualiza a data, ele retorna a mensagem ACK para o CSLU. O CSLU, por sua vez, armazena e encaminha a mensagem de volta ao PI.

A mensagem ACK consiste em:

- Confirmação de todos os relatórios enviados
- Política
- Código de Confiança


Se uma nova política estiver disponível para você no CSSM, ela também será atualizada para o PI. Se a política não for alterada, o mesmo será enviado para o PI.



Observação: se o relatório de mensagem ACK não for exigido de acordo com sua política, a mensagem ACK não será enviada.

A coluna de mensagem de alerta pode ter um destes status:

- Relatório de uso da instância do produto
- Relatório de uso carregado para a Cisco
- Solicitação de sincronização da instância do produto
- Solicitação de sincronização carregada no CSSM
- Confirmação recebida do CSSM
- Confirmação de relatório de uso para instância de produto

 **Observação:** no CSLU em um sistema HA, sempre a entrada é vista apenas para o UDI do Ative Directory. Somente o CSSM tem todo o UDI para dispositivos individuais no sistema listado.

Descoberta automática de CSLU

Para oferecer suporte a implantações em escala com configurações mínimas, a descoberta automática da CSLU é compatível. Isso significa que você não precisa configurar o endereço IP/URL da CSLU especificamente. Para conseguir isso, basta adicionar uma entrada ao servidor DNS. Isso permite que o dispositivo, que tem o modo de transporte como CSLU (que é o padrão), descubra automaticamente a CSLU e envie relatórios.

Algumas coisas a serem garantidas aqui:

- Crie uma entrada no servidor DNS. O endereço IP da CSLU deve ser mapeado para o nome cslu-local.
- Verifique se o servidor de nomes e as configurações DNS estão presentes no dispositivo para acessibilidade.

Com isso, sem configurações adicionais, os dispositivos na rede podem acessar a CSLU e enviar relatórios de RUM em intervalos regulares.

CSLU usando o modo PULL

O modo PULL é onde a CSLU inicia o processo para buscar os relatórios de RUM dos dispositivos. Aqui, os detalhes do dispositivo são adicionados à CSLU e a CSLU busca os dados em todos os dispositivos adicionados em intervalos regulares. O PULL da CSLU também pode ser acionado manualmente. O CSLU, por sua vez, envia o relatório RUM ao CSSM e as mensagens ACK que são recebidas de volta do CSSM são enviadas ao PI. O modo PULL é suportado por três meios diferentes - RESTAPI, NETCONF e RESTCONF.

Modo PULL usando RESTAPI

Para que o modo PULL funcione RESTAPI, as configurações necessárias do dispositivo e da CSLU são:

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  
!
```



Observação: o usuário deve ter acesso Priv level 15.

CSLU - Procedimento para configuração

O CSLU deve estar conectado ao CSSM para que os relatórios sejam sincronizados automaticamente.

Etapa 1. Escolha Add Single Product na página Inventário.

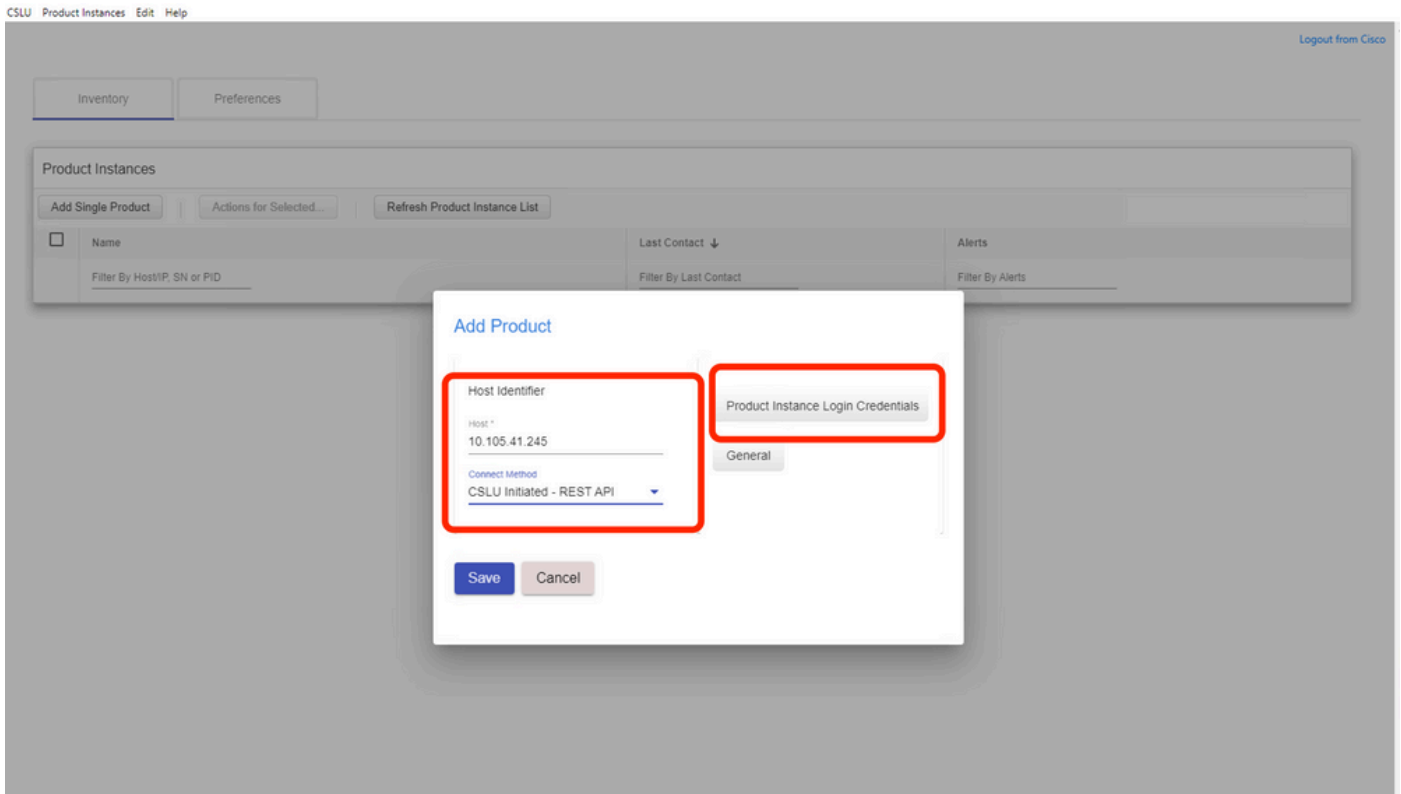
Etapa 2. Insira o IP do dispositivo.

Etapa 3. Escolha o método de conexão como RestAPI.

Etapa 4. Selecione a instância do produto Credenciais de login.

Etapa 5. Insira as credenciais do usuário com acesso Priv 15.

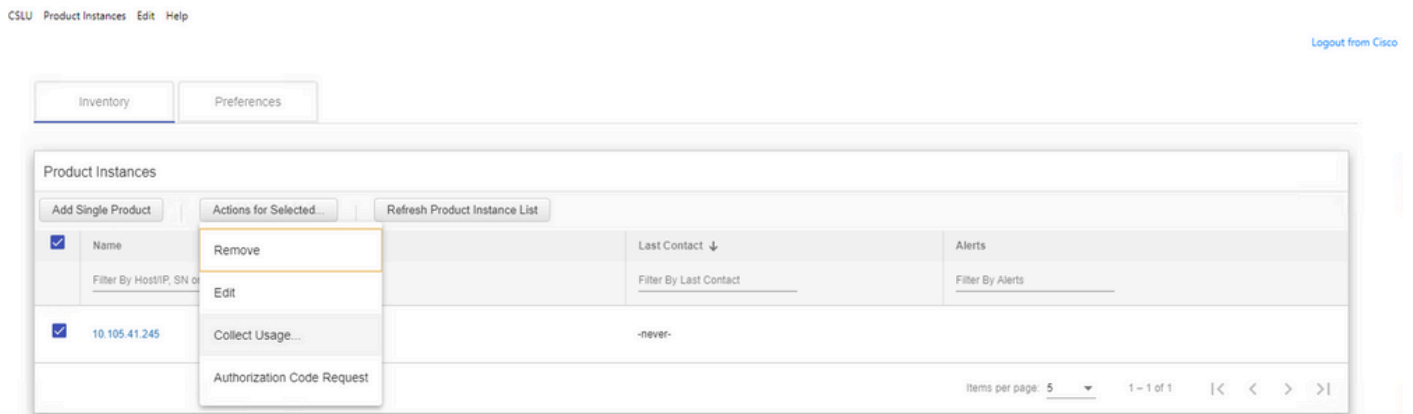
Etapa 6. Salve as configurações.



O dispositivo é adicionado com um único endereço IP no campo Nome.

Escolha o dispositivo e navegue até Actions for Selected > Collect Usage.

Quando os dados de uso são coletados com êxito, o campo Nome é atualizado para o UDI do PI e o carimbo de data e hora também é atualizado. O campo de alerta reflete o status mais recente.



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	
<input checked="" type="checkbox"/> UDI_PID:C9500-32QC; UDI_SN:CAT2148L15K	11-Nov-2020 23:53	COMPLETE: Usage report uploaded to CSSM	
		Items per page: 5	1 - 1 of 1

Se o dispositivo ainda estiver disponível quando a mensagem ACK for recebida do CSSM, o ACK será enviado de volta ao PI. Caso contrário, o ACK será enviado no próximo Intervalo de recebimento.

Modo PULL usando RESTCONF

Para que o modo PULL funcione RESTCONF, as configurações necessárias do dispositivo e as etapas do CSLU são:

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
!
```



Observação: essas configurações são para autenticação local. A autenticação remota também pode ser usada.

CSLU - Procedimento para configuração

O CSLU deve estar conectado ao CSSM para que os relatórios sejam sincronizados automaticamente. A configuração da CSLU é a mesma RESTAPI para a coleta e o relatório do RUM.

Etapa 1. Escolha Add Single Product na página Inventário.

Etapa 2. Insira o IP do dispositivo.

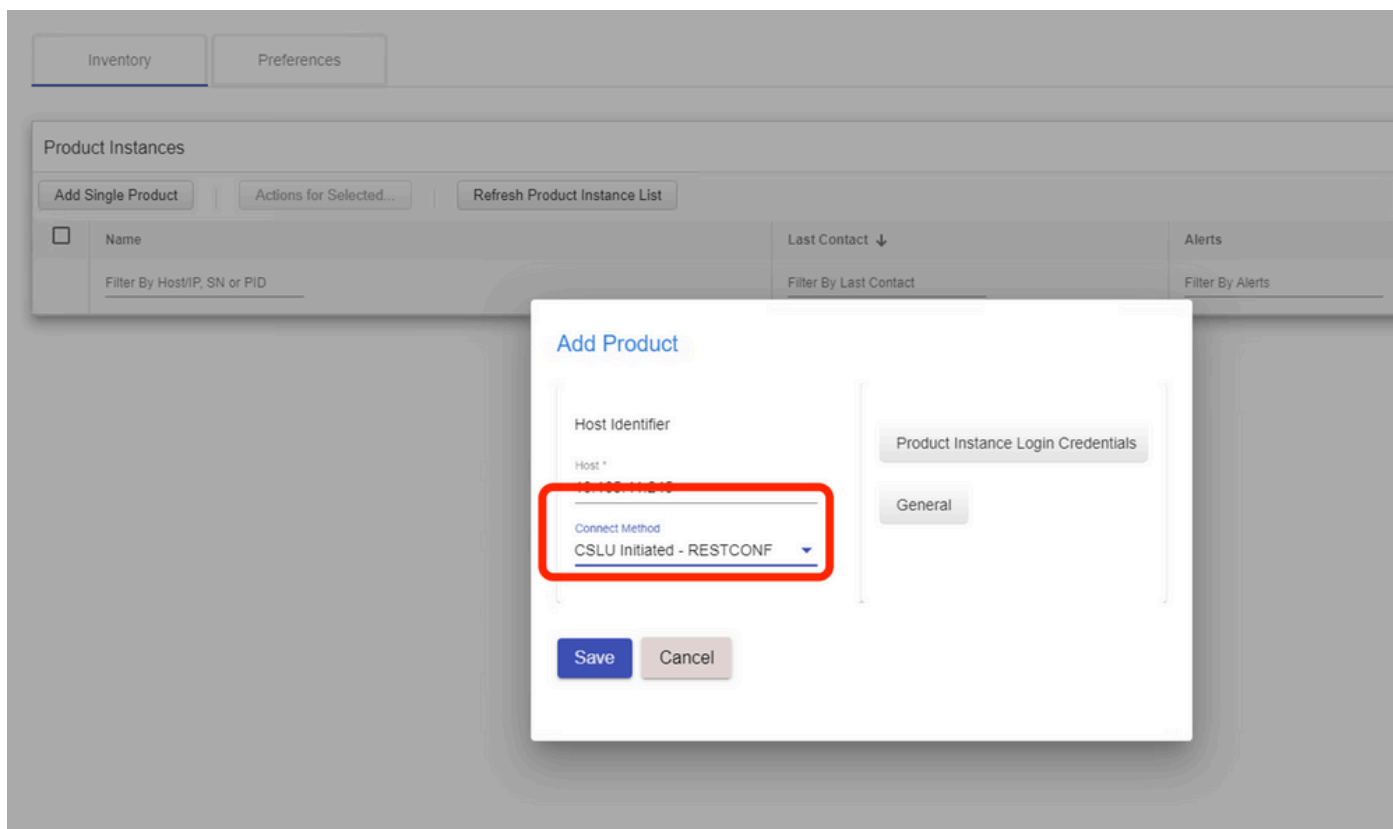
Etapa 3. Escolha o método de conexão como RESTCONF.

Etapa 4. Selecione a instância do produto Credenciais de login.

Etapa 5. Insira as credenciais do usuário com acesso Priv 15.

Etapa 6. Salve as configurações.

Passo 7. Coletar dados de uso para o dispositivo selecionado.



Modo PULL usando NETCONF

Para que o modo PULL funcione NETCONF, as configurações necessárias do dispositivo e as etapas do CSLU são:

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



Observação: essas configurações são para autenticação local. A autenticação remota também pode ser usada.

CSLU - Procedimento para configuração

O CSLU deve estar conectado ao CSSM para que os relatórios sejam sincronizados automaticamente. A configuração da CSLU é a mesma RESTAPI para a coleta e o relatório do RUM.

Etapa 1. Escolha Add Single Product na página Inventário.

Etapa 2. Insira o IP do dispositivo.

Etapa 3. Escolha o método de conexão como NETCONF.

Etapa 4. Selecione a instância do produto Credenciais de login.

Etapa 5. Insira as credenciais do usuário com acesso Priv 15.

Etapa 6. Salve as configurações.

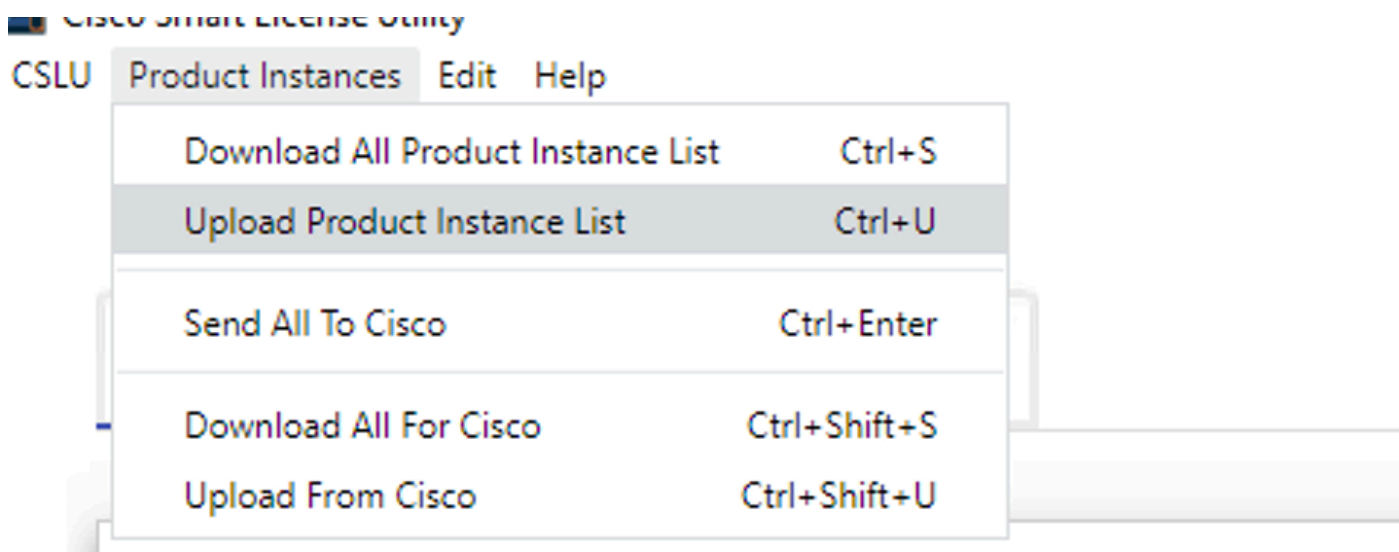
Passo 7. Coletar dados de uso para o dispositivo selecionado.

The screenshot shows the 'Product Instances' management interface. At the top, there are buttons for 'Add Single Product', 'Actions for Selected...', and 'Refresh Product Instance List'. Below these is a table with columns for 'Name', 'Last Contact', and 'Alerts'. A modal dialog titled 'Add Product' is open in the foreground. It has a 'Host Identifier' section with a 'Host *' input field. Below that is a 'Connect Method' dropdown menu, which is highlighted with a red rectangle and shows 'CSLU Initiated - NETCONF' as the selected option. To the right of the dropdown are two tabs: 'Product Instance Login Credentials' and 'General'. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

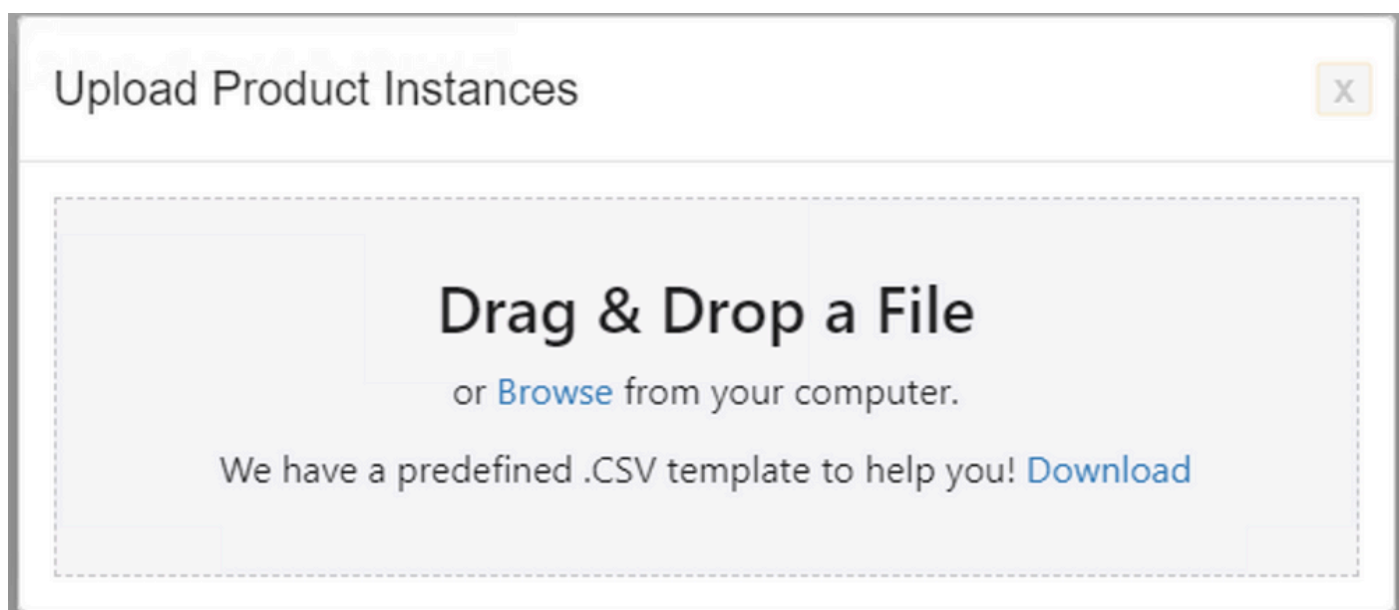


Observação: para todos os modelos, NETCONF, RESTCONF e RESTAPI, a lista de dispositivos pode ser adicionada em massa.

Para executar o carregamento em massa, na Menu barra, navegue para Product Instance > Upload Product Instance List, como mostrado nesta imagem.



Uma nova janela pop-up será aberta. O arquivo de modelo pode ser baixado a partir dele. No arquivo de formato CSV, preencha os detalhes do dispositivo da lista de dispositivos e carregue no CSLU para adicionar vários dispositivos.



Observação: para todos os tipos de modo PULL de CSLU, é recomendável definir o conjunto de transporte como Off no PI. Isso pode ser feito com o uso do CLI.

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

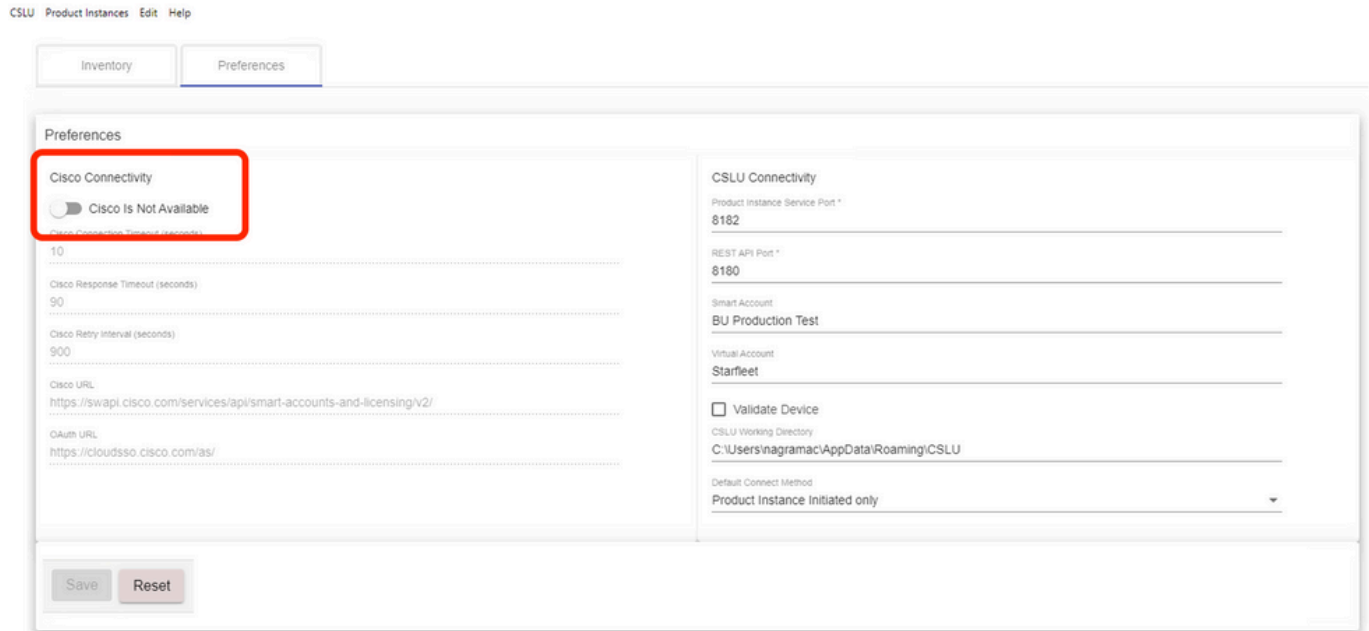
CSLU usando o modo desconectado

O CSLU pode operar no modo desconectado do CSSM. Isso se aplica a implantações que não permitem que a CSLU seja conectada à Internet. No modo desconectado, os relatórios de todos os dispositivos são baixados manualmente do CSLU e carregados no CSSM. Por sua vez, as

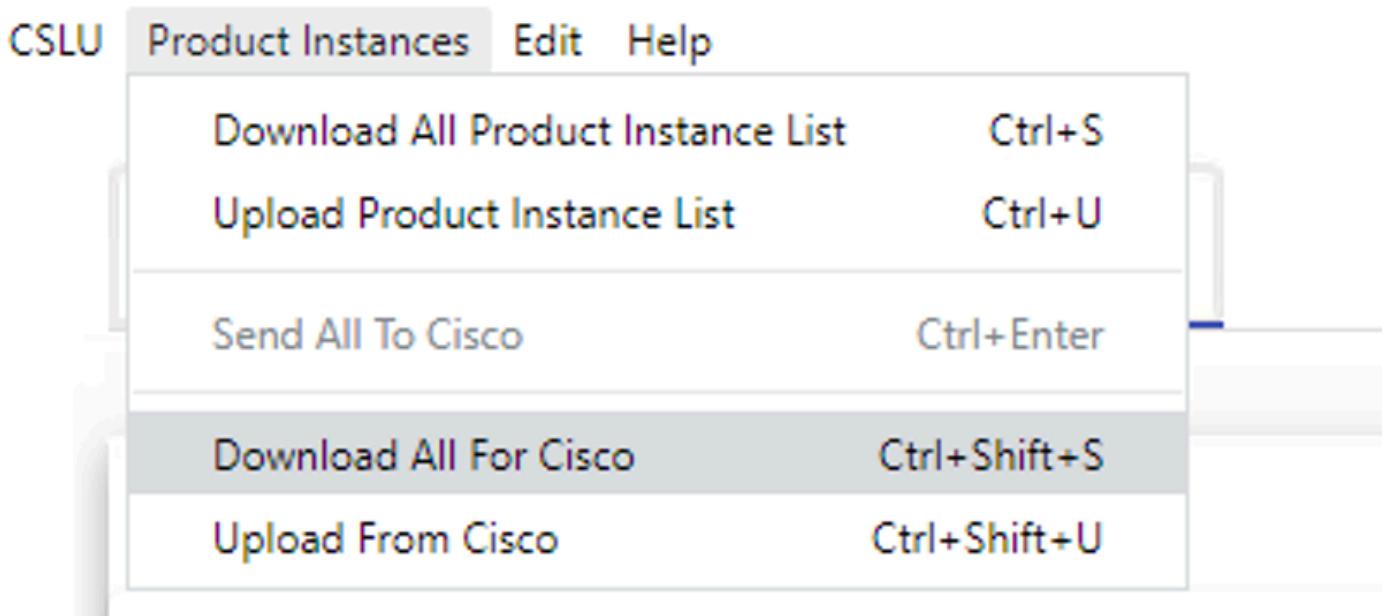
mensagens ACK são baixadas do CSSM e carregadas no CSLU. A CSLU ainda continua a receber as datas de uso de PULL/PUSH dos PIs e também envia a mensagem ACK de volta ao PI.

Etapa 1. Na CSLU Preference página, desative a opção Cisco Connectivity. Isso confirma que a Cisco não está disponível.

Etapa 2. Salve as configurações.



Etapa 3. Na barraMenu, clique em Product Instances > Download All for Cisco. Isso faz o download de um tar.gz arquivo para a CSLU.



Etapa 4. Carregue o arquivo no CSSM. Na página Smart Account do CSSM, navegue até Report > Usage Data Files > Upload usage data. No pop-up, carregue o arquivotar.gz.

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	📘 No Errors	2	Download
Usage_SLR.txt	2020-Oct-29	Quake	📘 No Errors	1	Download
+ UD_SA_BU_Production_Test_20Oct28_11_11_03	2020-Oct-28	DLC-VA1	📘 No Errors	1	Download
+ UD_SA_20Oct28_10_49_13_092.tar.gz	2020-Oct-28	DLC-VA1	📘 No Errors	1	Download
+ UD_SA_BU_Production_Test_20Oct28_10_46_25	2020-Oct-28	DLC-VA1	📘 No Errors	1	Download
Usage_17_3_2.txt	2020-Oct-28	Quake	📘 No Errors	1	Download
Usage_17_3_2.txt	2020-Oct-28	Quake	🚫 Errors (1)	1	Download
Usage_17_3_2.txt	2020-Oct-28	Quake	📘 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

Etapa 5. Depois que os dados são processados, a confirmação é gerada. Faça download do arquivo ACK e carregue-o no 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

Etapa 6. No CSLU, importe o arquivo ACK da barra Menu e navegue até Product Instances > Upload from Cisco, como mostrado nesta imagem.

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

Passo 7. Depois que o ACK é carregado, a mensagem é enviada aos PIs. O mesmo pode ser verificado pela coluna Alertas.

CSLU Product Instances Edit Help

Inventory Preferences

Product Instances

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

Name	Last Contact ↓	Alerts
Filter By HostIP, SN or PID	Filter By Last Contact	Filter By Alerts
<input type="checkbox"/> UDI_PID:C9500-32QC; UDI_SN:CAT2148L15K	12-Nov-2020 01:10	COMPLETE Usage report acknowledgement to product instance

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

SLP - Modo Offline

O SLP também pode funcionar no Modo Offline total. Isso é principalmente para redes com isolamento de ar, que não preferem a conectividade com a Internet e também optam por não usar a CSLU. No modo off-line, o transporte é definido como 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>

Sempre que quiser relatar os dados de uso ao CSSM, os relatórios de uso devem ser baixados como um arquivo e carregados manualmente no CSSM. Em um sistema HA, o ative coleta o uso de dispositivos de standby/membros.

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

Agora, esse relatório precisa ser carregado manualmente no CSSM.

Exporte os dados de uso salvos do PI para o desktop.

Na página Smart Account do CSSM, navegue até Report > Usage Data Files > Upload usage data. Na janela pop-up, escolha o relatório de uso e clique em upload.

Depois que o arquivo for carregado, você deve escolher o VA correto ao qual o dispositivo está associado.

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

Quando os dados forem processados completamente e a confirmação estiver pronta, baixe o arquivo e carregue-o no 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 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

Alterações de comportamento

Essas alterações são feitas no recurso Smart Licensing em versões:

- **Sincronização de Confiança** - A partir do 17.7.1, o Código de Confiança é instalado no switch em todas as topologias suportadas, como os métodos CSLU e Offline.
- **Alterações de privacidade** - A partir da versão 17.7.1, as informações de sequência de caracteres e nome de host da versão 17.9.1 são incluídas nos relatórios RUM enviados ao CSSM, se as respectivas configurações de privacidade estiverem desabilitadas.
- **Detalhes da conta** - A partir de 17.7.1, a mensagem ACK do CSSM inclui as informações da conta e os detalhes SA/VA.
- **Limitação de relatório RUM** - A partir de 17.9.1, o intervalo de relatório de quando o PI inicia a comunicação é acelerado. A frequência mínima de relatório é limitada a um dia. Isso significa que a instância do produto não envia relatórios RUM mais de uma vez por dia.

Troubleshooting

Questionário genérico de solução de problemas

Cenário 1: Alguns protocolos (ou seja, HSRP) não funcionam mais depois que você atualiza o Cisco IOS XE de uma versão muito anterior (ou seja, 16.9.x).

Verifique o nível de inicialização da licença para ver se ainda é o mesmo de antes de atualizar o Cisco IOS XE. É possível que o nível de inicialização da licença tenha sido redefinido para Networking-Essentials, que possivelmente não oferece suporte aos protocolos com falha (ou seja, HSRP).

Cenário 2: Status da licença com mensagens "Motivo da falha: falha ao enviar mensagem HTTP do Call Home" ou "Última tentativa de comunicação: PENDENTE"

Isso pode estar relacionado a problemas básicos de conectividade. Para resolver a verificação:

- Conectividade de rede para acessar o CSSM - endereço IP, rotas, etc.
- O ip http client source interface está configurado corretamente.
- Diferença de horário. (O NTP precisa ser configurado para fornecer um horário/fuso horário correto)
- Se a configuração interna do Firewall bloquear o tráfego para o CSSM

Cenário 3: E se o erro de log "%SMART_LIC-3-AUTH_RENEW_FAILED: Renovação de autorização com o Cisco Smart Software Manager (CSSM) : método indefinido 'each' para nil:NilClass" for observado após um ano de registro.

Registre novamente o produto. Gere uma nova ID de token no CSSM e registre a instância do produto novamente no CSSM.

Cenário 4: Mensagem de Erro "%SMART_LIC-3-COMM_FAILED: Communications failure", quando não há erros de conectividade com a Cisco.

Quando não há problemas de conectividade com o CSSM e se no PI, o erro mencionado ainda é visto, então pode ser porque a recente atualização do servidor fez com que o certificado fosse removido. O certificado é necessário para a autenticação TLS dos dois lados em comunicação. Nesse caso, configure o CLI ip http client secure-trustpoint SLA-TrustPoint no PI e tente novamente.

Depurar PI

Para solucionar quaisquer problemas, os comandos coletados do PI são:

```
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
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

Depurar CSLU

Se qualquer problema no CSLU for depurado, é importante que o arquivo de log desse diretório no PC instalado do CSLU seja capturado.

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

Referências relacionadas

- Migração para SL usando política - [Migração de licenças SL/SLR/PLR legadas para SL usando política](#)
- Notas de versão: [RN-9200](#), [RN-9300](#), [RN-9400](#), [RN-9500](#), [RN-9600](#)
- Guias de configuração: [Cat9200-CG](#), [Cat9300-CG](#), [Cat9400-CG](#), [Cat9500-CG](#), [Cat9600-CG](#)
- Referências de comando: [Cat9200-CR](#), [Cat9300-CR](#), [Cat9400-CR](#), [Cat9500-CR](#), [Cat9600-CR](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.