# Comprendre les licences Smart pour la commutation Catalyst

## Table des matières

# Introduction

Ce document décrit la fonction de gestion de licences Smart utilisant la politique sur les plates-formes de commutation Catalyst et le déploiement pris en charge.

# Objectif

À partir des versions 17.3.2 et 17.4.1 de la plate-forme Cisco IOS® XE, toutes les plates-formes de commutation Catalyst de la gamme pour Cat9k prennent en charge un nouveau modèle de licence SLP (Smart Licensing using Policy). L'objectif de ce document est de comprendre les différents modèles de mise en oeuvre et de déploiement de SLP pris en charge, principalement pour les déploiements de terrain vierge.

# Licence Smart utilisant la stratégie

Avec SLP, toutes les licences sont prêtes à l'emploi pour le périphérique. Les concepts précédents, le mode d'évaluation, l'enregistrement et la réservation disparaissent avec SLP. Avec SLP, il s'agit de rapporter les licences et leur utilisation. Les licences ne sont toujours pas appliquées et les niveaux de licence restent inchangés. Pour les plates-formes de commutateurs Catalyst, il n'existe pas de niveaux de licence contrôlés à l'exportation, à l'exception de la licence HSECK9. Le seul changement concerne l'infra de la notification de l'utilisation et du suivi des licences. Cette section décrit en détail les terminologies, les raisons des modifications, les nouveaux composants livrés avec SLP, CSLU (Cisco Smart Licensing Utility) et le flux de commande des produits.

## Terminologie

- CSSM ou SSM - Cisco Smart Software Manager
- SA - Compte Smart
- VA - Compte virtuel
- SL - Licences Smart
- PLR - Réservation de licence permanente
- SLR - Réservation de licence Smart
- PID - ID de produit
- SCH - Smart Call Home
- PI - Instances de produit
- CSLU - Utilitaire Cisco Smart Licensing
- RUM - Mesure de l'utilisation des ressources
- ACK - Accusé de réception
- UDI - Identification de périphérique unique - PID + SN
- SLP - Licence Smart utilisant la politique

## Pourquoi ce changement ?

Avec l'introduction du modèle de licence intelligente de trust and verify, Cisco a pris en charge divers mécanismes de

déploiement pour suivre et signaler l'utilisation des licences au CSSM. Cependant, elle n'était pas facilement adaptable à tous les types de déploiements : les commentaires et les exigences du terrain ont été exprimés pour rendre les licences Smart plus favorables à l'adoption. Voici quelques-uns des défis à relever :

- Avec l'enregistrement SL : les périphériques doivent toujours être connectés à Internet pour atteindre CSSM, ce qui constitue un problème de déploiement.
- Les serveurs satellite sur site augmentent les coûts de déploiement et de maintenance.
- Le reflex ne facilite que les réseaux à entrefer.
- Tous les déploiements qui ne prennent en charge aucun de ces modèles doivent exécuter leurs périphériques dans l'Unregistered/Eval expired état, même après l'achat des licences.

La procédure SLP est introduite pour faciliter diverses demandes de ce type depuis le terrain. Avec SLP, vous n'avez pas besoin d'enregistrer le produit auprès de CSSM. Tous les niveaux de licence achetés sont prêts à l'emploi dès leur livraison. Cela supprime la friction de jour 0 qui était présente sur le périphérique. SLP réduit également le workflow de mise en service des licences et réduit les points de contact excédentaires. Il n'est pas nécessaire que le périphérique soit connecté à CSSM 24 heures sur 24. SLP permet également d'utiliser des licences sur le réseau déconnecté, de signaler l'utilisation des licences hors ligne et de signaler les licences à des intervalles déterminés par les stratégies du client.

Licences disponibles

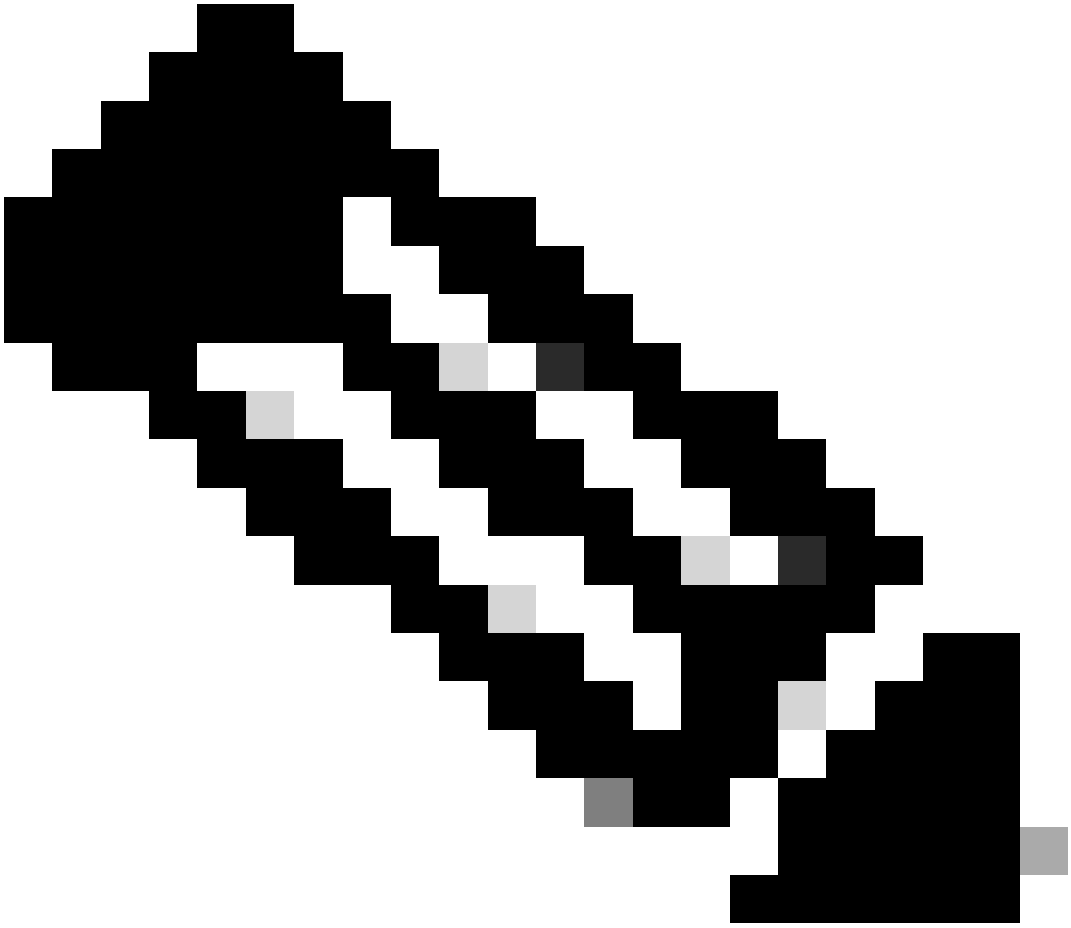
Les fonctionnalités logicielles disponibles sont incluses dans les niveaux de licence de base ou d'extension. Les licences de base sont des licences perpétuelles et les licences complémentaires sont disponibles pour trois, cinq et sept ans.

Licences de base

- Network Essentials
- Avantage du réseau
- HSECK9

Licences complémentaires

- DNA Essentials
- Avantage de l'ADN



**Remarque** : HSECK9 est une licence d'exportation contrôlée. Il nécessite une SLAC pour activer la licence et la fonctionnalité correspondante.

---

Les nouveaux composants

Policy (politique)

La stratégie détermine le comportement par défaut de l'interpréteur de protocole. Il indique les attributs des exigences de rapport de licence pour les différents niveaux et conditions de licence. La stratégie détermine également si le message ACK doit être renvoyé à l'IP, pour chaque rapport qui est envoyé à CSSM ou non. La stratégie contient également le nom de la stratégie et le moment où elle est installée. La politique par défaut de Cisco est commune et standard pour tous les produits Catalyst. Toutefois, la stratégie définie par le client est également autorisée si vous souhaitez avoir des intervalles de rapport différents et une omission de réponse ACK.

La stratégie peut être installée sur un PI à diverses occasions.

- Stratégie par défaut présente dans le logiciel
- Politique installée par le service de fabrication Cisco
- Stratégie installée via la réponse ACK
- Stratégie installée manuellement via CLI
- Stratégie diffusée à l'aide de la requête Yang

Ce résultat montre à quoi ressemble une stratégie par défaut.

```
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)
```

---

**Remarque** : une stratégie ne peut pas être effacée lorsque vous effacez/modifiez une configuration système, effacez la mémoire vive non volatile ou formatez la mémoire Flash : filesystem. La stratégie est définie sur Cisco par défaut, lors de la **réinitialisation de la** licence **Smart Factory**.

---

Rapports RUM

RUM est un rapport d'utilisation généré et stocké par l'interpréteur de protocole. Les rapports RUM standard ISO19770-4 sont complétés pour SLP. Les rapports RUM stockent toutes les modifications apportées à l'utilisation de la licence dans l'interface de programmation sous forme de fichiers de rapport. Les données d'utilisation de chaque niveau de licence sont stockées dans des rapports RUM distincts. Les mesures du rapport RUM sont recueillies et stockées dans PI à intervalles réguliers. Chaque fois qu'il y a un changement dans l'utilisation de la licence de l'IP ou qu'un rapport d'utilisation a été déclenché ou lorsque les rapports ont atteint la taille maximale/échantillons, de nouveaux rapports RUM pour

tous les niveaux de licence sont générés. Dans d'autres cas, les rapports RUM existants peuvent être remplacés par un nouvel échantillon et un horodatage mis à jour. La mesure par défaut de l'utilitaire de rapport RUM est toutes les 15 minutes. À chaque intervalle de rapport, les rapports RUM sont envoyés à Cisco CSSM.

Tous les rapports RUM sont signés par le PI et vérifiés par le CSSM. Lorsque CSSM reçoit les données du rapport RUM de PI, il valide le rapport, vérifie la chronologie de la modification de l'utilisation de la licence et met à jour les données CSSM en conséquence. CSSM accuse alors réception de l'IP via le message de réponse ACK.

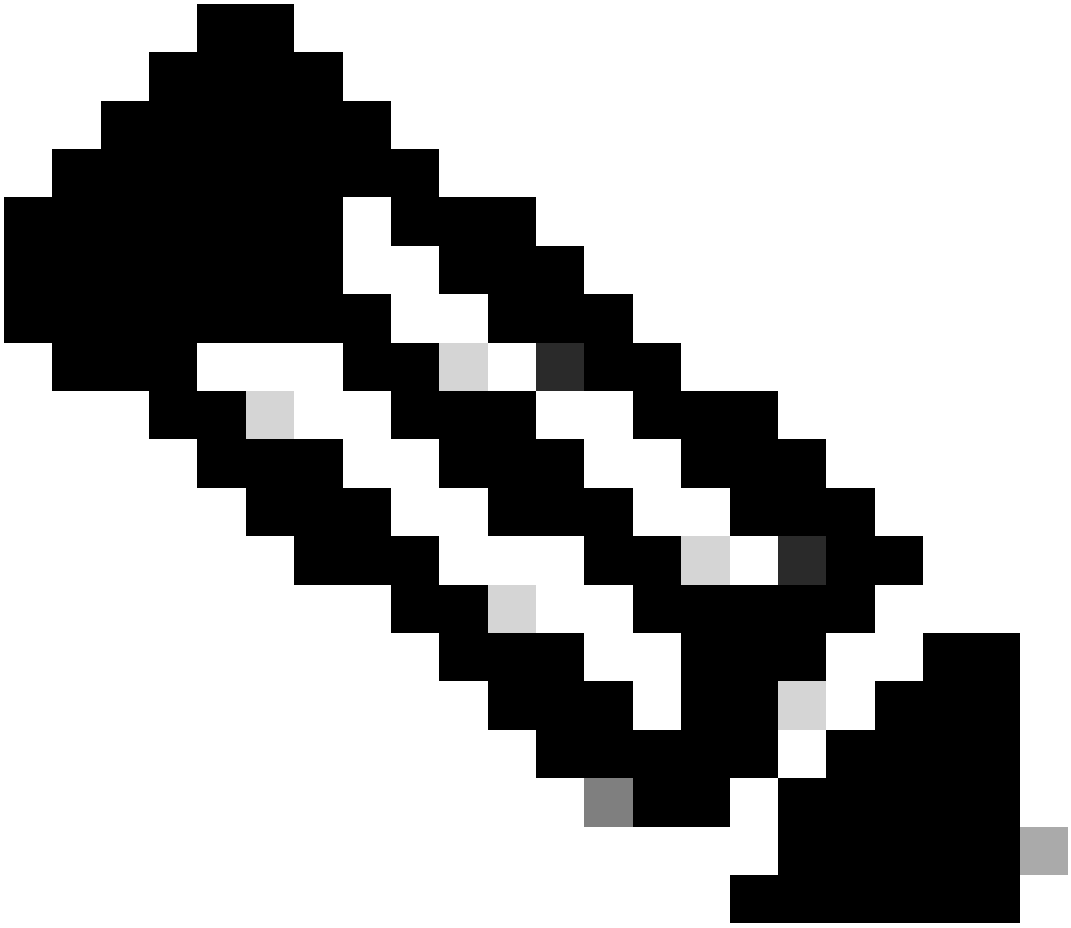
Les rapports RUM peuvent être envoyés à CSSM de plusieurs manières :

- PI envoie des rapports RUM à CSSM directement sur l'intervalle de rapport.
- PI envoie le rapport RUM à CSLU.
- CSLU extrait les rapports RUM de PI à intervalles réguliers via RESTAPI et les YANG modèles.
- Les rapports RUM sont enregistrés manuellement sur l'interface de programmation via l'interface de ligne de commande et téléchargés manuellement dans CSSM.

---

**Remarque** : les rapports RUM ne peuvent pas être effacés lorsque vous effacez/modifiez une configuration système, effacez la mémoire vive non volatile ou formatez la mémoire flash : filesystem. Tous les rapports RUM peuvent être supprimés de l'interface de programmation, sur « license smart factory reset ».

---



**Remarque** : l'intervalle de rapport par défaut est de 30 jours.

---

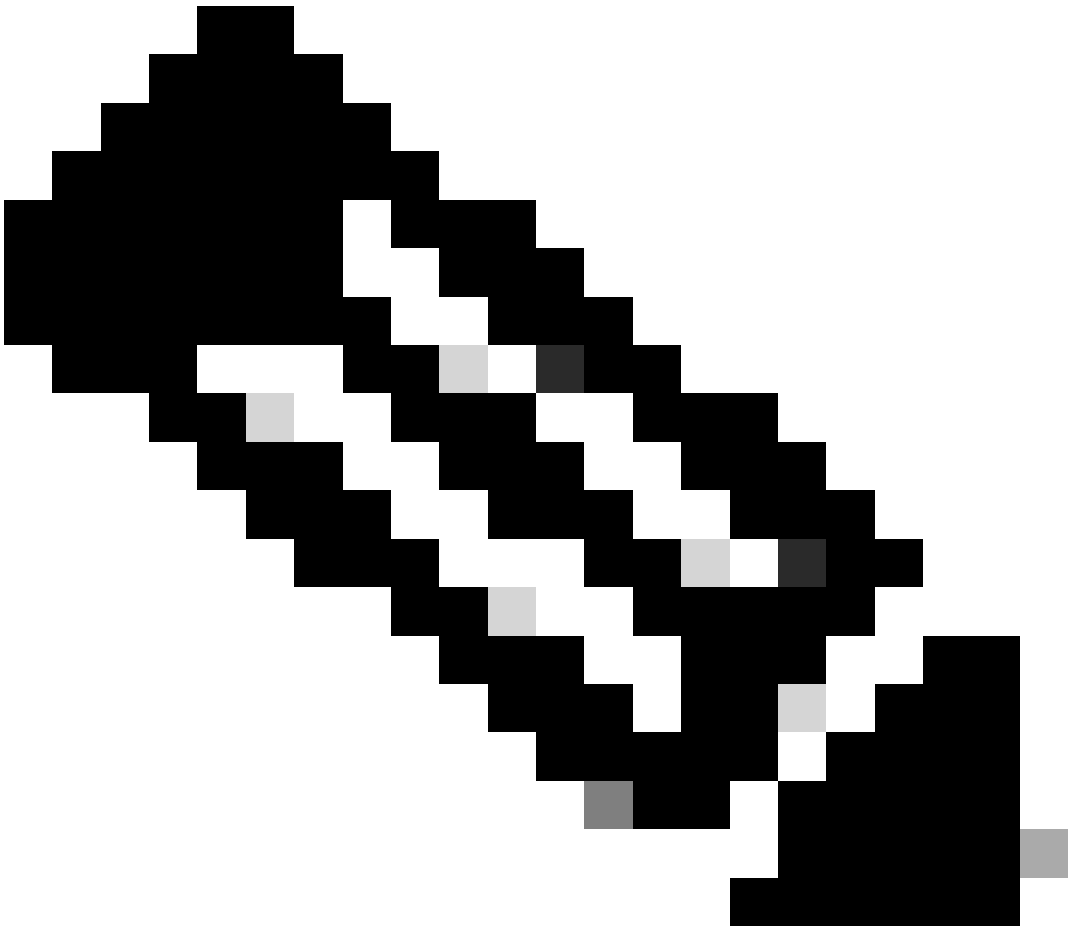
Flux de fabrication pour le cas de déploiement Greenfield

Une fois qu'une nouvelle commande de produit est passée dans Cisco CCW (Cisco Commerce Workspace), l'IP suit le flux des opérations effectuées par l'équipe de fabrication. Cela permet de faciliter le processus sécurisé de signature des rapports RUM et d'éliminer la friction du jour 0 dans l'enregistrement du PI. Une fois la commande passée, toute SA/VA existante ou nouvelle SA/VA créée est associée au produit. L'équipe de fabrication de Cisco s'occupe de ces opérations avant de vous expédier le produit :

- Installez le code de confiance sur le périphérique. La signature du code de confiance est installée en fonction de l'UDI du périphérique. Il est installé sur chaque produit.

- Install Purchase Code (Code d'achat d'installation) : informations sur les niveaux de licence achetés avec le produit. Il est installé sur chaque produit.
- SLAC - Smart License Auth Code - Non applicable aux plates-formes Catalyst.
- Installer la stratégie - Stratégie par défaut ou personnalisée en fonction de vos informations.
- Signalez l'utilisation de la licence à CSSM - SA/VA.

**Remarque** : avec la version 17.3.3, ce flux est suivi pour toutes les plates-formes de commutation Catalyst à l'exception de C9200/C9200L.

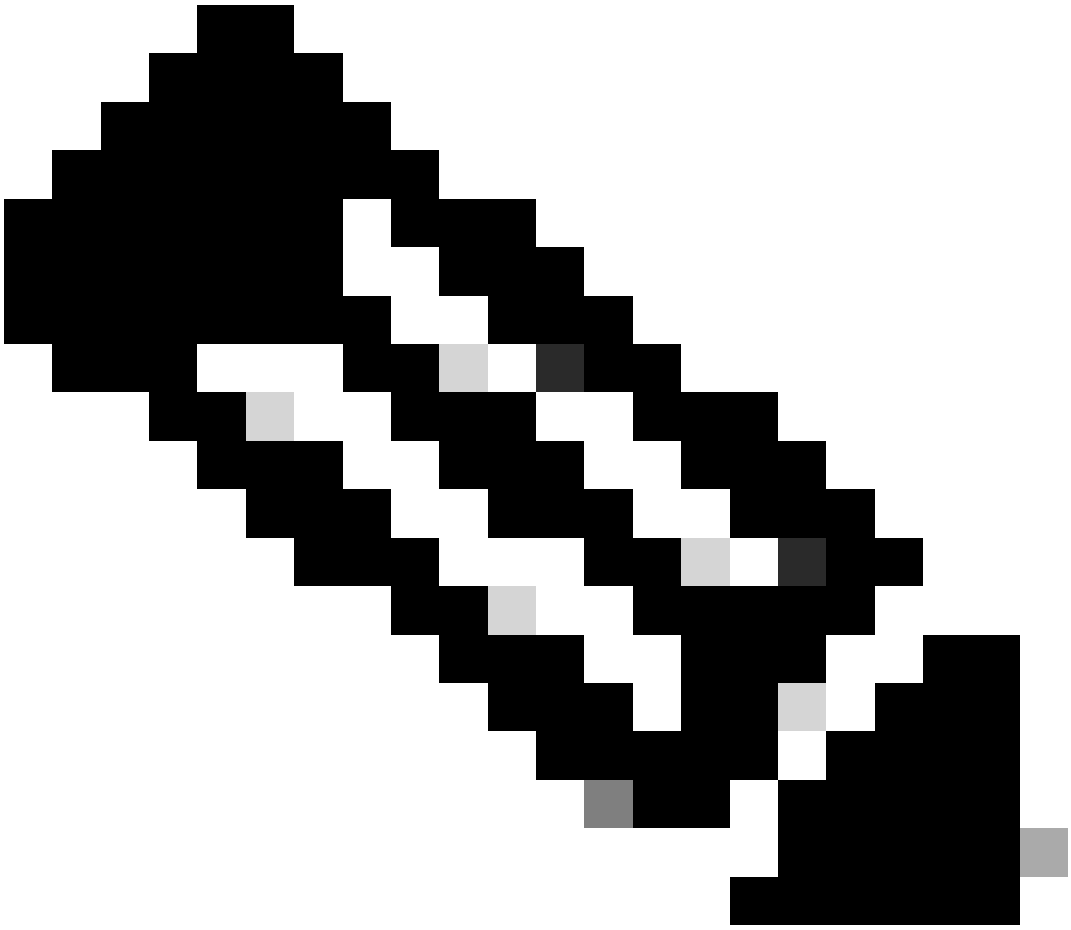


**Remarque** : le code de confiance est installé uniquement dans la fabrication avec la version 17.7.1 pour toutes les plates-formes de

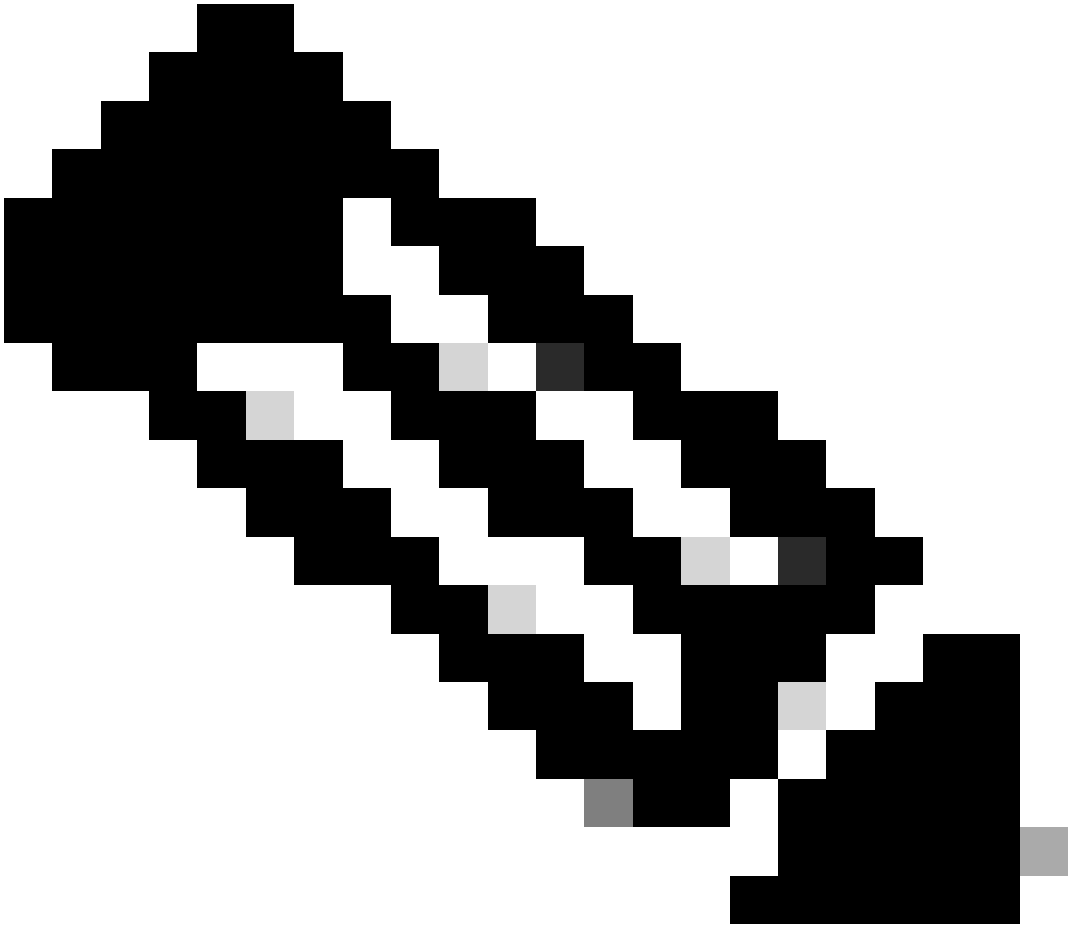
commutation Catalyst, à l'exception de C9200/C9200L.

CSLU

SLP introduit un nouvel outil CSLU simple mais puissant. CSLU est un outil basé sur une interface graphique utilisateur, qui fonctionne sur le système d'exploitation Windows 10 ou la version Linux basée sur RHEL/Debian. CSLU, qui peut être exécuté sur votre réseau privé local, est chargé de collecter les ports RUM à partir des PI associés à CSSM. CSLU doit être provisionné de manière à collecter des rapports RUM sur les IP du réseau local et à transmettre périodiquement le rapport RUM à CSSM via Internet. CSLU est un outil simple, qui affiche uniquement les détails des UDI des périphériques provisionnés. Toutes les données d'utilisation des licences pour les PI, les licences achetées et les licences inutilisées dans le pool sont affichées uniquement dans la SA/VA de CSSM, pour que vous puissiez vérifier. Elle est puissante car elle peut collecter des rapports d'utilisation de 10 000 IP maximum. CSLU est également chargé de repousser les messages ACK de CSSM vers PI.



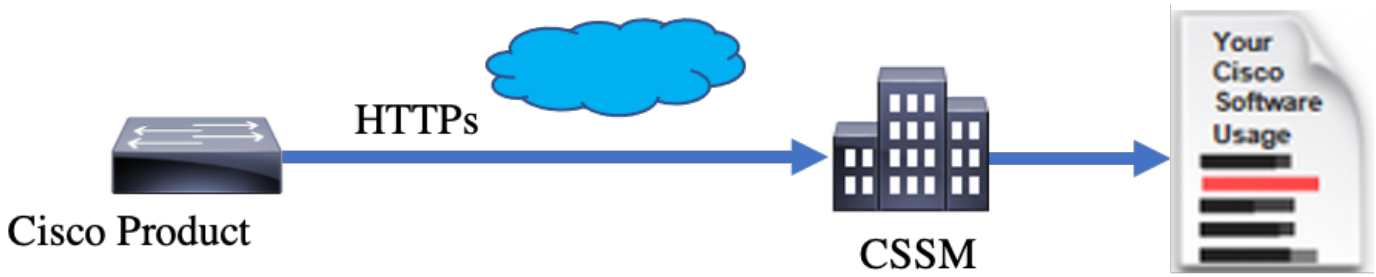
**Remarque** : reportez-vous à la section Topologie CSLU pour une configuration détaillée et les modes de fonctionnement pris en charge de CSLU.

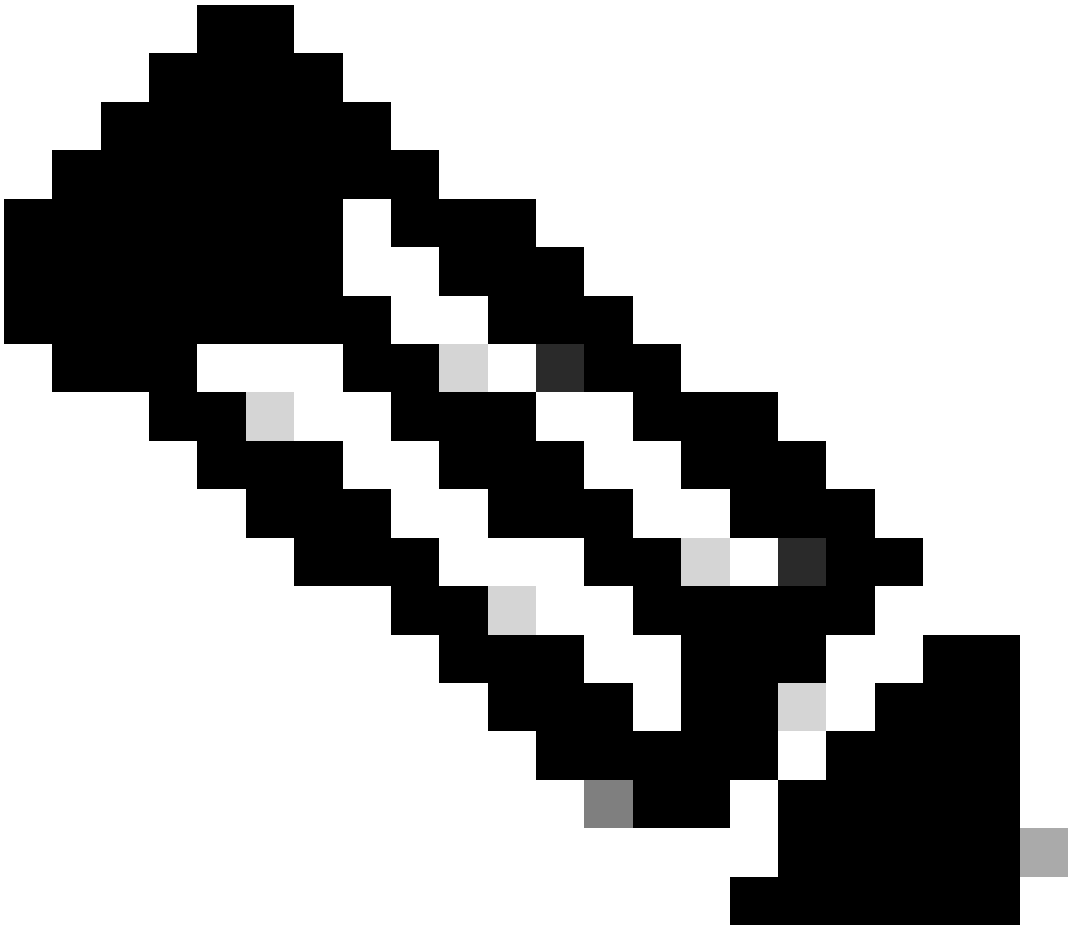


**Remarque** : la version Linux de CSLU est prise en charge à partir de la version 17.7.1.

SLP - Connexion directe

Sur un produit livré en usine, le mode de transport par défaut est CSLU. Si vous souhaitez utiliser la méthode de connexion directe, vous devez changer le mode de transport en Call-home ou SMART en fonction des besoins. La condition de base de la méthode de topologie de connexion directe est d'avoir une connectivité Internet pour l'accessibilité à CSSM. En outre, il faut s'assurer que pour la connectivité au CSSM, les configurations C3, DNS et de domaine requises sont présentes dans le périphérique.



**Remarque** : le transport intelligent est la méthode de transport recommandée lorsque vous vous connectez directement à CSSM.

Rapport de licence

Dans la topologie de connexion directe, les rapports RUM sont directement envoyés au CSSM. Les rapports de licence nécessitent l'installation d'un code de confiance sur le périphérique. Le code de confiance est installé par le fabricant Cisco sur le périphérique avant son expédition. Vous pouvez également installer un code de confiance sur le périphérique.

Le code de confiance est une chaîne de jeton extraite de CSSM, sur la page Compte virtuel - Général. Le code de confiance peut être installé via l'interface de ligne de commande.

Switch#license smart trust idtoken < > all/local

**Remarque** : toutes les options doivent être utilisées pour la haute disponibilité ou le système de rétrogradation. Pour un périphérique autonome, l'option locale peut être utilisée.

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

Une fois que le code de confiance est installé avec succès, l'IP peut signaler l'utilisation directement à CSSM. Ces conditions entraînent la déclaration des licences :

- Installation réussie du code de confiance
- À chaque intervalle de rapport par défaut
- Rechargement/démarrage sur le périphérique
- Un basculement
- Ajout ou suppression d'un membre de pile
- Déclenchement manuel de la synchronisation de licence

Les rapports de licence vers CSSM peuvent être déclenchés avec ces CLI :

Switch#license smart sync all

La section Rapports d'utilisation de l' show license status vous indique les délais du dernier accusé de réception reçu, la date d'échéance du prochain accusé de réception, la diffusion suivante du rapport et la diffusion précédente du rapport.

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>

Connexion directe - Smart Transport

Dans une topologie en mode de connexion directe ou d'accès direct au cloud, si SMART Transport est utilisé, il s'agit des configurations requises sur le périphérique.

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
!

Connexion directe - Transport Call-Home

Dans une topologie en mode de connexion directe ou d'accès direct au cloud, si le transport Call-home est utilisé, il s'agit des configurations requises sur le périphérique.

Configure the desired Transport mode using below CLI.

Switch(config)#license smart transport callhome

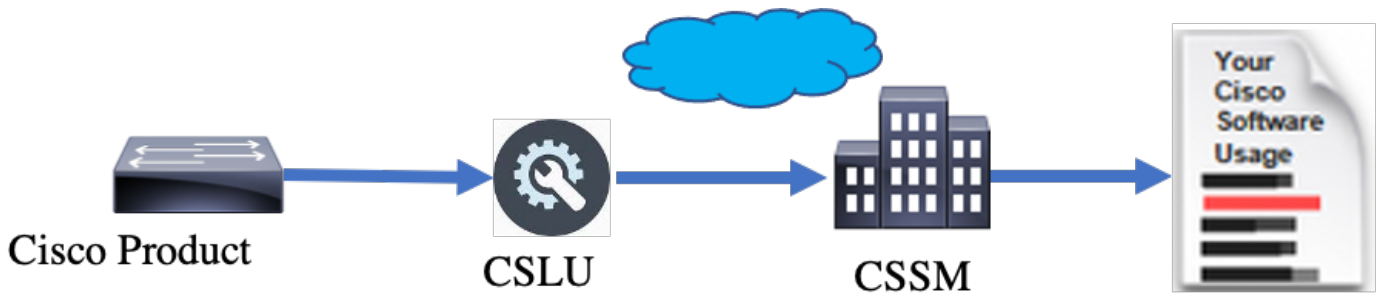
Running config on Smart Transport Mode:

```
!
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
!
```

**Remarque** : par défaut, l'adresse de destination de Call-home est configurée sur l'URL CSSM. Cela peut être vérifié dans la show run all configuration.

SLP - CSLU

Le mode CSLU est le mode de transport par défaut sur les périphériques livrés en usine qui exécutent 17.3.2 ou version ultérieure. En outre, si vous migrez à partir de licences d'évaluation/d'évaluation expirées, le mode de transport après le passage à SLP est CSLU. Dans une topologie CSLU, le CSLU se trouve entre le PI et le CSSM. CSLU évite aux utilisateurs de ne pas disposer d'une connectivité réseau directe au cloud Cisco - CSSM. CSLU peut s'exécuter localement sur un réseau privé et télécharger des rapports d'utilisation à partir de tous les PI associés. Les rapports d'utilisation sont enregistrés localement sur le PC Windows avant d'être envoyés au CSSM via Internet. CSLU est un outil léger. Vous ne pouvez voir que la liste des IP qui lui sont associées et elle peut être identifiée avec l'utilisation d'UDI. CSLU ne peut pas afficher ou contenir les informations de redondance de PI, de niveaux de licence ou d'utilisation de licence.

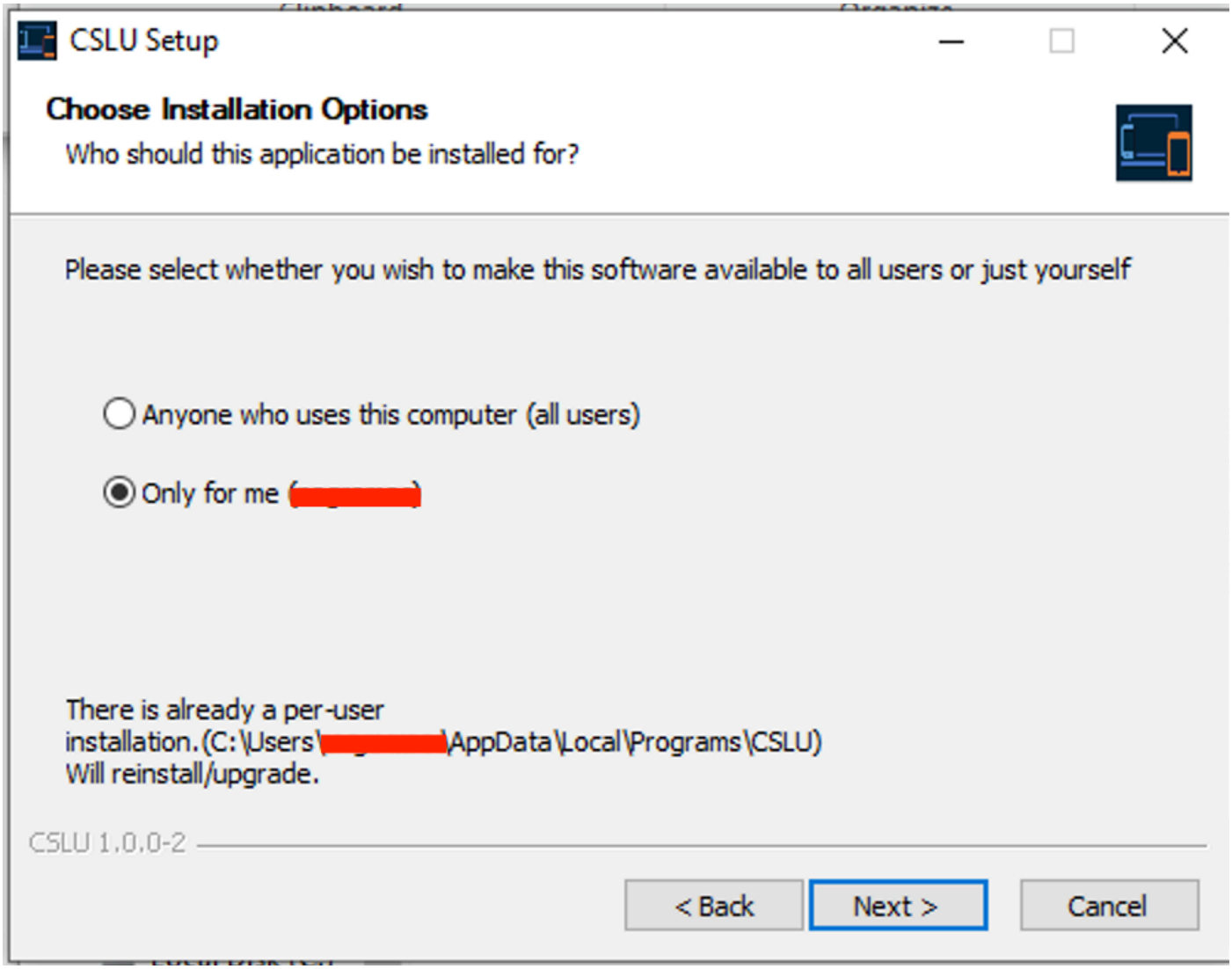



Installation et configuration de CSLU

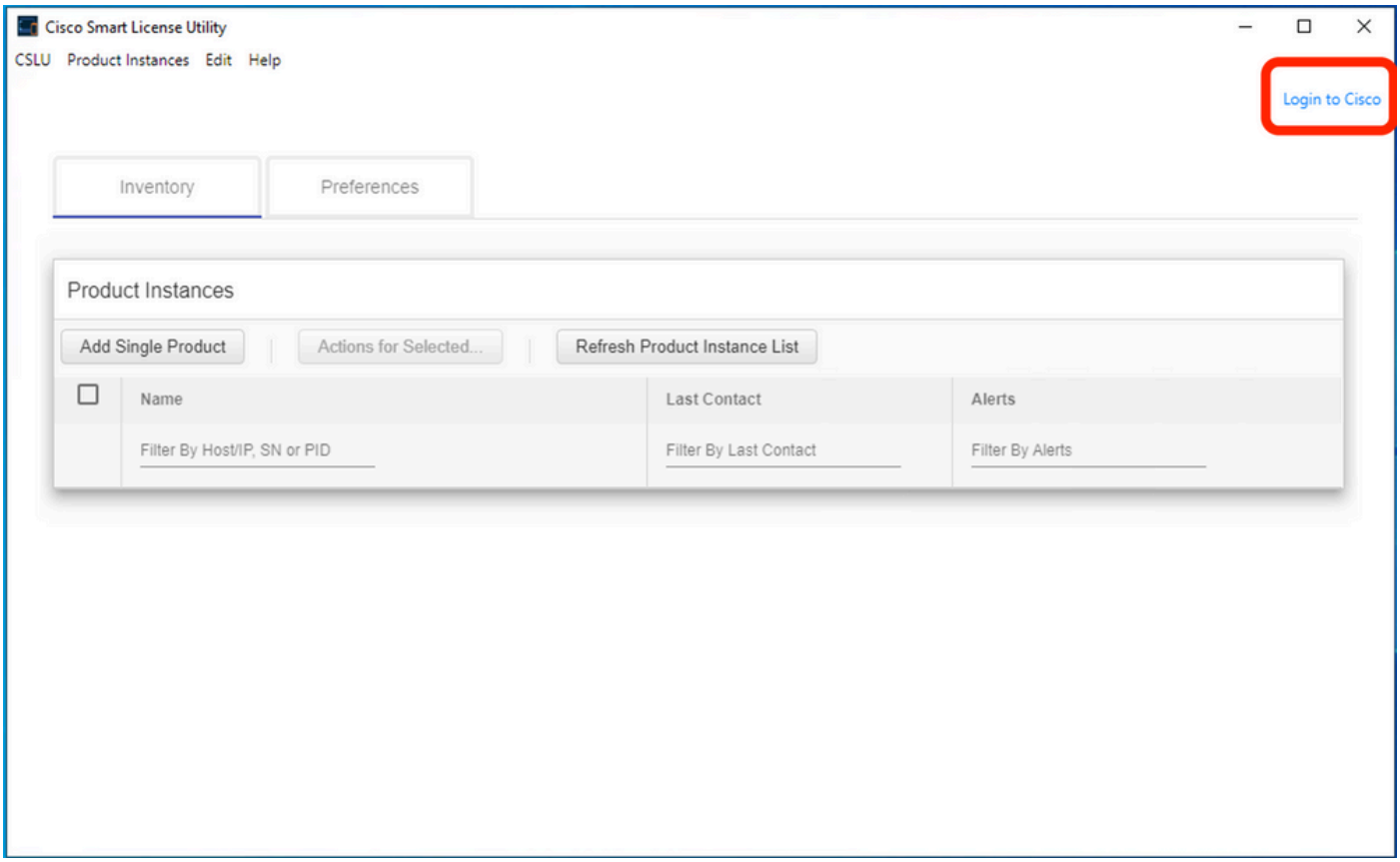
L'outil CSLU est installé et utilisé sur les machines Windows 10. Le logiciel est disponible dans le CCO pour téléchargement et pour une utilisation gratuite. Une fois l'outil installé, le Guide de démarrage rapide/Manuel de l'utilisateur peut être téléchargé à partir du menu Aide, accédez à Help > Download Help Manual.

L'installation de CSLU nécessite que vous acceptiez le contrat de licence.

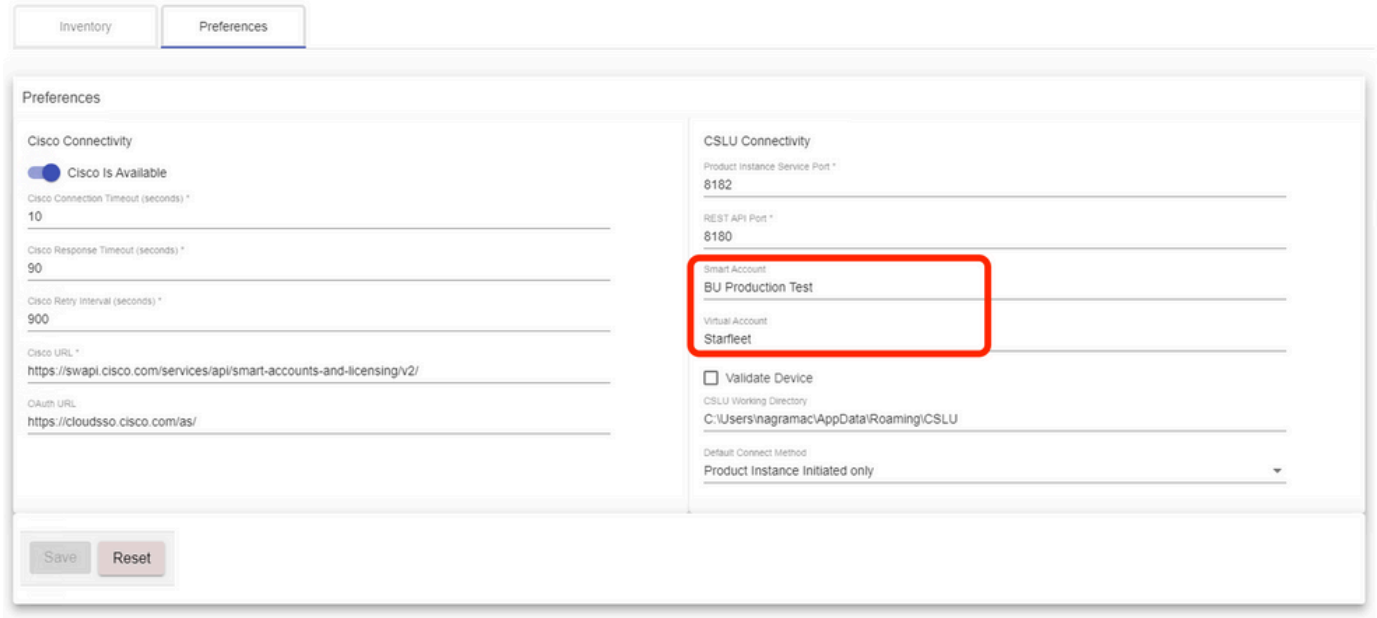
Il est recommandé d'installer l'application uniquement pour l'utilisateur actuel et non pour tous les utilisateurs qui travaillent sur l'ordinateur. Si une version antérieure de CSLU est déjà présente sur le PC, il est recommandé de la désinstaller au préalable. Néanmoins, la nouvelle installation prend soin de mettre à niveau le logiciel.




Après l'installation, connectez-vous à Cisco, en utilisant l'option de connexion présente dans le coin supérieur droit de l'application. Ceci utilise vos identifiants CEC. Et par connexion, la confiance est établie entre CSLU et CSSM.




Après vous être connecté à Cisco, assurez-vous que les détails SA et VA sont sélectionnés correctement dans le menu déroulant, dans le volet Préférences de l'outil. Veillez à enregistrer les configurations.



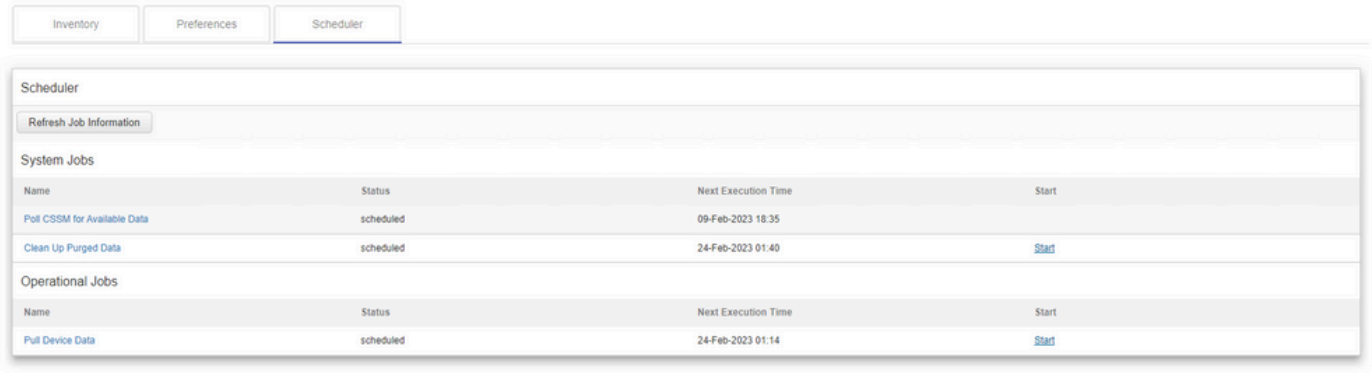

Onglet Schedule sur CSLU - L'onglet Schedule sur CSLU vous permet de configurer les éléments suivants :

- Sondage du CSSM pour les données disponibles : affiche les horaires des tâches, l'heure de la dernière extraction et l'heure de la prochaine extraction des données du CSSM.

- Nettoyer les données purgées : supprime toutes les données purgées du datastore CSLU. Il peut également être déclenché

manuellement.

- Données du périphérique d'extraction : active le mode d'extraction CSLU.




CSLU utilisant le mode PUSH

CSLU fonctionne par défaut en mode PUSH. En mode PUSH, l'interpréteur de protocole envoie les rapports d'utilisation à CSLU à intervalles réguliers. À partir du périphérique, vous devez vous assurer que l'accessibilité du réseau de couche 3 vers CSLU est disponible. Pour que l'IP puisse parler à CSLU, l'adresse IP de l'ordinateur Windows qui exécute CSLU doit être configurée.

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>

Les rapports sont envoyés à CSLU par PI dans les conditions suivantes :

- À chaque intervalle de rapport par défaut
- Rechargement/démarrage sur le périphérique
- Sur la commutation
- Ajout ou suppression de membres de la pile
- Déclenchement manuel de la synchronisation de licence

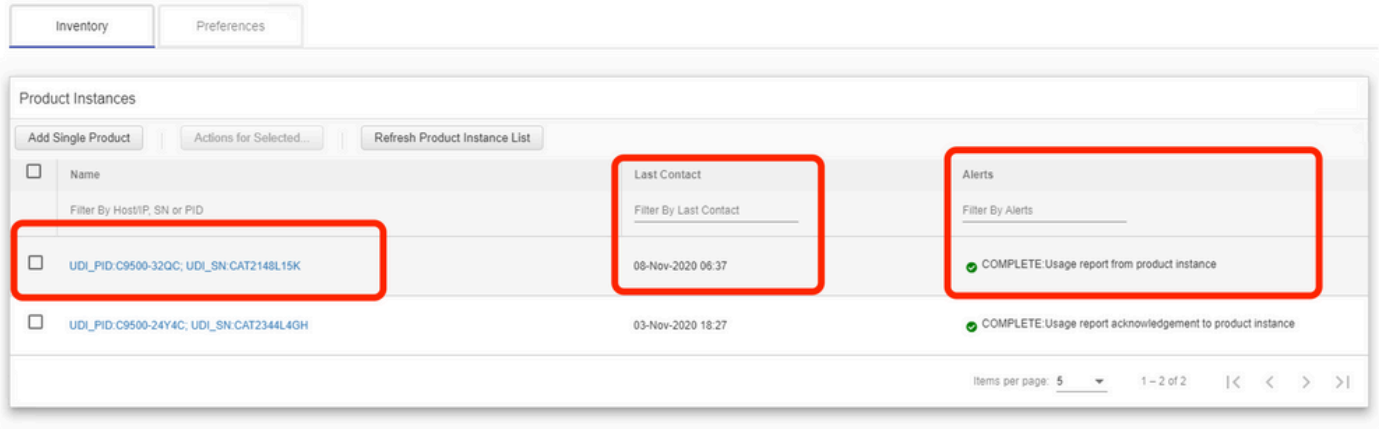
Dans CSLU, la page d'inventaire répertorie les périphériques actuellement associés à CSLU. Les périphériques de la liste peuvent être identifiés via l'UDI. Les périphériques peuvent être filtrés en fonction du PID ou du SN de la liste pour identifier un périphérique particulier.

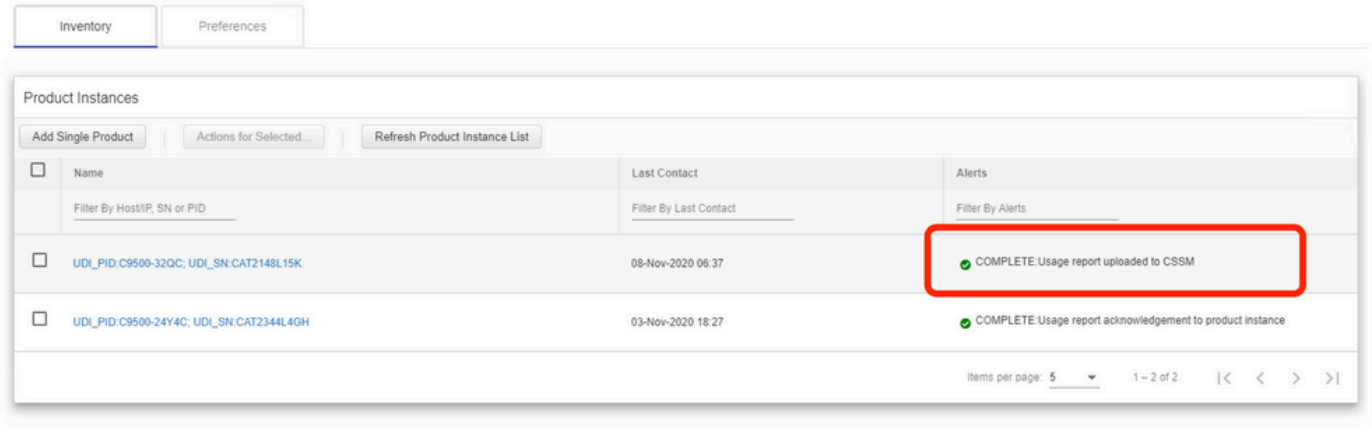
La page d'inventaire CSLU comporte également deux autres colonnes :

- La colonne **Dernier contact** - Affiche l'horodatage le plus récent lorsque l'état du rapport a changé.

- **Colonne Alerte** - Affiche le dernier état de rapport de l'IP.

Une fois que le PI envoie le rapport à CSLU, CSLU crée l'entrée PI dans CSSM. L'état Dernier contact TS ainsi que l'état Alertes sont mis à jour.




CSSM traite les rapports envoyés par CSLU et ajoute/met à jour l'instance de produit sur CSSM, en fonction de l'utilisation de la licence. Une fois que le CSSM traite et met à jour la date, il renvoie le message ACK à CSLU. CSLU à son tour stocke et réachemine le message à PI.

Le message ACK se compose des éléments suivants :

- Accusé de réception pour tous les rapports envoyés
- Policy (politique)
- Code de confiance

Si une nouvelle stratégie est disponible pour vous dans le CSSM, elle est désormais également mise à jour vers le PI. Si la politique est inchangée, la même chose est transmise à PI.

**Remarque** : si le signalement des messages ACK n'est pas requis conformément à votre stratégie, le message ACK n'est pas envoyé.

La colonne de message d'alerte peut avoir l'un des états suivants :

- Rapport d'utilisation de l'instance de produit
- Rapport d'utilisation téléchargé vers Cisco
- Demande de synchronisation depuis une instance de produit
- Demande de synchronisation téléchargée vers CSSM
- Accusé de réception reçu de CSSM
- Accusé de réception du rapport d'utilisation à l'instance de produit

---

**Remarque** : dans CSLU sur un système haute disponibilité, l'entrée est toujours visible uniquement pour l'UDI de l'actif. Seul CSSM possède tous les UDI pour les périphériques individuels du système répertoriés.

---

Détection automatique CSLU

Pour prendre en charge des déploiements évolutifs avec des configurations minimales, la détection automatique de CSLU est prise en charge. Cela signifie que vous n'avez pas à configurer l'adresse IP/URL de CSLU spécifiquement. Pour ce faire, il vous suffit d'ajouter une entrée à leur serveur DNS. Cela permet au périphérique, qui a le mode de transport CSLU (qui est le mode par défaut), de détecter automatiquement CSLU et d'envoyer des rapports.

Voici quelques points à prendre en compte :

- Créez une entrée dans le serveur DNS. L'adresse IP de la CSLU doit être mappée au nom cslu-local.
- Assurez-vous que le serveur de noms et les configurations DNS sont présents dans le périphérique pour l'accessibilité.

Ainsi, sans configuration supplémentaire, les périphériques du réseau peuvent atteindre CSLU et envoyer des rapports RUM à intervalles réguliers.

CSLU utilisant le mode PULL

Le mode PULL est l'endroit où l'unité CSLU lance le processus de récupération des rapports RUM à partir des périphériques. Ici, les détails du périphérique sont ajoutés au CSLU et le CSLU récupère les données sur tous les périphériques ajoutés à intervalles réguliers. L'appel de CSLU peut également être déclenché manuellement. CSLU envoie à son tour le rapport RUM à CSSM, et les messages ACK qui sont reçus en retour de CSSM sont envoyés à l'IP. Le mode PULL est pris en charge par trois moyens différents : RESTAPI, NETCONF, et RESTCONF.

Mode PULL avec RESTAPI

Pour que le mode PULL fonctionne correctementRESTAPI, les configurations requises du périphérique et de CSLU sont les suivantes :

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
!
```

---

**Remarque** : l'utilisateur doit disposer d'un accès de niveau Priv 15.

---

CSLU - Procédure de configuration

CSLU doit être connecté à CSSM pour que les rapports soient synchronisés automatiquement.

Étape 1. Sélectionnez Add Single Product sur la page d'inventaire.

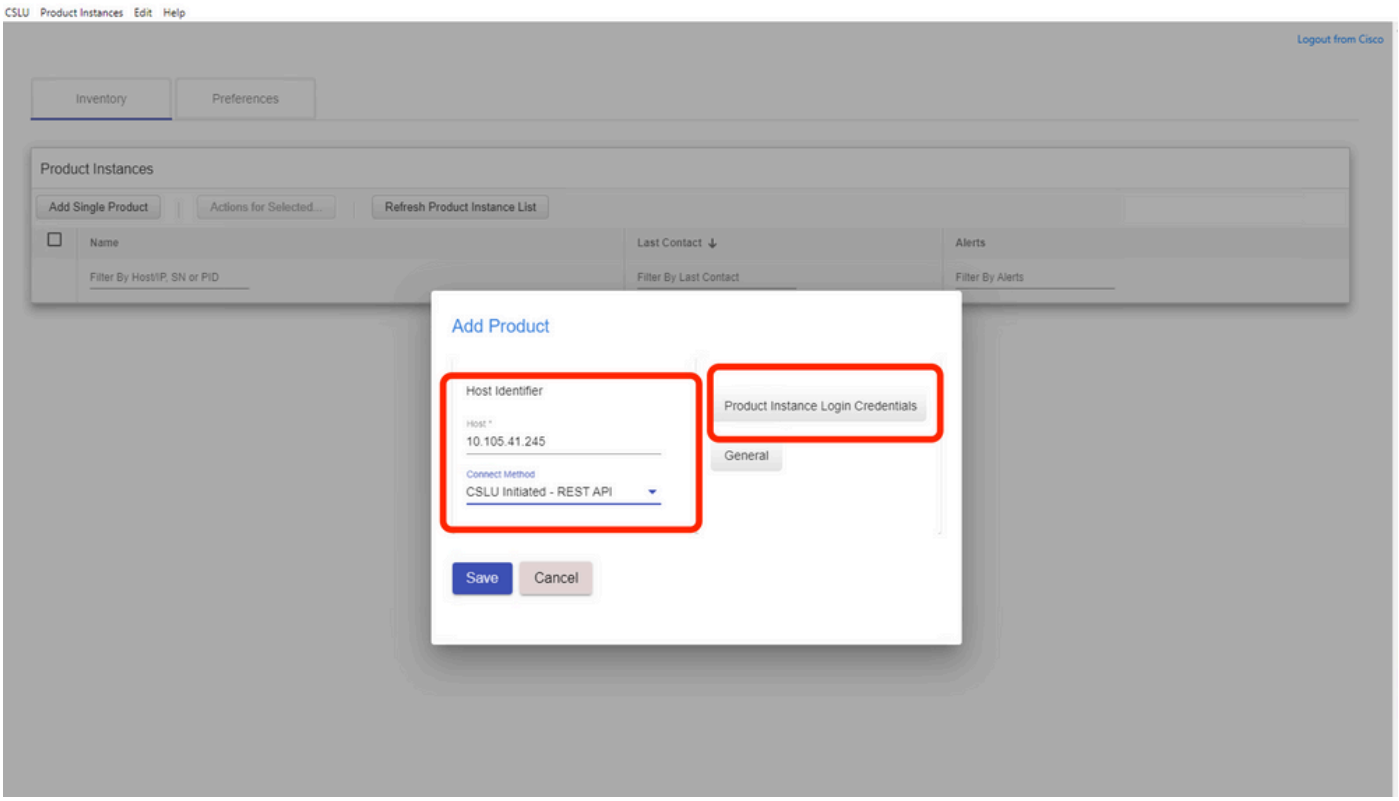
Étape 2. Saisissez l'adresse IP du périphérique.

Étape 3. Sélectionnez la méthode de connexion RestAPI.

Étape 4. Sélectionnez Informations de connexion de l'instance de produit.

Étape 5. Saisissez les informations d'identification de l'utilisateur disposant de l'accès Priv 15.

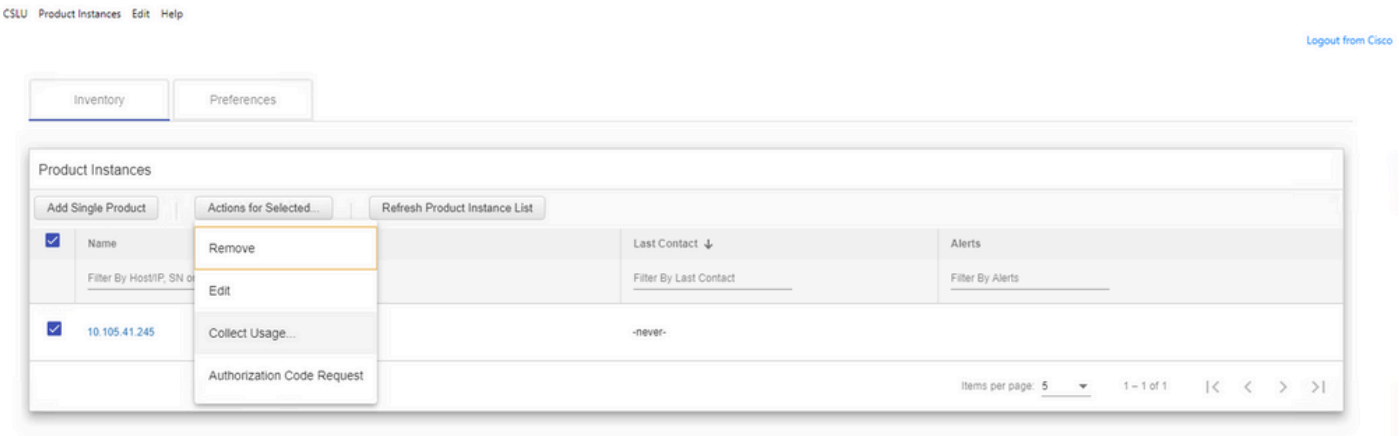
Étape 6. Enregistrez les configurations.

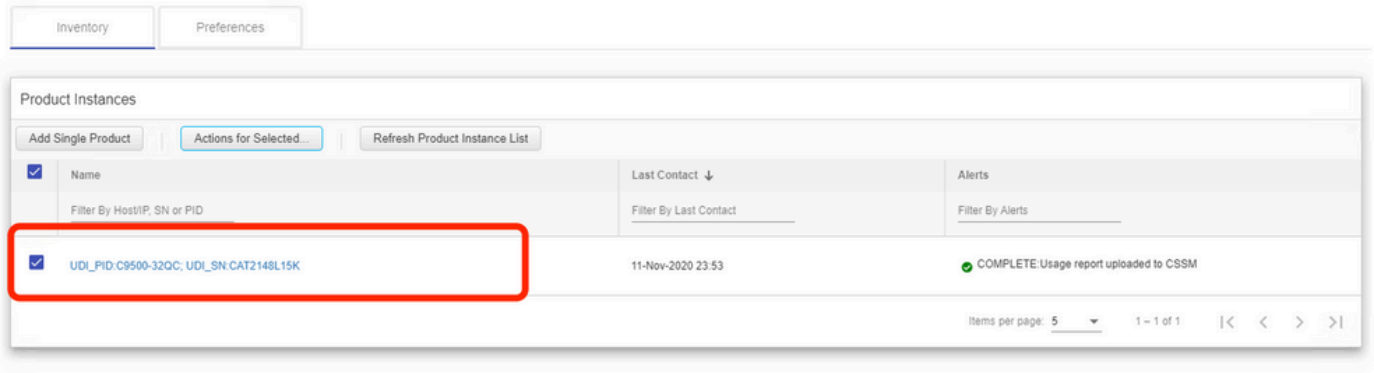



Le périphérique est ajouté avec une seule adresse IP dans le champ Nom.

Sélectionnez le périphérique et accédez à Actions for Selected > Collect Usage.

Une fois que les données d'utilisation ont été collectées avec succès, le champ Nom est mis à jour avec l'UDI de l'IP et l'horodatage est également mis à jour. Le champ d'alerte reflète le dernier état.






Si le périphérique est toujours disponible lorsque le message ACK est reçu de CSSM, l'ACK est renvoyé à PI. Sinon, ACK est envoyé au prochain intervalle d'extraction.

Mode PULL avec RESTCONF

Pour que le mode PULL fonctionne via RESTCONF , les configurations requises du périphérique et les étapes de CSLU sont les suivantes :

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
!
```

**Remarque** : ces configurations sont destinées à l'authentification locale. L'authentification à distance peut également être utilisée.

CSLU - Procédure de configuration

CSLU doit être connecté à CSSM pour que les rapports soient synchronisés automatiquement. La configuration CSLU est identique à celle de la collecte et de la génération de rapportsRESTAPI RUM.

Étape 1. Sélectionnez Add Single Product sur la page d'inventaire.

Étape 2. Saisissez l'adresse IP du périphérique.

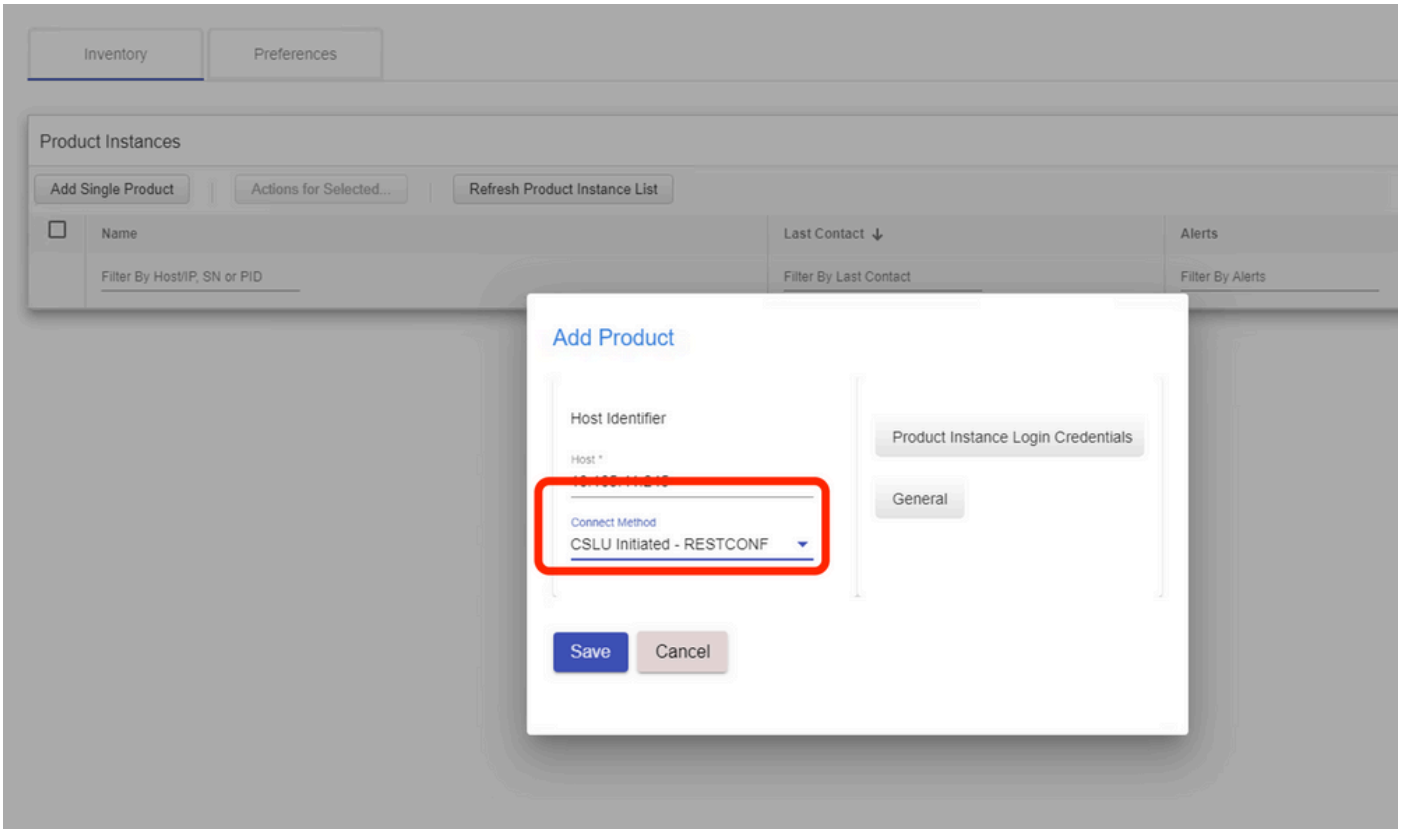
Étape 3. Sélectionnez la méthode de connexion RESTCONF.

Étape 4. Sélectionnez Informations de connexion de l'instance de produit.

Étape 5. Saisissez les informations d'identification de l'utilisateur disposant de l'accès Priv 15.

Étape 6. Enregistrez les configurations.

Étape 7. Collecter les données d'utilisation du périphérique sélectionné.




Mode PULL avec NETCONF

Pour que le mode PULL fonctionne correctementNETCONF, les configurations requises du périphérique et les étapes de CSLU sont les suivantes :

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

**Remarque** : ces configurations sont destinées à l'authentification locale. L'authentification à distance peut également être utilisée.

CSLU - Procédure de configuration

CSLU doit être connecté à CSSM pour que les rapports soient synchronisés automatiquement. La configuration CSLU est identique à celle de la collecte et de la génération de rapportsRESTAPI RUM.

Étape 1. Sélectionnez Add Single Product sur la page d'inventaire.

Étape 2. Saisissez l'adresse IP du périphérique.

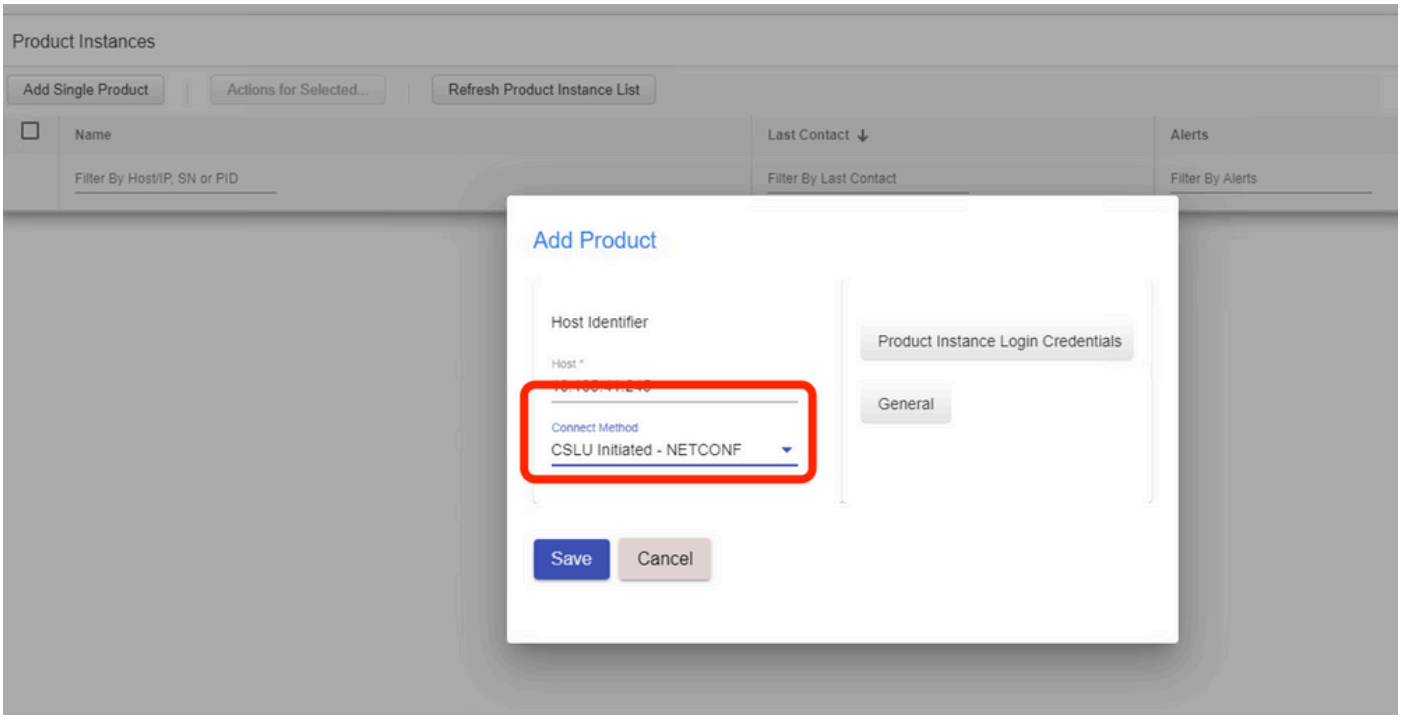
Étape 3. Sélectionnez la méthode de connexion NETCONF.

Étape 4. Sélectionnez Informations de connexion de l'instance de produit.

Étape 5. Saisissez les informations d'identification de l'utilisateur disposant de l'accès Priv 15.

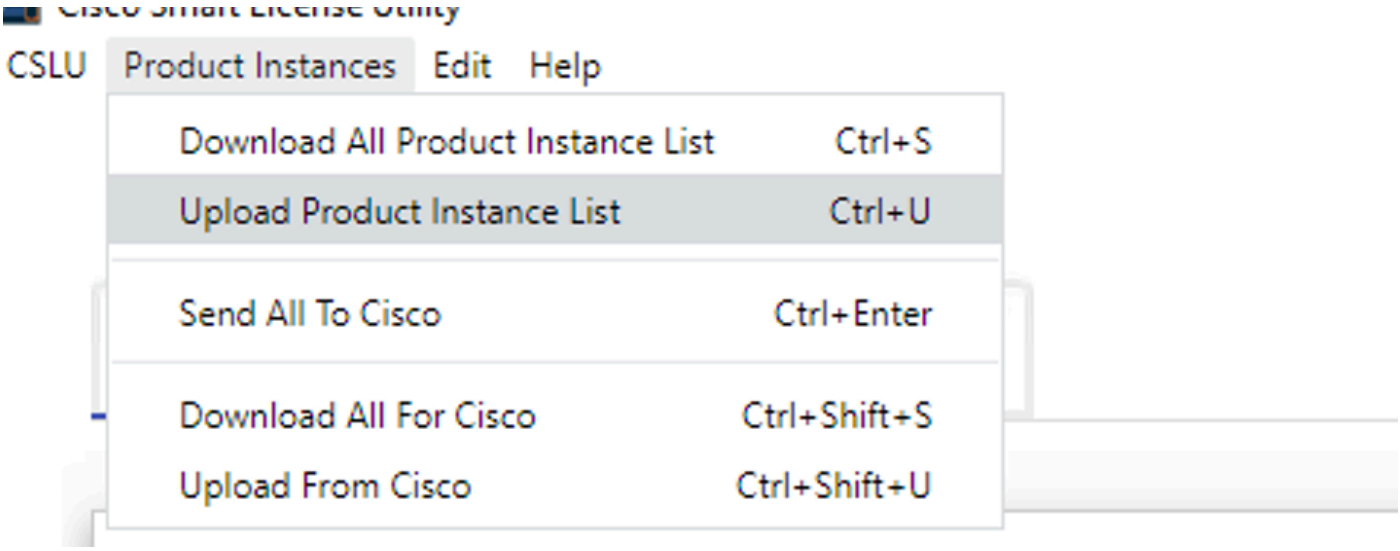
Étape 6. Enregistrez les configurations.

Étape 7. Collecter les données d'utilisation du périphérique sélectionné.

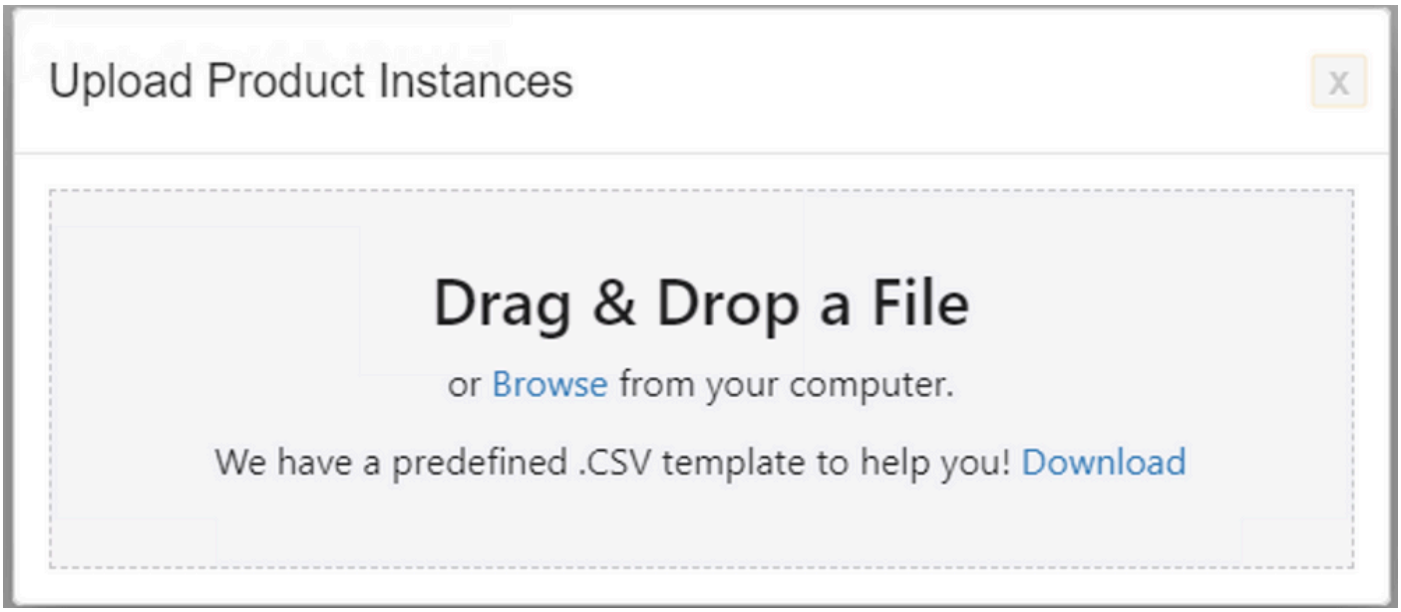



**Remarque** : pour tous les modèlesNETCONF, RESTCONF et RESTAPI, la liste des périphériques peut être ajoutée en bloc.

Afin d'effectuer le téléchargement en masse, sur la barre,Menu naviguez jusqu'à Product Instance > Upload Product Instance List, comme illustré dans cette image.




Une nouvelle fenêtre contextuelle s'ouvre. Le fichier modèle peut être téléchargé à partir de celui-ci. Dans le fichier au format CSV, renseignez les détails de périphérique de la liste des périphériques et téléchargez vers CSLU pour ajouter plusieurs périphériques.




**Remarque** : pour tous les types de mode CSLU PULL, il est recommandé de définir le mode de transport sur Off sur le PI. Cela peut être fait à l'aide de l'interface de ligne de commande.

Switch(config)#license smart transport off

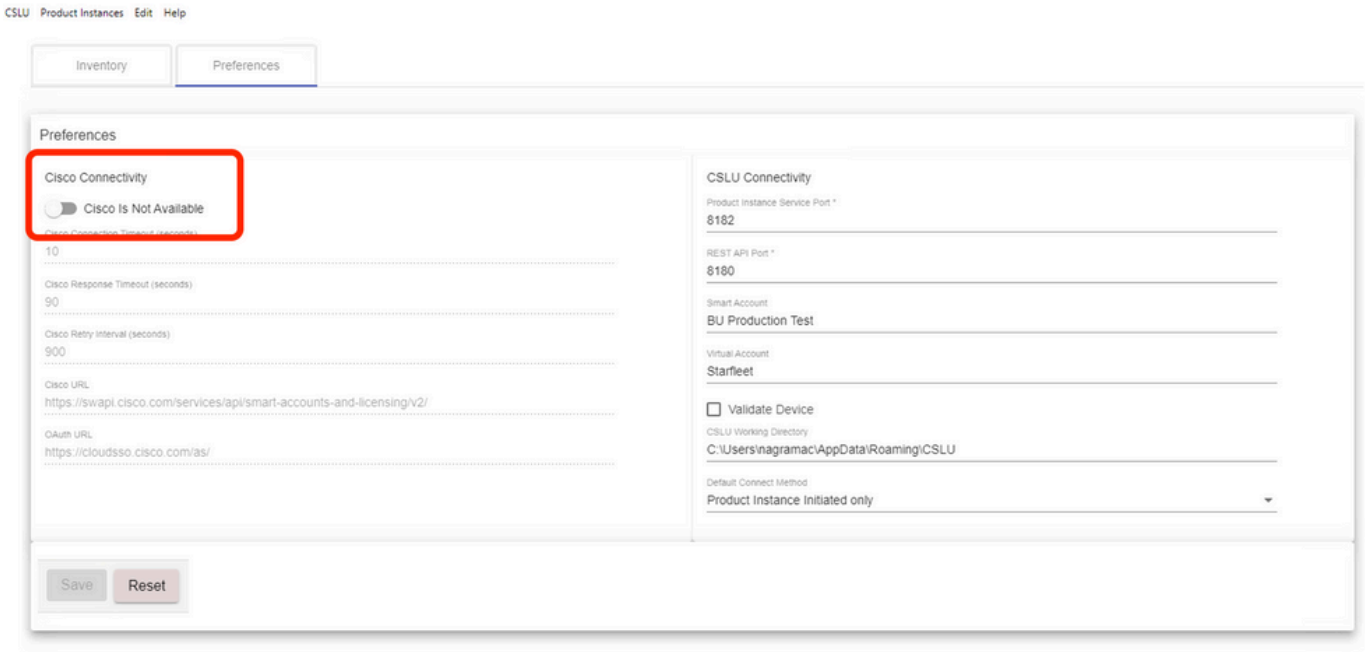
CSLU utilisant le mode déconnecté

CSLU peut fonctionner en mode déconnecté à partir de CSSM. Ceci s'applique à tous les déploiements qui ne permettent pas à l'unité CSLU d'être connectée à Internet. En mode déconnecté, les rapports de tous les périphériques sont téléchargés manuellement à partir de CSLU et

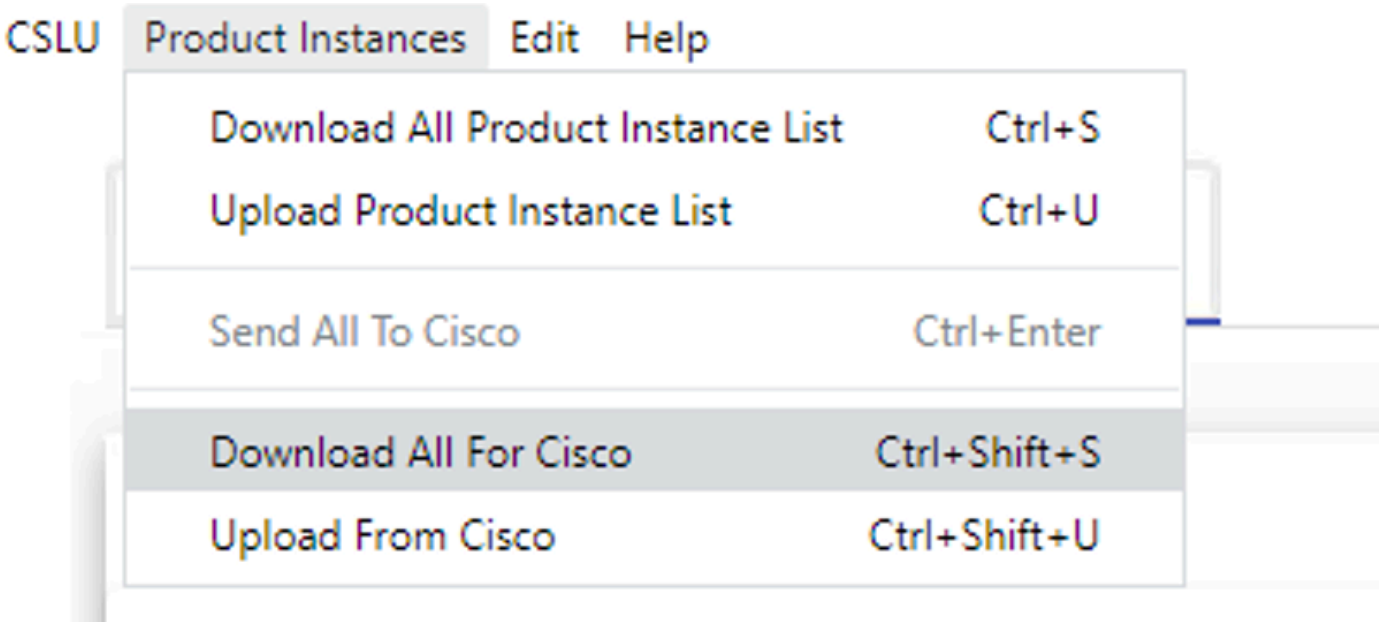
téléchargés vers CSSM. À leur tour, les messages ACK sont téléchargés depuis CSSM et téléchargés vers CSLU. CSLU continue d'extraire/envoyer les dates d'utilisation des PI et renvoie également le message ACK à PI.

Étape 1. Sur la pageCSLU Preference, désactivez l'option Cisco Connectivity. Cela confirme que Cisco n'est pas disponible.

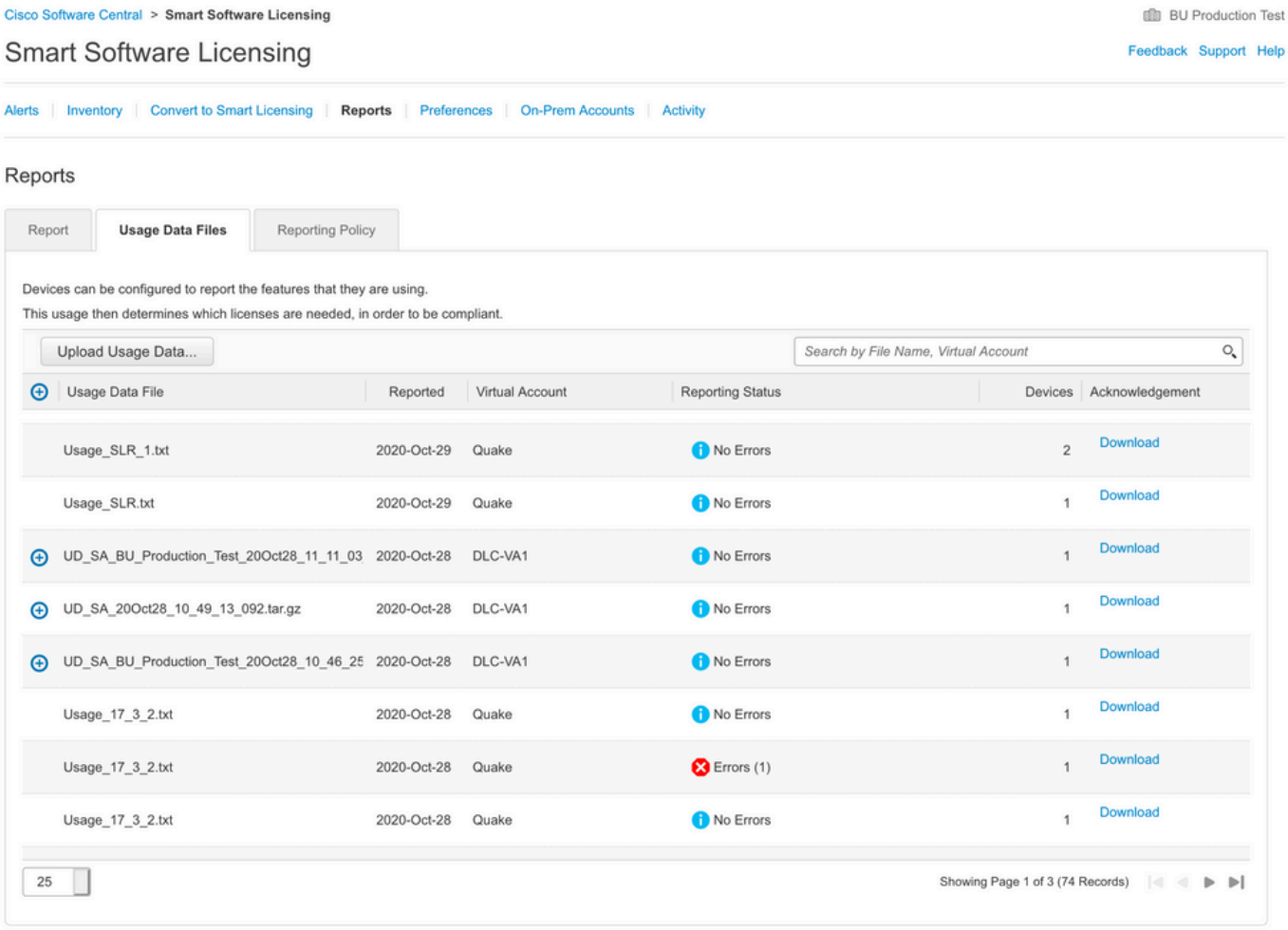
Étape 2. Enregistrez les paramètres.

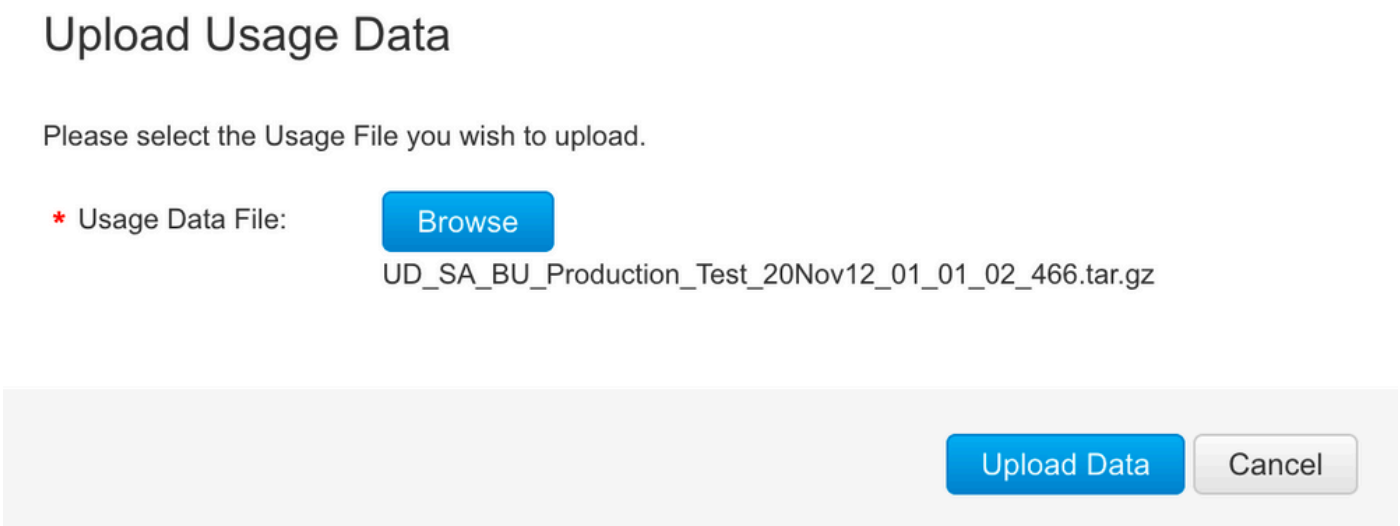



Étape 3. Dans la barre,Menu cliquez sur Product Instances > Download All for Cisco. Cette opération télécharge un fichiertar.gz sur le CSLU.

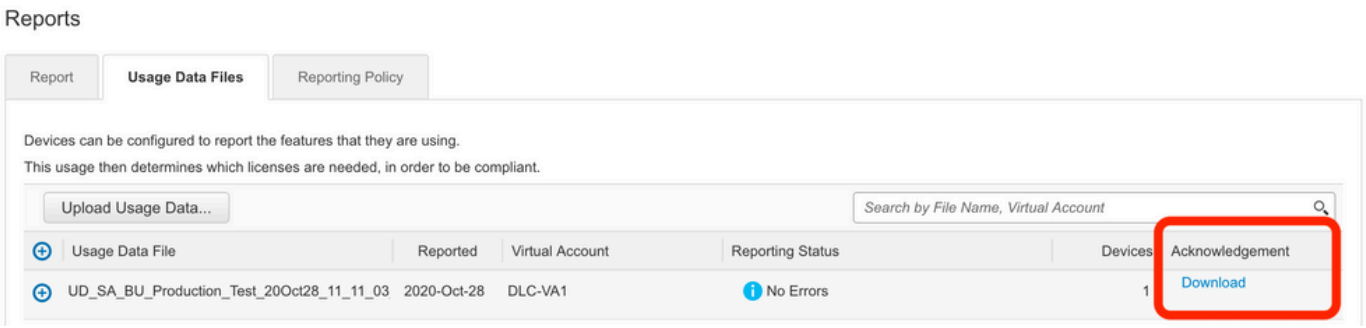



Étape 4. Téléchargez le fichier sur CSSM. Dans la page Compte Smart CSSM, accédez à Report > Usage Data Files > Upload usage data. Dans la fenêtre contextuelle, téléchargez le fichiertar.gz.

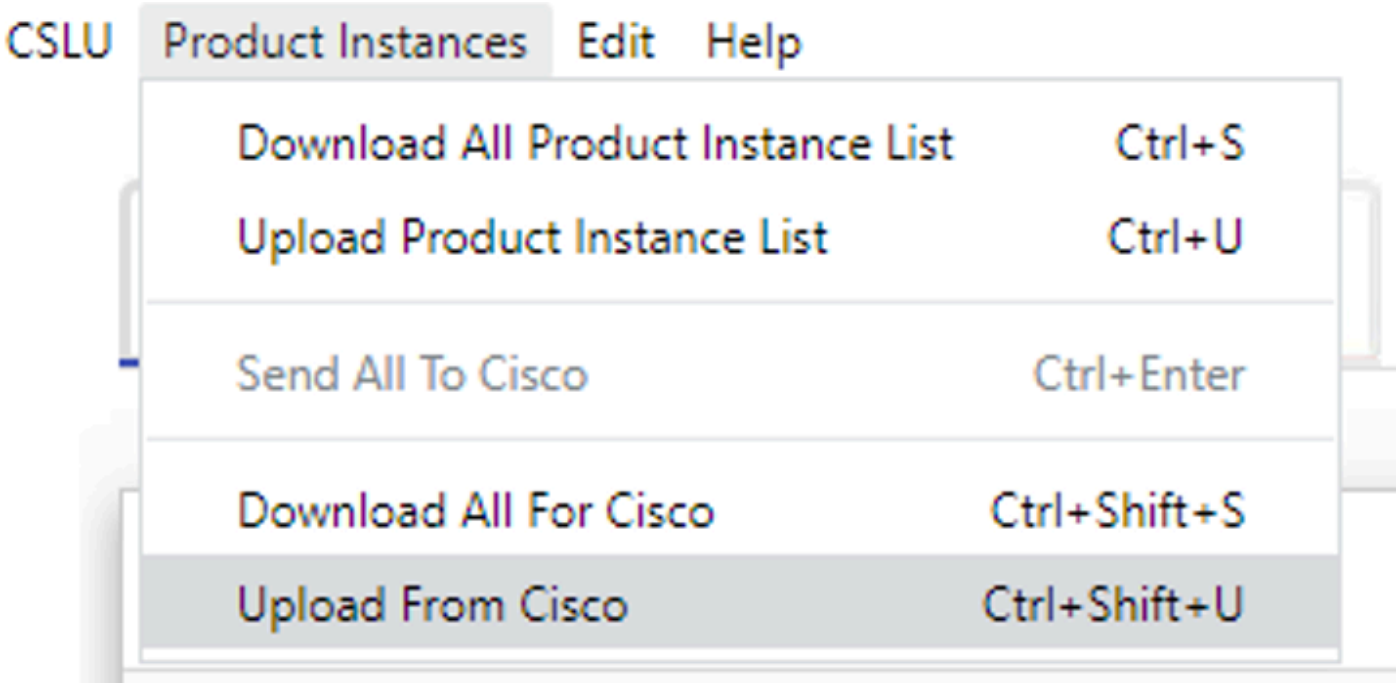


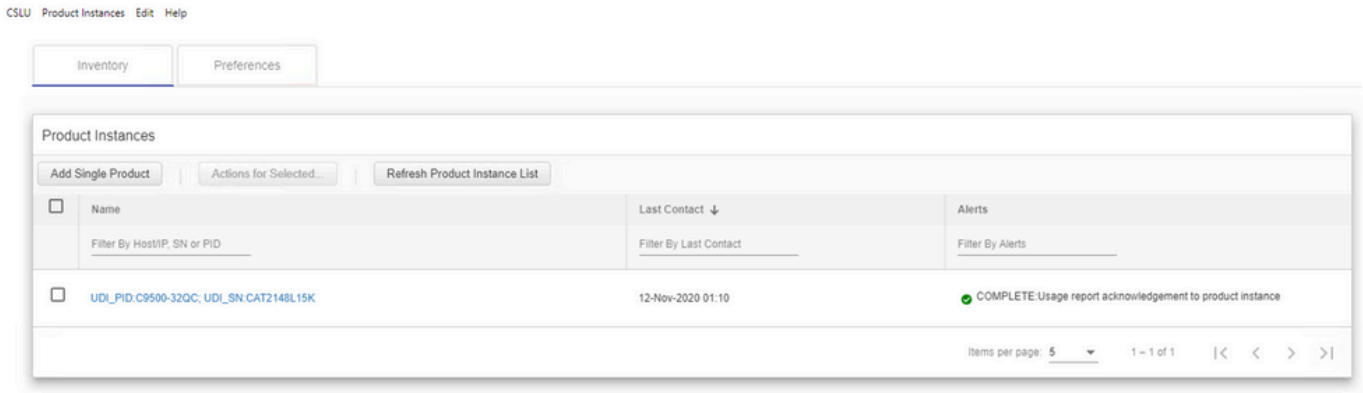

Étape 5. Une fois les données traitées, l'accusé de réception est généré. Téléchargez le fichier ACK et téléchargez-le sur CSLU.




Étape 6. Dans CSLU, importez le fichier ACK à partir de la barre de menus et accédez à Product Instances > Upload from Cisco, comme illustré dans cette image.




Étape 7. Une fois l'ACK téléchargé, le message est envoyé aux IP. La même chose peut être vérifiée par la colonne Alertes.




SLP - Mode hors connexion

SLP peut également fonctionner en mode hors connexion total. Il s'agit principalement des réseaux à répartition d'air, qui ne préfèrent pas la connectivité Internet et choisissent également de ne pas utiliser CSLU. En mode hors connexion, le transport est défini sur 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>

Chaque fois que vous souhaitez rapporter les données d'utilisation à CSSM, les rapports d'utilisation doivent être téléchargés sous forme de fichier et téléchargés manuellement dans CSSM. Dans un système haute disponibilité, active collecte l'utilisation pour les périphériques en veille/membres.

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

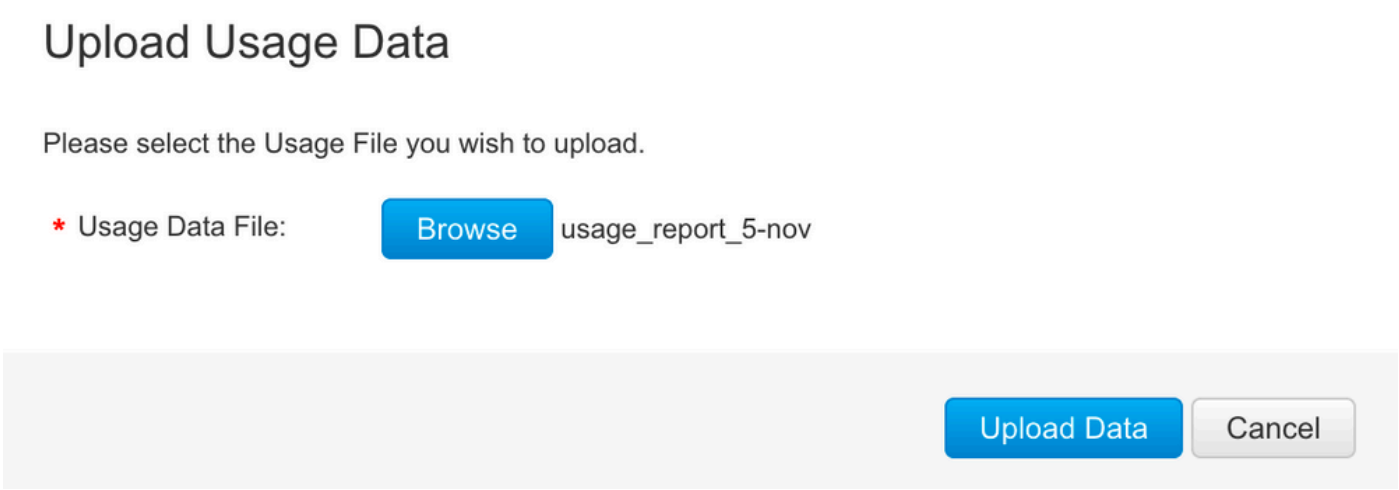
Switch#license smart save usage ?
all Save all reports
days Save reports from last n days
rum-Id Save an individual RUM report
unreported Save all previously un reported reports

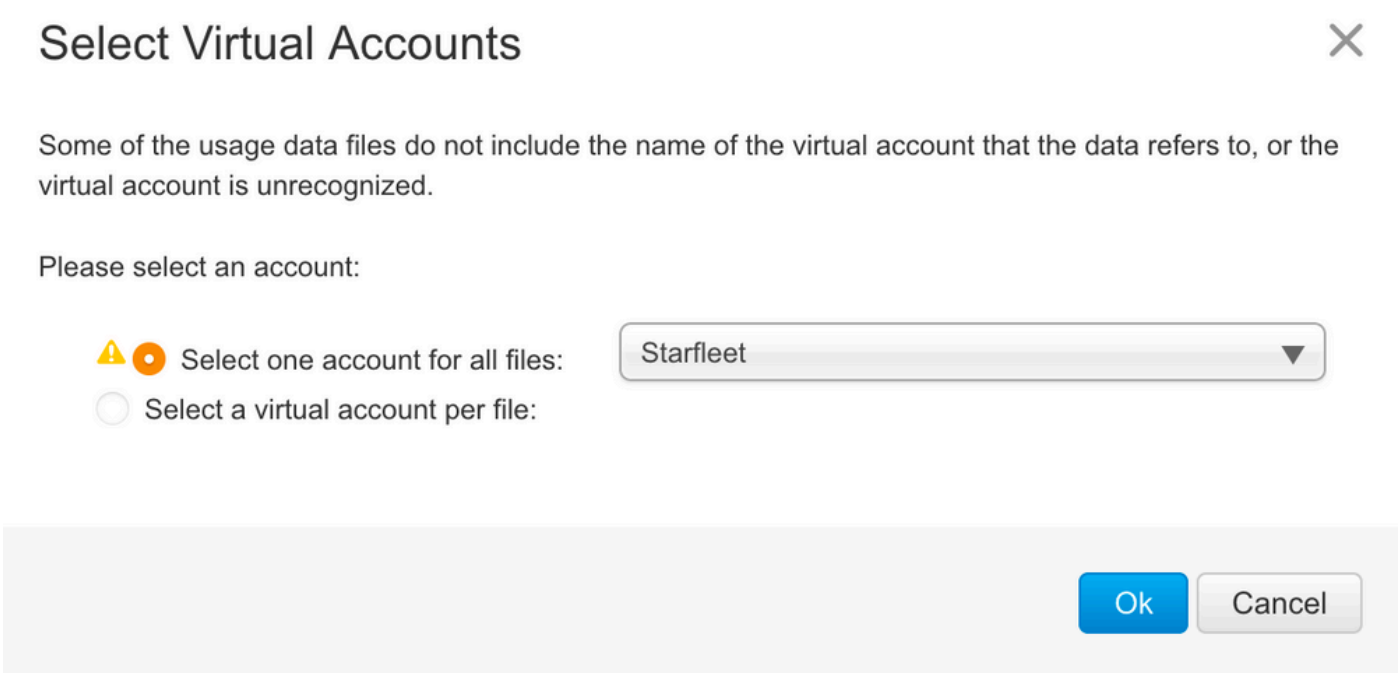
Maintenant, ce rapport doit être téléchargé manuellement dans CSSM.

Exportez les données d'utilisation enregistrées de PI vers le bureau.

Sur la page CSSM Smart Account, accédez à Report > Usage Data Files > Upload usage data. Dans la fenêtre contextuelle, sélectionnez le rapport d'utilisation et cliquez sur upload.

Une fois le fichier téléchargé, vous devez choisir l'adresse MAC correcte à laquelle le périphérique est associé.






Une fois que les données sont traitées et que l'accusé de réception est prêt, téléchargez le fichier et chargez-le sur l'interface de programmation.

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

Changements de comportement

Les modifications suivantes sont apportées à la fonction Smart Licensing sur les versions :

- **Trust Sync** - À partir de la version 17.7.1, le code de confiance est installé sur le commutateur sur toutes les topologies prises en charge, telles que les méthodes CSLU et Offline.
- **Changements de confidentialité** - À partir de la version 17.7.1, les informations de chaîne de version et de nom d'hôte de la version 17.9.1 sont incluses dans les rapports RUM envoyés à CSSM, si les paramètres de confidentialité respectifs sont désactivés.
- **Détails du compte** - Depuis la version 17.7.1, le message ACK de CSSM inclut les informations du compte et les détails SA/VA.
- **RUM Report Throttling** : à partir de la version 17.9.1, l'intervalle de rapport du moment où l'IP initie la communication est limité. La fréquence minimale des rapports est limitée à un jour. Cela signifie que l'instance de produit n'envoie pas de rapports RUM plus d'une fois par jour.

Dépannage

Questionnaire de dépannage générique

**Scénario 1 :** Certains protocoles (c'est-à-dire HSRP) ne fonctionnent plus après la mise à niveau de Cisco IOS XE à partir d'une version très ancienne (16.9.x).

Vérifiez le niveau de démarrage de la licence pour voir s'il est toujours le même qu'avant la mise à niveau de Cisco IOS XE. Il est possible que le niveau de démarrage de la licence ait été réinitialisé à Networking-Essentials, ce qui ne prend peut-être pas en charge les protocoles défaillants (c'est-à-dire HSRP).

**Scénario 2 :** état de la licence avec les messages « Raison de l'échec : échec de l'envoi du message HTTP Call Home » ou « Dernière tentative de communication : EN ATTENTE »

Cela peut être lié à des problèmes de connectivité de base. Pour résoudre le contrôle :

- Connectivité réseau pour atteindre le CSSM : adresse IP, routes, etc.
- Le ip http client source interface est configuré correctement.
- Décalage horaire. (NTP doit être configuré pour fournir une heure/un fuseau horaire correct)
- Si la configuration interne du pare-feu bloque le trafic vers CSSM

**Scénario 3 :** Que se passe-t-il si l'erreur « %SMART_LIC-3-AUTH_RENEW_FAILED : Renouvellement de l'autorisation avec Cisco Smart Software Manager (CSSM) : undefined method 'each' for nil : NilClass » est observée après un an d'enregistrement.

Réenregistrez le produit. Générez un nouvel ID de jeton sur CSSM et enregistrez à nouveau l'instance de produit sur CSSM**.**

**Scénario 4 :** Message d'erreur « %SMART_LIC-3-COMM_FAILED : échec des communications », en l'absence d'erreurs de connectivité avec Cisco.

Quand il n'y a pas de problèmes de connectivité à CSSM et si sur PI, toujours l'erreur mentionnée est vue, alors cela peut être parce que la récente mise à niveau du serveur a causé la suppression du certificat. Le certificat est requis pour l'authentification TLS des deux côtés en communication. Dans ce cas, configurez l'interface de ligne de commande ip http client secure-trustpoint SLA-TrustPoint sur l'interface IP et réessayez.

Debug PI

Pour résoudre les problèmes, les commandes collectées à partir de PI sont les suivantes :

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
```

Debug CSLU

Si un problème sur CSLU est débogué, il est important que le fichier journal de ce répertoire sur le PC CSLU installé soit pris.

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

Références connexes

- Migration vers SL à l'aide d'une politique - Migration des licences SL/SLR/PLR héritées vers SL à l'aide d'une politique
- Notes de mise à jour : RN-9200, RN-9300, RN-9400, RN-9500, RN-9600
- Guides de configuration : Cat9200-CG, Cat9300-CG, Cat9400-CG, Cat9500-CG, Cat9600-CG
- Références des commandes : Cat9200-CR, Cat9300-CR, Cat9400-CR, Cat9500-CR, Cat9600-CR
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.