Dépannage des licences Smart sur les plateformes Catalyst

Table des matières

Introduction

Le présent document décrit utiliser Cisco Smart Licensing (système infonuagique) pour gérer les

licences logicielles sur les commutateurs Catalyst.

Qu'est-ce que Cisco Smart Licensing ?

Cisco Smart Licensing est un système de gestion des licences unifié basé sur le cloud qui gère toutes les licences logicielles sur l'ensemble des produits Cisco. Il vous permet d'acheter, de déployer, de gérer, de suivre et de renouveler des licences logicielles Cisco. Il fournit également des informations sur la propriété et la consommation des licences via une interface utilisateur unique

La solution se compose de comptes Smart en ligne (sur le portail Cisco Smart Licensing Portal) utilisés pour suivre les ressources logicielles Cisco et du gestionnaire Cisco Smart Software Manager (CSSM) utilisé pour gérer les comptes Smart. CSSM permet d'effectuer toutes les tâches liées à la gestion des licences, telles que l'enregistrement, la désinscription, le déplacement et le transfert de licences. Les utilisateurs peuvent être ajoutés et bénéficier d'un accès et d'autorisations au compte Smart et à des comptes virtuels spécifiques.

Pour en savoir plus sur Cisco Smart Licensing, visitez :

a) Page d'accueil de Cisco Smart Licensing

b) Communauté Cisco - Formation à la demande

Pour plus d'informations sur la nouvelle méthode de gestion des licences Smart utilisant la stratégie dans Cisco IOS® XE 17.3.2 et versions ultérieures, consultez Gestion des licences Smart utilisant la stratégie sur les commutateurs Catalyst

Vous êtes novice en matière de licences Smart et/ou d'administration de comptes Smart ? Visitez et inscrivez-vous au nouveau cours de formation des administrateurs et enregistrez : Communauté Cisco - Devenez intelligent avec les comptes/licences Smart Cisco et Mes droits Cisco

Les comptes Smart peuvent être créés ici : Comptes Smart

Les comptes Smart peuvent être gérés ici : Smart Software Licensing

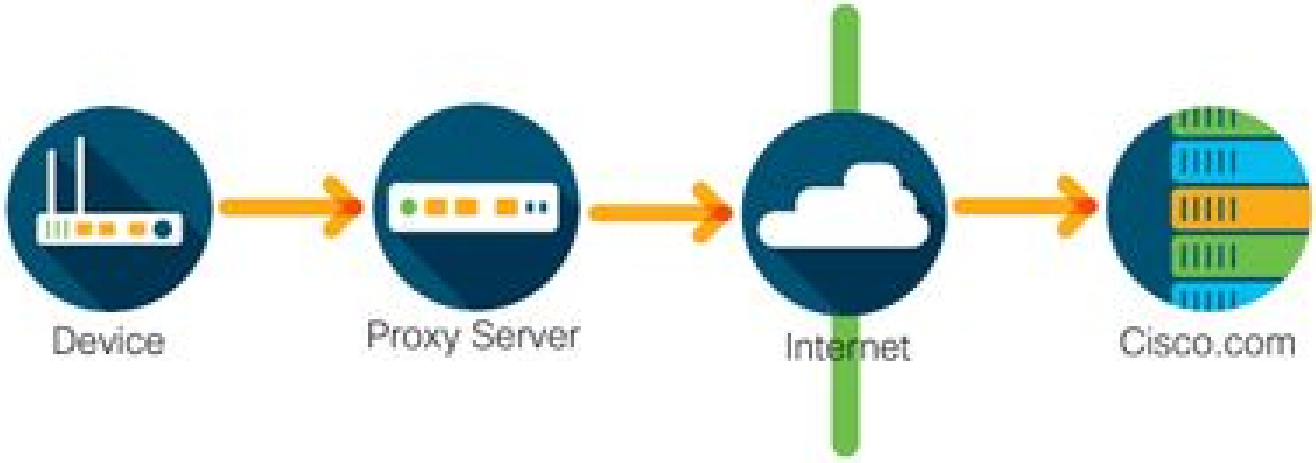
Méthodes de mise en oeuvre des licences Smart

Il existe plusieurs méthodes de déploiement de Cisco Smart Licensing qui peuvent être exploitées en fonction du profil de sécurité d'une entreprise, notamment :

Accès direct au cloud

Les produits Cisco envoient des informations d'utilisation directement sur Internet en toute sécurité à l'aide de HTTPS. Aucun composant supplémentaire n'est nécessaire.

Accès via un proxy HTTPS



Les produits Cisco envoient des informations d'utilisation via un serveur proxy HTTP en utilisant HTTPS en toute sécurité. Vous pouvez utiliser un serveur proxy existant ou le déployer via la passerelle de transport Cisco. (cliquez ici pour plus d'informations).

Serveur de licences sur site (également appelé Cisco Smart Software Manager satellite)

Les produits Cisco envoient les informations d'utilisation à un serveur sur site plutôt que directement sur Internet. Une fois par mois, le serveur accède à tous les périphériques via Internet via HTTPS ou peut être transféré manuellement pour synchroniser sa base de données. CSSM On-prem (Satellite) est disponible en tant que machine virtuelle (VM) et peut être téléchargé ici. Pour plus d'informations, consultez la page Smart Software Manager Satellite.

Plates-formes Cisco IOS XE prises en charge

- À partir de la version 16.9.1 de Cisco IOS XE, les plates-formes de commutation des gammes Catalyst 3650/3850 et Catalyst 9000 prennent en charge la méthode Cisco Smart Licensing comme seule méthode de licence.
- À partir de la version 16.10.1 de Cisco IOS XE, les plates-formes de routeurs telles que ASR1K, ISR1K, ISR4K et les routeurs virtuels (CSRv / ISRv) prennent en charge la méthode Cisco Smart Licensing comme seule méthode de licence.

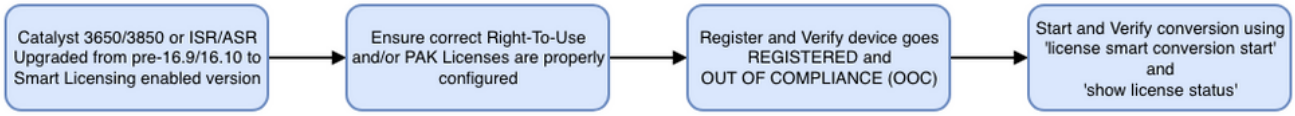
Migration des anciennes licences vers les licences Smart

Il existe deux méthodes pour convertir une licence héritée, comme le droit d'utilisation (RTU) ou la clé d'activation de produit (PAK) en licence Smart. Pour plus d'informations sur la méthode à suivre, reportez-vous aux notes de version et/ou au guide de configuration correspondant au périphérique Cisco concerné.

Conversion via la conversion DLC (Device Led Conversion)

- La conversion DLC (Device Led Conversion) est une méthode ponctuelle dans laquelle le produit Cisco peut indiquer les licences qu'il utilise et les licences sont automatiquement déposées dans leur compte Smart correspondant sur le Cisco Smart Software Manager (CSSM). La procédure DLC est exécutée directement à partir de l'interface de ligne de commande (CLI) du périphérique Cisco spécifique.

- Le processus DLC est uniquement pris en charge sur les plates-formes Catalyst 3650/3850 et certains routeurs. Pour connaître les modèles de routeur spécifiques, reportez-vous au guide de configuration de la plate-forme et aux notes de version. Exemple : procédure DLC pour Catalyst 3850 exécutant les versions Fuji 16.9.x.



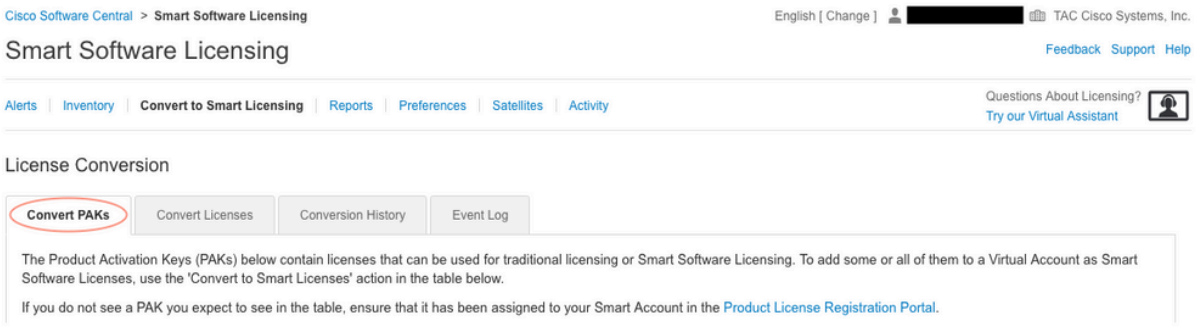
Conversion via Cisco Smart Software Manager (CSSM) ou License Registration Portal (LRP)

Méthode de Cisco Smart Software Manager (CSSM) :

1. Connectez-vous à Cisco Smart Software Manager (CSSM) à l'adresse https://software.cisco.com/

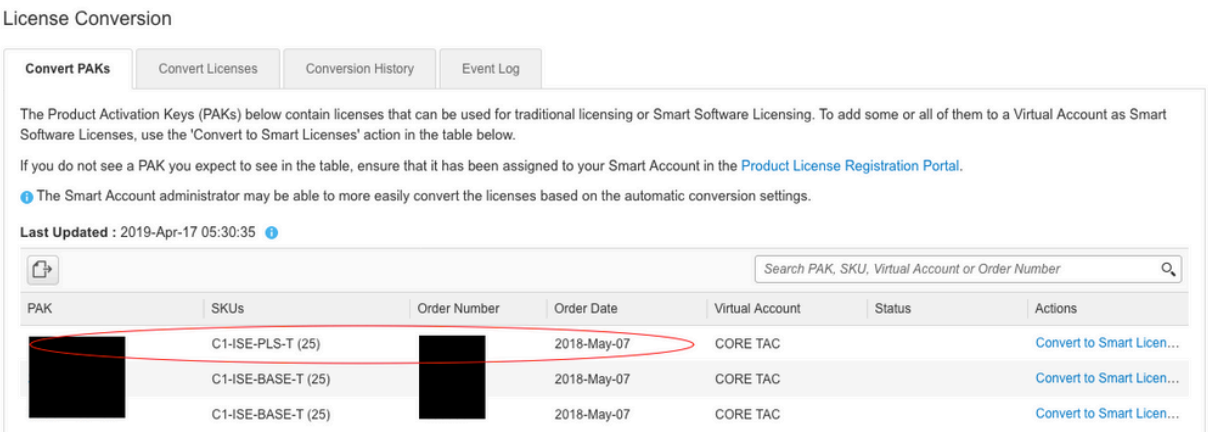
2. Accédez à Licence logicielle Smart > Convertir en licence Smart

3. Choisissez Convertir PAK ou Convertir les licences

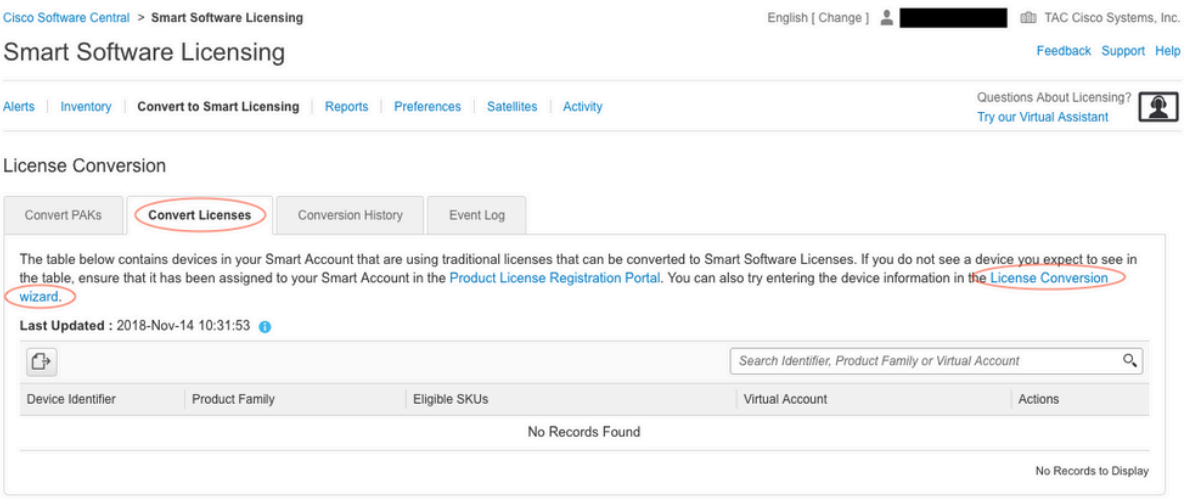


4. Pour convertir une licence PAK, recherchez la licence dans ce tableau. Pour convertir une licence non PAK, utilisez l'Assistant Conversion de licence pour obtenir des instructions détaillées.

Emplacement des fichiers PAK connus associés au compte :

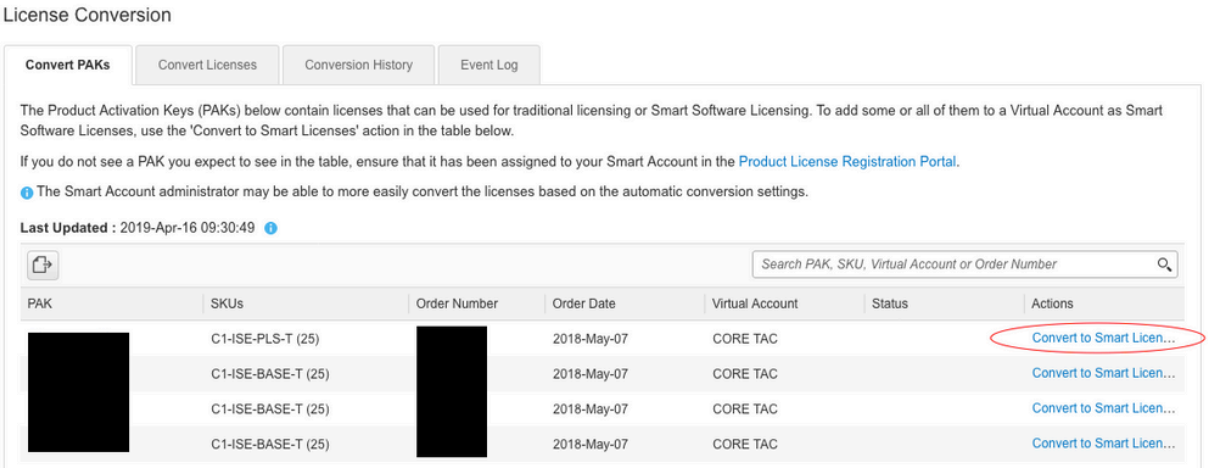


Emplacement du lien Assistant Conversion de licence :

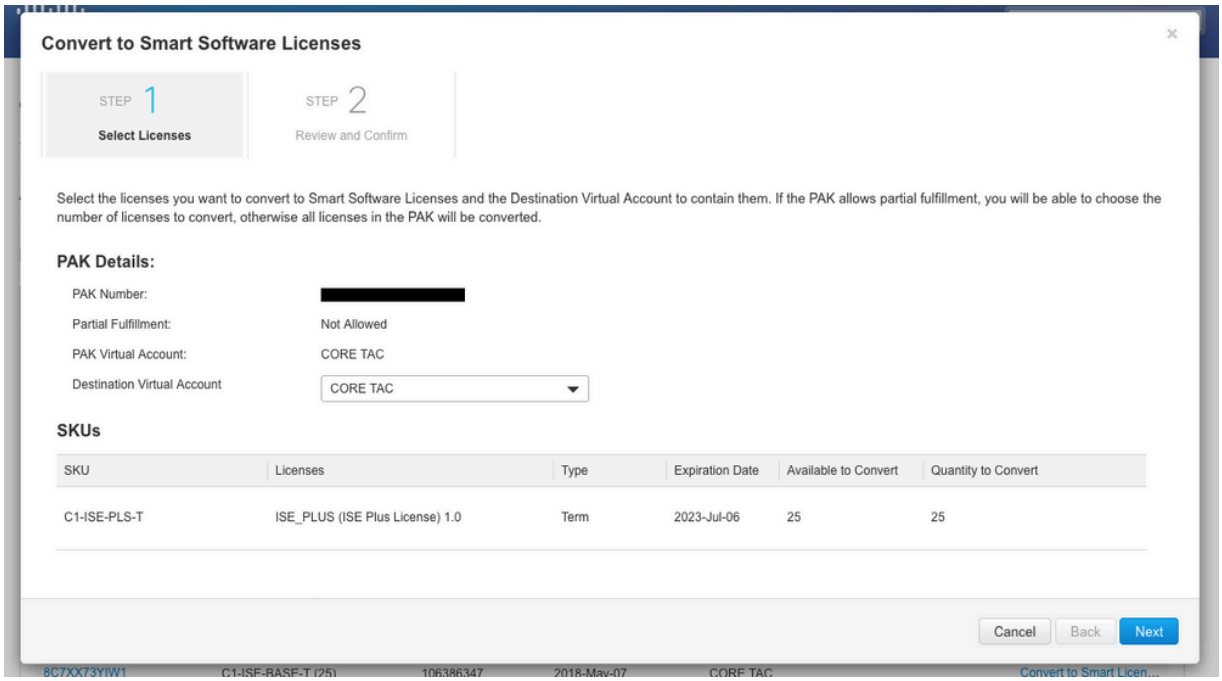


5. Localisez la combinaison de licence et de produit souhaitée.

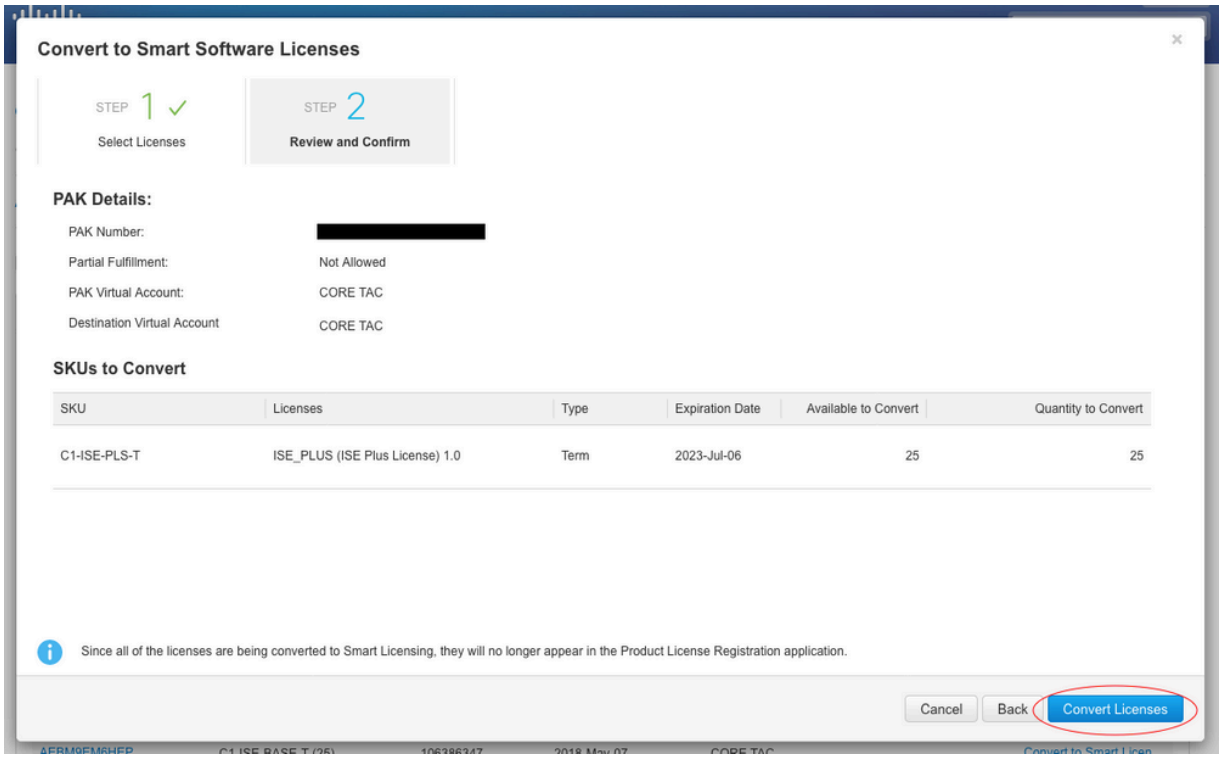
6. Cliquez sur (sous Actions) : Convertir en licence Smart.



7. Choisissez un compte virtuel, une licence, puis cliquez sur Suivant.



8. Vérifiez les sélections, puis cliquez sur Convertir les licences.

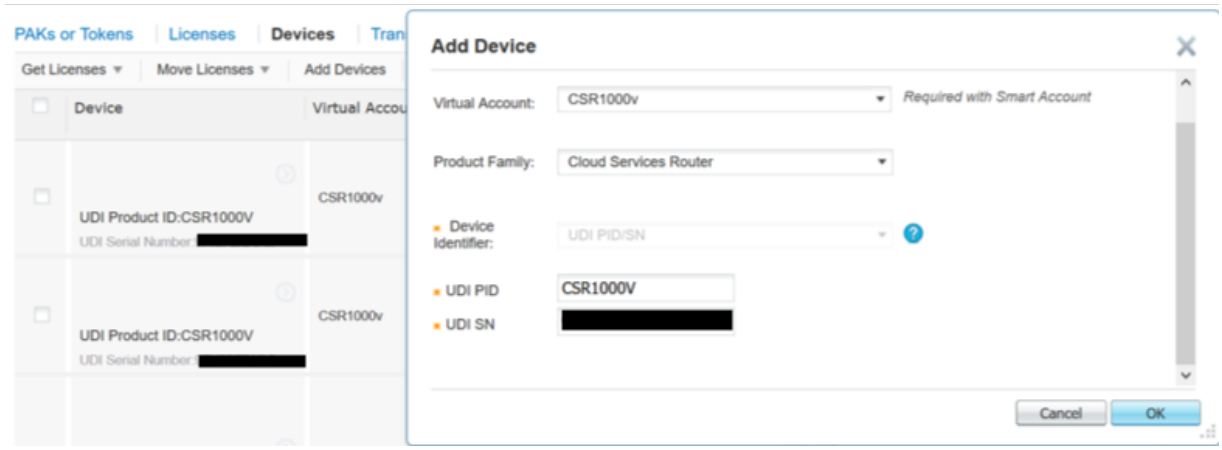


Méthode LRP (License Registration Portal) :

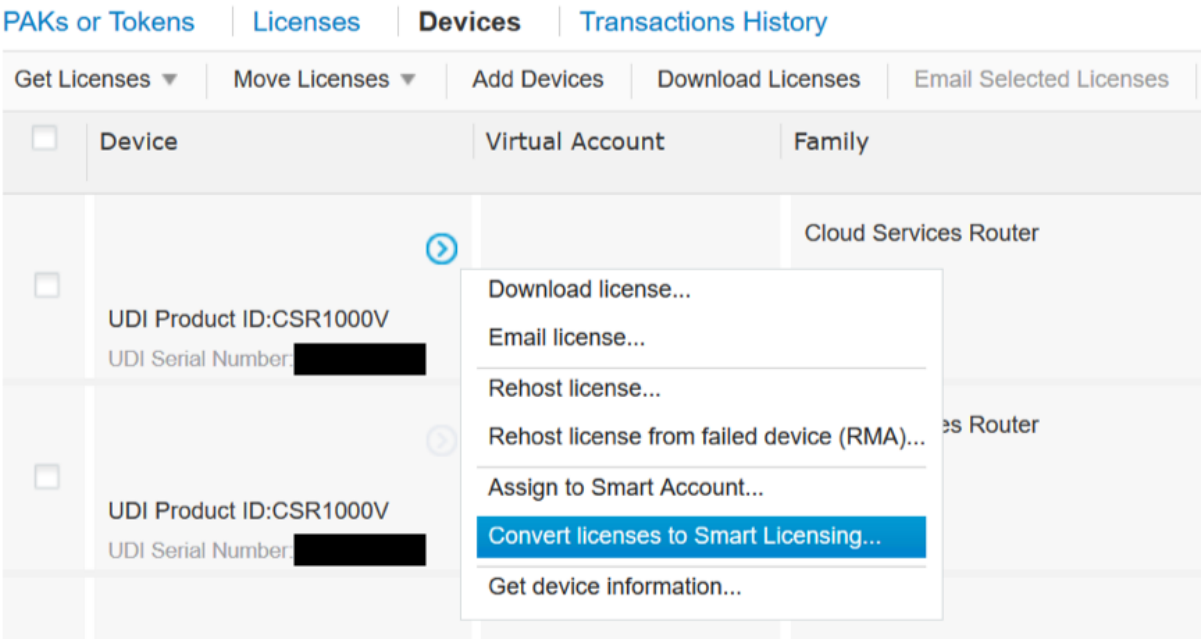
1. Connectez-vous au portail d'enregistrement des licences (LRP) http://tools.cisco.com/SWIFT/LicensingUI/Home

2. Accédez à Périphériques > Ajouter des périphériques.

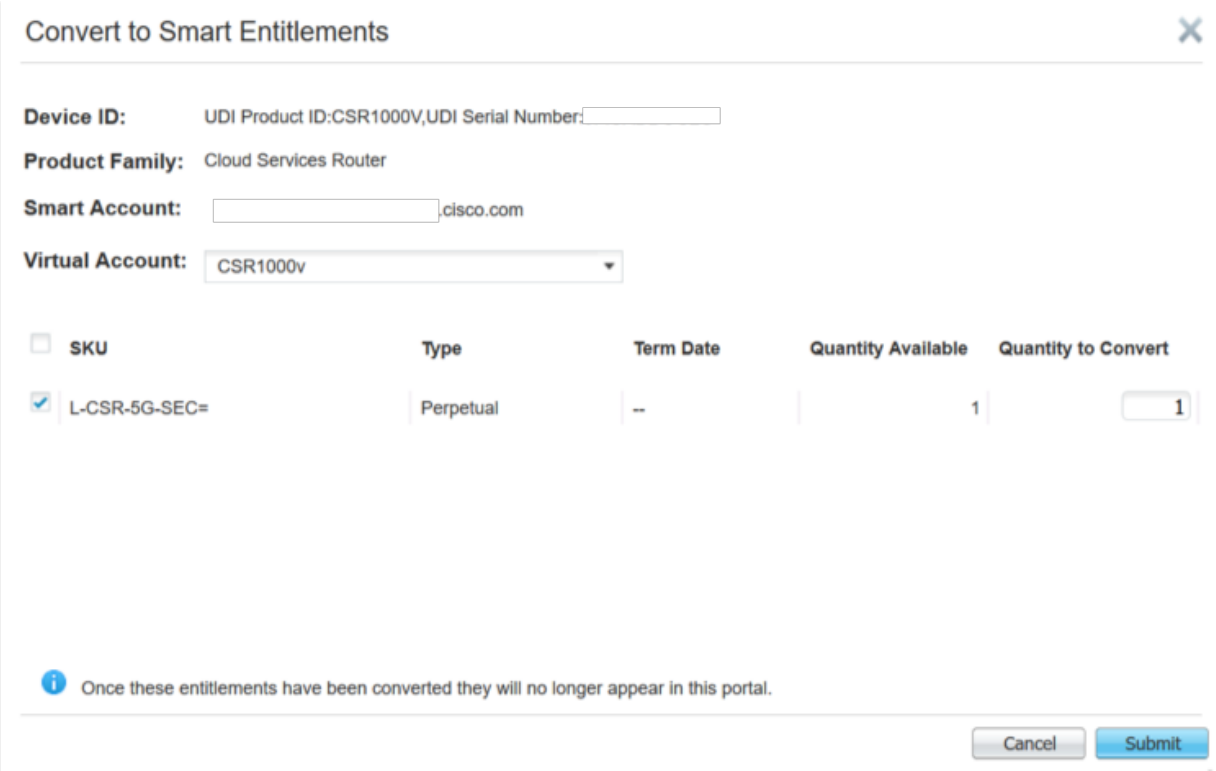
3. Entrez l'ID de produit et le numéro de série de la famille de produits et de l'identifiant de périphérique unique (UDI) appropriés, puis cliquez sur OK. Les informations UDI peuvent être obtenues à partir de la commande show version ou show inventory de l'interface de ligne de commande (CLI) du périphérique Cisco.



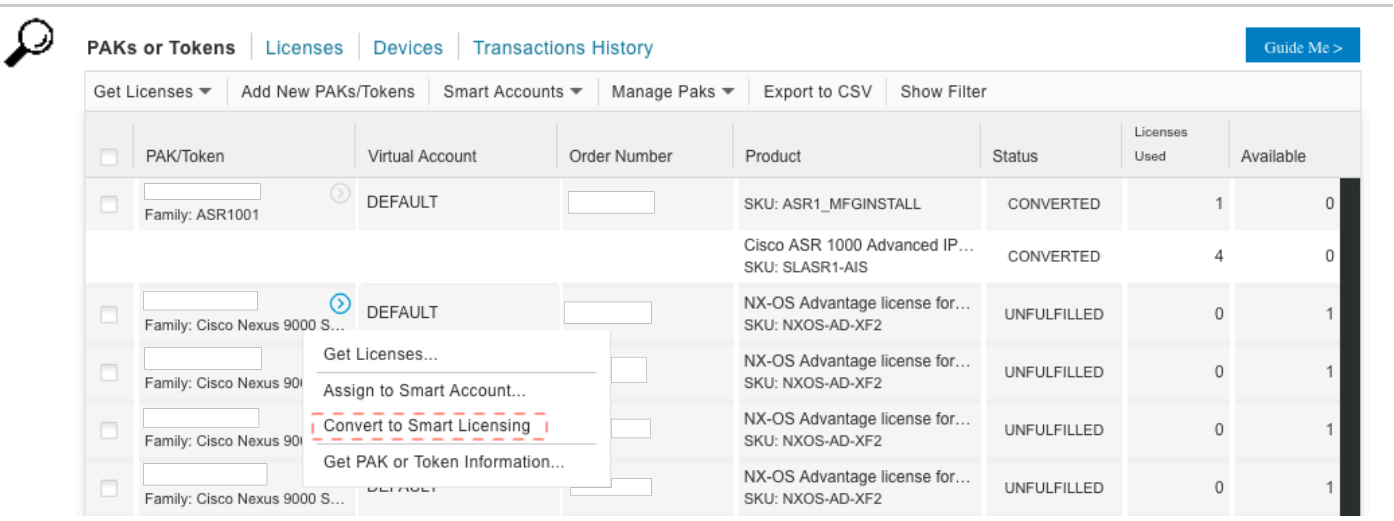
4. Choisissez le périphérique ajouté et Convertissez les licences en licences Smart



5. Attribuez le compte virtuel approprié, choisissez les licences à convertir et cliquez sur Submit.



Conseil : l'outil LRP peut également être utilisé en recherchant la famille de licences/produits dans l'onglet PAK ou Tokens. Cliquez sur la liste déroulante en regard de la clé PAK/du jeton et choisissez Convertir en licence Smart :



Convertir via le service Cisco Global Licensing Operations (GLO) et le contacter

Le département Global Licensing Operations est accessible ici à partir de nos centres de contacts internationaux.

Changement de comportement hautes performances du Catalyst 9500 de 16.9 à 16.12.3

Comme les autres modèles Catalyst 9000, les modèles hautes performances Catalyst 9500 ont été activés avec Smart Licensing dans la catégorie Cisco IOS XE version 16.9 et ultérieures. Toutefois, pour les modèles hautes performances Catalyst 9500, chaque modèle possédait sa propre étiquette d'autorisation de licence. Il a été décidé plus tard, par les équipes produit et marketing, d'unifier les balises d'autorisation des plates-formes C9500. Cette décision a modifié le comportement sur les modèles hautes performances C9500, en remplaçant l'utilisation d'étiquettes de droits spécifiques par des licences C9500 génériques.

Ce changement de comportement est documenté dans les défauts suivants :

a) ID de bogue Cisco CSCvp30661

b) ID de bogue Cisco CSCvt01955

Voici les modifications de licence avant et après les modifications susmentionnées pour les modèles hautes performances C9500 :

Cisco IOS XE versions 16.11.x et antérieures

Chaque modèle hautes performances C9600 possède ses propres balises d'autorisation.

Maquette	Licence
C9500-32C	C9500 32C NW Essentials

	C9500 32C NW Advantage C9500 32C DNA Essentials Avantage de l'ADN C9500 32C
C9500-32QC	C9500 32QC NW Essentials C9500 32QC NW Advantage C9500 32QC DNA Essentials C9500 32QC DNA Advantage
C9500-24Y4C	C9500 24Y4C NW Essentials C9500 24Y4C NW Advantage C9500 24Y4C DNA Essentials C9500 24Y4C DNA Advantage
C9500-48Y4C	C9500 48Y4C NW Essentials C9500 48Y4C NW Advantage C9500 48Y4C DNA Essentials C9500 48Y4C DNA Advantage

Remarque : les versions 16.12.1 et 16.12.2 de Cisco IOS XE présentent des défauts tels que l'ID de bogue Cisco CSCvp3061 et l'ID de bogue Cisco CSCvt01955. Ces défauts sont traités dans les versions 16.12.3a et ultérieures.

Cisco IOS XE versions 16.12.3 et ultérieures

Les plates-formes hautes performances Catalyst 9500 utilisent désormais des balises de licence réseau génériques et des balises de licence DNA distinctes. Ce tableau présente les modifications des droits mises en évidence dans Cisco IOS XE version 16.12.3 et ultérieure :

Maquette	Licence
C9500-32C	C9500 Network Essentials

	Avantage du réseau C9500 C9500 32C DNA Essentials Avantage de l'ADN C9500 32C
C9500-32QC	C9500 Network Essentials Avantage du réseau C9500 C9500 32QC DNA Essentials C9500 32QC DNA Advantage
C9500-24Y4C	C9500 Network Essentials Avantage du réseau C9500 C9500 24Y4C DNA Essentials C9500 24Y4C DNA Advantage
C9500-48Y4C	C9500 Network Essentials Avantage du réseau C9500 C9500 48Y4C DNA Essentials C9500 48Y4C DNA Advantage

Remarque : les mises à niveau à partir des versions 16.12.1 et 16.12.2 de Cisco IOS XE affichent ce comportement de licence. Les mises à niveau de Cisco IOS XE versions 16.9.x, 16.10.x, 16.11.x à 16.12.3 reconnaissent les anciennes configurations de licence.

FAQ sur le changement hautes performances du C9500

1. Pourquoi le support Cisco alloue-t-il une licence réseau générique alors que mon périphérique utilise une licence réseau spécifique à un périphérique ?

Des balises génériques sont fournies car elles constituent les balises d'autorisation appropriées pour le périphérique réseau. Cela permet d'utiliser les étiquettes d'autorisation sur l'ensemble de la plate-forme Cat9500, et pas seulement sur les modèles hautes performances spécifiques du C9500. Les images antérieures à la version 16.12.3 qui demandent des balises de licence spécifiques à un périphérique sont conformes aux balises de licence génériques, car les licences plus spécifiques tombent sous les licences génériques

dans la hiérarchie des licences.

2. Pourquoi deux balises réseau apparaissent-elles parfois dans le compte Smart ?

   Ce comportement est dû à la hiérarchie des licences et se produit lorsque le périphérique s'exécute sur une image plus ancienne qui utilise des balises de licence spécifiques au périphérique. Les images plus anciennes qui demandent des balises de licence spécifiques à un périphérique sont conformes aux balises de licence génériques, car les balises plus spécifiques tombent sous les licences génériques dans la hiérarchie de licence.

Configuration

Configuration de base

Vous trouverez la procédure exacte de configuration de Smart Licensing dans le Guide de configuration de la gestion du système disponible pour chaque version/plate-forme.

Par exemple : System Management Configuration Guide, Cisco IOS XE Fuji 16.9.x (commutateurs Catalyst 9300)

Jeton d'enregistrement/ID de périphérique

Avant d'enregistrer le périphérique, un jeton doit être généré. Le jeton d'enregistrement, également appelé jeton d'ID de périphérique, est un jeton unique généré à partir du portail de licences Smart ou de Cisco Smart Software Manager sur site lors de l'enregistrement initial d'un périphérique Cisco sur le compte Smart correspondant. Un jeton individuel peut être utilisé pour enregistrer plusieurs périphériques Cisco en fonction des paramètres utilisés lors de la création.

Le jeton d'enregistrement n'est également requis que lors de l'enregistrement initial d'un périphérique Cisco, car il fournit les informations au périphérique pour qu'il puisse appeler le back-end Cisco et être lié au compte Smart correct. Une fois le périphérique Cisco enregistré, le jeton n'est plus nécessaire.

Pour plus d'informations sur les jetons d'enregistrement et sur la manière dont ils sont générés, cliquez ici pour obtenir un guide général. Pour plus de détails, reportez-vous au guide de configuration du périphérique Cisco spécifique.

États d'enregistrement et de licence

Lors du déploiement et de la configuration de Smart Licensing, plusieurs états sont possibles pour un périphérique Cisco. Ces états peuvent être affichés en regardant show license all ou show license status à partir de l'interface de ligne de commande (CLI) du périphérique Cisco.

Voici une liste de tous les états et leur description :

État d'évaluation (non identifié)

- Evaluation est l'état par défaut du périphérique lors de son premier démarrage.

- Généralement, cet état est visible lorsqu'un périphérique Cisco n'a pas encore été configuré pour la licence Smart ou enregistré sur un compte Smart.
- Dans cet état, toutes les fonctionnalités sont disponibles et le périphérique peut modifier librement les niveaux de licence.
- La période d'évaluation est utilisée lorsque le périphérique est à l'état non identifié. Le périphérique ne tente pas de communiquer avec Cisco dans cet état.
- Cette période d'évaluation est de 90 jours d'utilisation et non de 90 jours calendaires. Une fois la période d'évaluation expirée, elle n'est jamais réinitialisée.
- Il y a une période d'évaluation pour l'ensemble du périphérique ; il ne s'agit pas d'une période d'évaluation par autorisation.
- Lorsque la période d'évaluation expire au bout de 90 jours, le périphérique passe en mode EVAL EXPIRY. Cependant, il n'y a pas d'impact fonctionnel ou d'interruption dans la fonctionnalité, même après le rechargement. Actuellement, il n'y a pas d'application en place.
- Le compte à rebours est maintenu au fil des redémarrages.
- La période d'évaluation est utilisée si le périphérique n'est pas encore enregistré auprès de Cisco et n'a pas reçu ces deux messages du back-end Cisco :
    1. Réponse positive à une demande d'enregistrement.
    2. Réponse réussie à une demande d'autorisation d'habilitation.

État enregistré

- Registered est l'état attendu une fois l'enregistrement terminé.
- Cet état indique que le périphérique Cisco a réussi à communiquer avec un compte Smart Cisco et à s'enregistrer.
- Le périphérique reçoit un certificat d'identification, valide pendant un an, qui est utilisé pour les communications futures.
- Le périphérique envoie une requête au CSSM pour autoriser les droits pour les licences qui sont utilisées sur le périphérique.
- Selon la réponse du CSSM, le périphérique passe alors à l'état Autorisé ou Non conforme.
- Le certificat d'identification expire à la fin d'une année. Au bout de six mois, le processus de l'agent logiciel tente de renouveler le certificat. Si l'agent ne peut pas communiquer avec le CSSM, il continue à essayer de renouveler le certificat d'ID jusqu'à la date d'expiration (un an). Au bout d'un an, l'agent revient à l'état Non identifié et tente d'activer la période d'évaluation. Le CSSM supprime l'instance de produit de sa base de données.

- État Agréé
- Autorisé est l'état attendu lorsque le périphérique utilise un droit et est en conformité (pas de solde négatif).
- Cet état indique que le type et le nombre de licences du compte virtuel sur CSSM étaient corrects pour autoriser la consommation des licences pour ce périphérique.
- Au bout de 30 jours, le périphérique envoie une nouvelle demande au CSSM pour renouveler l'autorisation.
- Cet état a une durée de 90 jours. Après 90 jours (si le renouvellement a échoué), le périphérique passe à l'état Autorisation expirée.

État non conforme

- Non conforme est l'état dans lequel le périphérique utilise un droit et n'est pas en conformité (solde négatif).
- Cet état s'affiche lorsque le périphérique ne dispose pas d'une licence disponible dans le compte virtuel correspondant auquel le périphérique Cisco est enregistré dans le compte Smart Cisco.
- Pour passer à l'état Conformité / Autorisé, vous devez ajouter le nombre et le type de licences corrects au compte Smart.
- Lorsqu'un périphérique est à l'état Non conforme, il envoie automatiquement une demande de renouvellement d'autorisation chaque jour.
- Les licences et les fonctionnalités continuent à fonctionner et n'ont aucun impact fonctionnel.

État Autorisation expirée

- L'autorisation expirée est l'état dans lequel le périphérique utilise un droit et n'a pas pu communiquer avec le compte Smart Cisco associé depuis plus de 90 jours.
- Cet état est généralement visible si le périphérique Cisco perd l'accès à Internet ou ne peut pas se connecter à tools.cisco.com après l'enregistrement initial.
- Les méthodes de gestion des licences Smart en ligne nécessitent que les périphériques Cisco communiquent au moins tous les 90 jours pour empêcher ce statut.
- CSSM renvoie toutes les licences utilisées pour ce périphérique au pool, car il n'a pas eu de communications avec le périphérique depuis 90 jours.
- Dans cet état, le périphérique continue d'essayer de contacter Cisco toutes les heures afin de renouveler l'autorisation d'autorisation, jusqu'à l'expiration de la période d'enregistrement (certificat d'ID).
- Si l'agent logiciel rétablit les communications avec Cisco et reçoit sa demande d'autorisation, il traite cette réponse normalement et entre dans l'un des états établis.

Considérations et mises en garde

À partir de la version 16.9.1 pour les commutateurs et de la version 16.10.1 pour les routeurs, un profil Call-home par défaut appelé CiscoTAC-1 est généré pour faciliter la migration vers Smart Licensing. Par défaut, ce profil est configuré pour la méthode d'accès direct au cloud.

<#root>

```
#show call-home profile CiscoTAC-1

Profile Name: CiscoTAC-1
Profile status: ACTIVE
Profile mode: Full Reporting
Reporting Data: Smart Call Home, Smart Licensing
Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Transport Method: http
HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService
Other address(es): default
<snip>
```

Lors de l'utilisation d'un serveur sur site Cisco Smart Software Manager, l'adresse de destination sous la configuration d'appel à distance active doit pointer vers elle (sensible à la casse !) :

<#root>

```
(config)#call-home
(cfg-call-home)#profile "CiscoTAC-1"
(cfg-call-home-profile)#destination address http https://
```

<IP/FQDN>

```
/Transportgateway/services/DeviceRequestHandler
```

DNS est requis pour résoudre tools.cisco.com. Si la connectivité du serveur DNS est dans un VRF, assurez-vous que l'interface source et le VRF appropriés sont définis :

```
Global Routing Table Used:
(config)#ip domain-lookup [source-interface <INTERFACE>]
(config)#ip name-server <IP>

VRF Routing Table Used:
(config)#ip domain-lookup [source-interface <INTERFACE>]     <<-- "ip vrf forwarding <VRF-NAME>" define
(config)#ip name-server vrf <VRF-NAME> <SERVER-IP>
```

Sinon, si DNS n'est pas disponible, configurez de manière statique le mappage DNS local vers IP (en fonction de la résolution DNS locale sur votre périphérique final) ou remplacez le nom DNS dans la configuration d'appel à distance par l'adresse IP. Référez-vous à l'exemple pour l'accès direct au cloud (pour que Cisco Smart Software Manager on-prem utilise son propre nom DNS au lieu de tools.cisco.com) :

```
(config)#ip host tools.cisco.com <x.x.x.x>
```

Si la communication vers tools.cisco.com doit provenir de l'interface dans un VRF spécifique (par exemple, Mgmt-vrf), cette CLI doit être configurée :

```
(config)#ip http client source-interface <VRF_INTERFACE>
```

Un nombre différent de licences peut être utilisé en fonction de la configuration du périphérique Cisco, par exemple avec les commutateurs Catalyst qui s'exécutent dans StackWise ou StackWise Virtual :

Commutateurs traditionnels pris en charge par pile (par exemple, la gamme Catalyst 9300) :

Licence réseau : 1 licence est utilisée par commutateur dans la pile

Licence DNA : 1 licence est utilisée par commutateur de la pile

Châssis modulaire (par exemple, gamme Catalyst 9400) :

Licence réseau : 1 licence est utilisée par superviseur dans le châssis

Licence DNA : 1 licence est utilisée par châssis

Commutateurs virtuels fixes pris en charge par pile (par exemple, gamme Catalyst 9500) :

Licence réseau : 1 licence est utilisée par commutateur dans la pile

Licence DNA : 1 licence est utilisée par commutateur de la pile

- Un seul profil Call Home peut être actif pour Smart Licensing.
- Les licences ne sont utilisées que si une fonction correspondante est configurée.
- Les périphériques Cisco configurés pour la licence Smart doivent être configurés avec la date et l'heure système correctes afin de s'assurer qu'ils sont correctement synchronisés avec le compte Smart Cisco correspondant. Si le décalage horaire du périphérique Cisco est trop éloigné, le périphérique peut ne pas s'enregistrer. L'horloge doit être définie ou configurée manuellement via un protocole de synchronisation tel que le protocole NTP (Network Time Protocol) ou le protocole PTP (Precision Time Protocol). Pour connaître les étapes exactes requises pour mettre en oeuvre ces modifications, reportez-vous au guide de configuration du périphérique Cisco spécifique.
- La clé PKI (Public Key Infrastructure) générée lors de l'enregistrement du périphérique Cisco doit être enregistrée si elle ne l'est pas automatiquement après l'enregistrement. Si le périphérique ne parvient pas à enregistrer la clé PKI, un syslog est généré qui vous invite à enregistrer la configuration via la commande copy running-config startup-config ou write memory.
- Si la clé PKI du périphérique Cisco n'est pas correctement enregistrée, l'état de la licence peut être perdu lors des basculements ou des rechargements.
- Smart Licensing ne prend pas en charge l'interception de certificat SSL de proxy HTTPS par défaut lors de l'utilisation de proxies tiers pour la méthode Proxy HTTPS. Pour prendre en charge cette fonctionnalité, vous pouvez désactiver l'interception SSL sur le proxy ou importer manuellement la certification envoyée à partir du proxy.

<#root>

How to Manually Import Certification as a TrustPoint:

```
The certificate will need be in a BASE64 format to be copied and pasted onto the device as a TrustPoint

The following example shown below uses "LicRoot" as the TrustPoint name, however, this name can be chan
```

```
Device#conf t
Device(config)#crypto pki trustpoint LicRoot
Device(ca-trustpoint)#enrollment terminal
Device(ca-trustpoint)#revocation-check none
Device(ca-trustpoint)#exit
Device(config)#crypto pki authenticate LicRoot
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
-----END CERTIFICATE-----
Certificate has the following attributes:
     Fingerprint MD5: XXXXXXXX
   Fingerprint SHA1: XXXXXXX
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

tools.cisco.com Lors de l'utilisation du proxy HTTP de la passerelle de transport, l'adresse IP doit être remplacée par le proxy, comme dans l'exemple suivant :

adresse de destination http https://tools.cisco.com/its/service/oddce/services/DDCEService PAR

adresse de destination http https://<TransportGW-IP_Address>:<numéro_port>/Transportgateway/services/DeviceRequestHandler

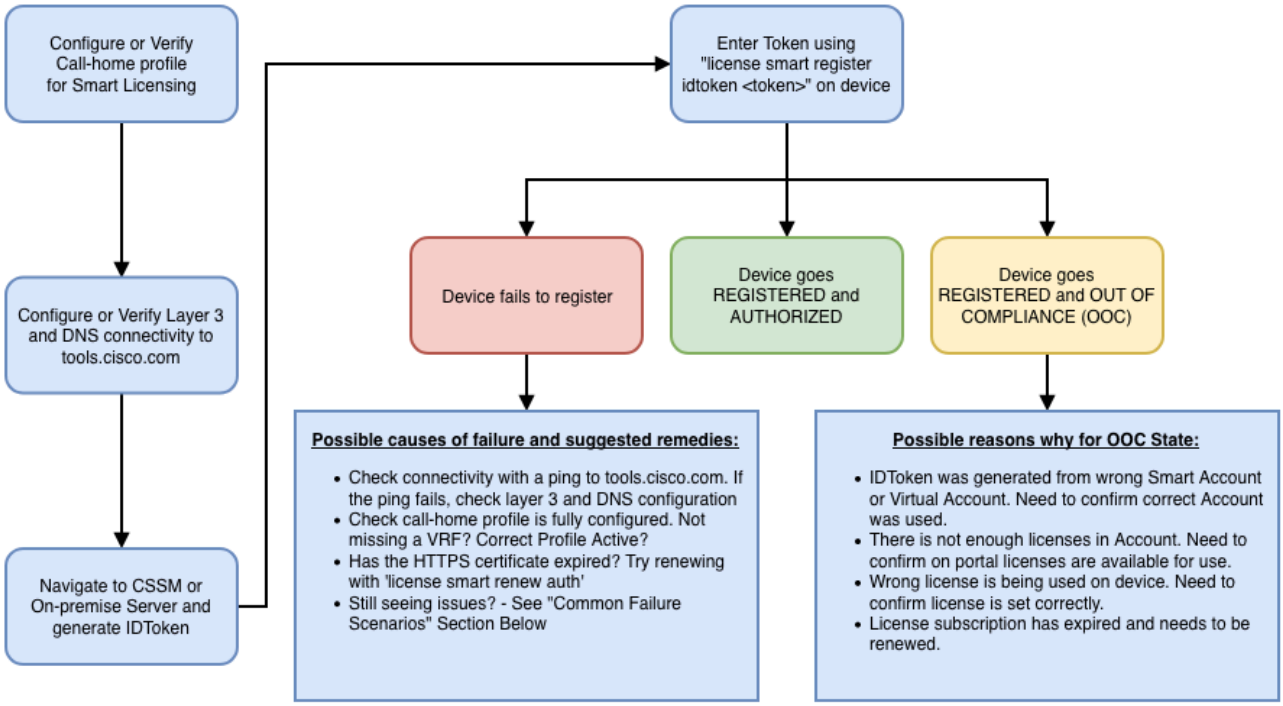
L'adresse IP de la passerelle de transport peut être trouvée en naviguant jusqu'aux paramètres HTTP et en recherchant sous les URL de service HTTP sur l'interface utilisateur graphique de la passerelle de transport Cisco.

Pour plus d'informations, reportez-vous au guide de configuration de la passerelle de transport Cisco ici.

Dépannage

Lorsque vous migrez un périphérique Cisco vers une version logicielle compatible avec les licences Smart, vous pouvez utiliser cet organigramme comme guide général pour les trois méthodes (Direct Cloud Access, HTTPS Proxy et Cisco Smart Software Manager On-prem).

Périphérique mis à niveau ou livré avec une version logicielle prenant en charge Smart Licensing (reportez-vous à la section 1.3 pour obtenir la liste des versions prises en charge de Cisco IOS XE).



Ces étapes de dépannage se concentrent principalement sur un scénario dans lequel le périphérique ne parvient pas à s'enregistrer.

Échec de l'enregistrement du périphérique

Après la configuration initiale, afin d'activer Smart Licensing, Token, qui est généré sur CSSM / Cisco Smart Software Manager sur site, doit être enregistré sur le périphérique via l'interface de ligne de commande :

```
license smart register idtoken <TOKEN>
```

Cette action génère les événements suivants :

<#root>

```
! Smart licensing process starts

!

Registration process is in progress. Use the 'show license status' command to check the progress and re

!

! Crypto key is automatically generated for HTTPS communication
```

```
!


Generating 2048 bit RSA keys, keys will be exportable... [OK] (elapsed time was 1 seconds)
%CRYPTO_ENGINE-5-KEY_ADDITION: A key named SLA-KeyPair has been generated or imported by crypto-engine
%PKI-4-NOCONFIGAUTOSAVE: Configuration was modified.  Issue "write memory" to save new IOS PKI configur

!


! Call-home start registration process


!

%CALL_HOME-6-SCH_REGISTRATION_IN_PROGRESS: SCH device registration is in progress. Call-home will poll

!


! Smart Licensing process connects with CSSM and check entitlement.


!

%SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features is allowed
%SMART_LIC-6-AGENT_REG_SUCCESS: Smart Agent for Licensing Registration with the Cisco Smart Software Ma
%SMART_LIC-4-CONFIG_NOT_SAVED: Smart Licensing configuration has not been saved

%SMART_LIC-5-IN_COMPLIANCE: All entitlements and licenses in use on this device are authorized

%SMART_LIC-6-AUTH_RENEW_SUCCESS: Authorization renewal with the Cisco Smart Software Manager or satelli
```

Pour vérifier la configuration de la fonction Call Home, exécutez l'interface CLI suivante :

<#root>

```
#show call-home profile all


Profile Name: CiscoTAC-1

    Profile status: ACTIVE

    Profile mode: Full Reporting


Reporting Data: Smart Call Home, Smart Licensing

    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes


Transport Method: http
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

    Other address(es): default

    Periodic configuration info message is scheduled every 1 day of the month at 09:15
```

```
    Periodic inventory info message is scheduled every 1 day of the month at 09:00

    Alert-group               Severity
    ------------------------  ------------
    crash                     debug
    diagnostic                minor
    environment               warning
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
    APF-.-WLC_.*              warning
    .*                        major
```

Pour vérifier l'état des licences Smart, exécutez cette CLI :

<#root>

```
#show license summary

Smart Licensing is ENABLED

Registration:


Status: REGISTERED

  Smart Account: TAC Cisco Systems, Inc.
  Virtual Account: Krakow LAN-SW
  Export-Controlled Functionality: ALLOWED
  Last Renewal Attempt: None
  Next Renewal Attempt: Nov 22 21:24:32 2019 UTC

License Authorization:


Status: AUTHORIZED



Last Communication Attempt: SUCCEEDED


 Next Communication Attempt: Jun 25 21:24:37 2019 UTC

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  C9500 Network Advantage (C9500 Network Advantage)         1 AUTHORIZED
  C9500-DNA-40X-A         (C9500-40X DNA Advantage)         1 AUTHORIZED
```

Si le périphérique ne s'enregistre pas (et si l'état est différent de REGISTERED), la non-conformité pointe vers un problème sur CSSM, tel qu'une licence manquante dans le compte virtuel Smart, un mappage incorrect (par exemple, un jeton d'un autre compte virtuel a été utilisé lorsque les licences ne sont pas disponibles), et ainsi de suite. Vérifiez les éléments suivants :

1. Vérifiez les paramètres de configuration et les scénarios d'échec courants

Reportez-vous à la section 2.1 pour connaître les étapes de configuration de base. Consultez également la section 5 pour les scénarios de défaillance courants observés sur le terrain.

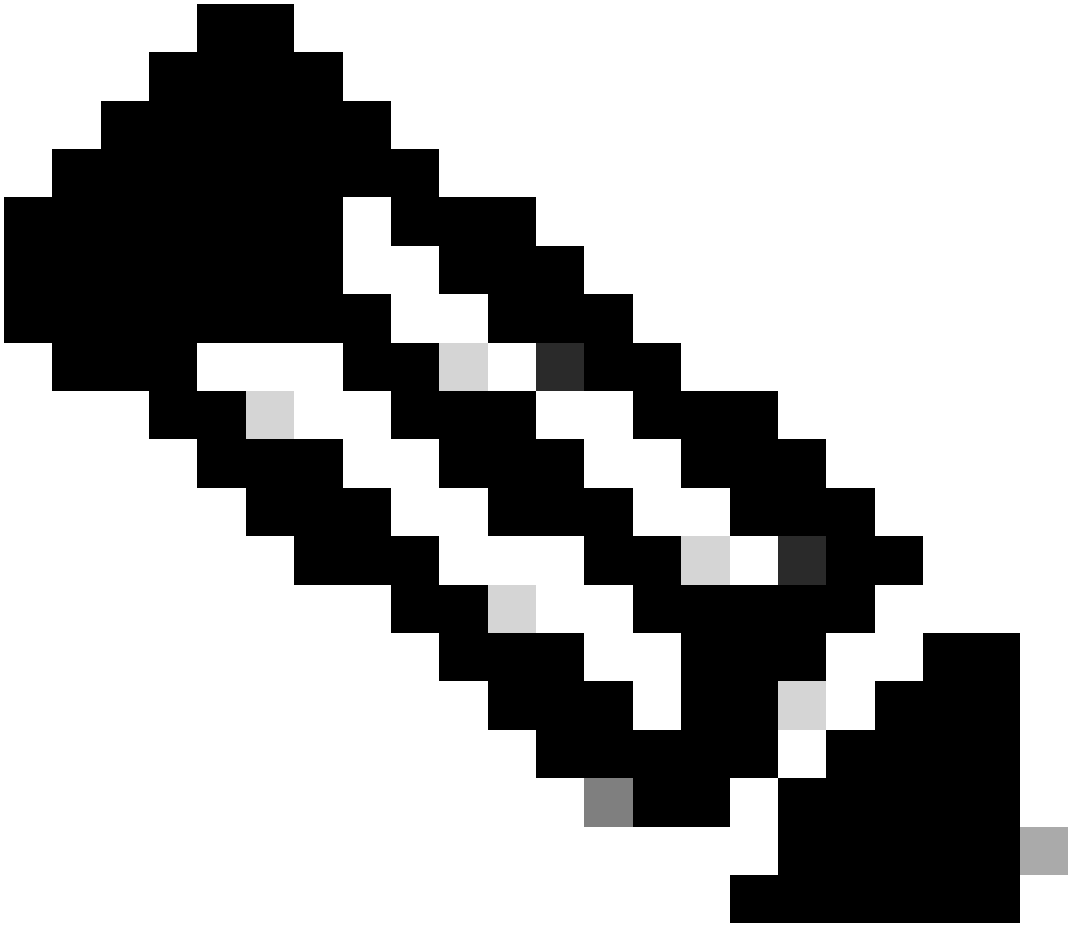
2. Vérifiez la connectivité de base

Vérifiez que le périphérique peut accéder (et ouvrir le port TCP) à tools.cisco.com (en cas d'accès direct) ou au serveur sur site Cisco Smart Software Manager :

<#root>

```
#show run all | in destination address http

  destination address http

https://tools.cisco.com

/its/service/oddce/services/DDCEService
!
! check connectivity
!

#telnet tools.cisco.com 443 /source-interface gi0/0

Trying tools.cisco.com (x.x.x.x, 443)... Open
[Connection to tools.cisco.com closed by foreign host]
```

Si ces commandes ne fonctionnent pas, vérifiez à nouveau vos règles de routage, votre interface source et vos paramètres de pare-feu.



Remarque : le protocole HTTP (TCP/80) est déconseillé et le protocole recommandé est HTTPS (TCP/443).

Reportez-vous à la section : 3. Considérations et mises en garde dans ce document pour obtenir des instructions supplémentaires sur la configuration des détails DNS et HTTP.

3. Vérifiez les paramètres de licence Smart

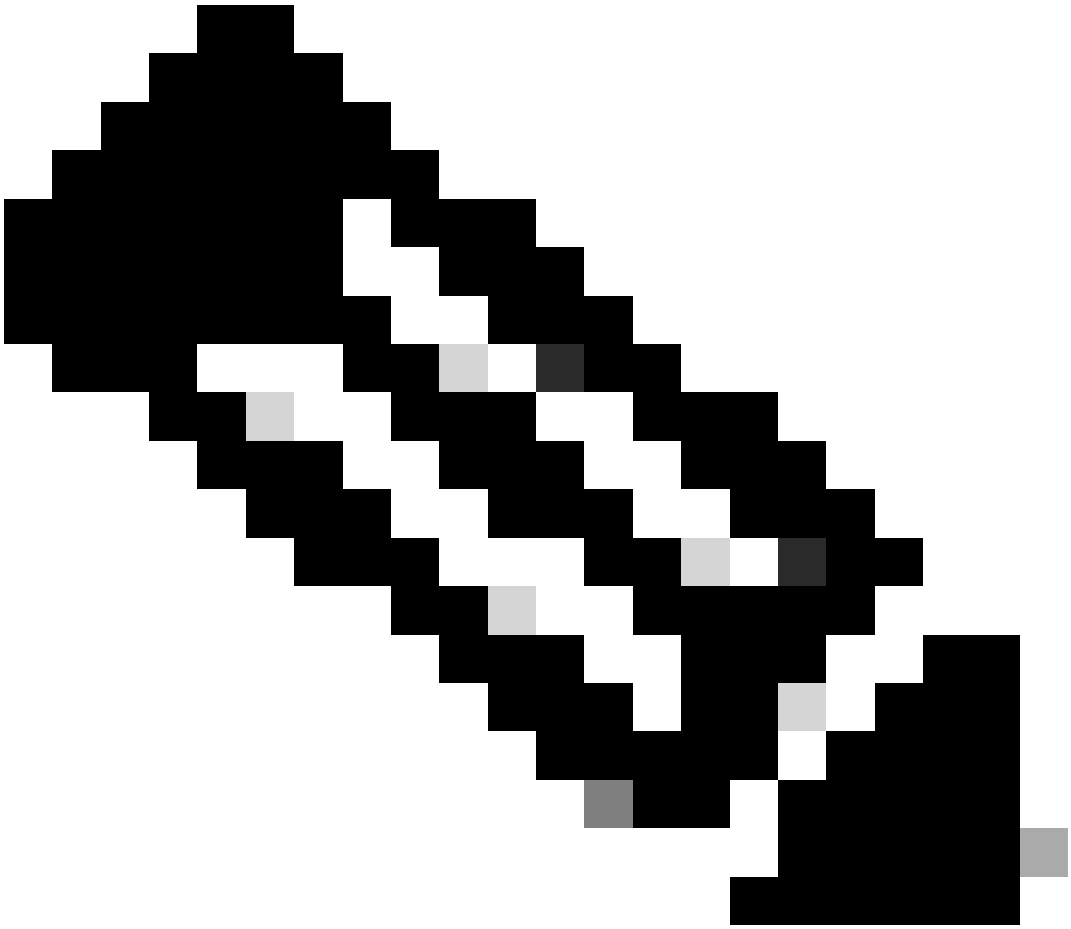
Collecter le résultat de :

```
#show tech-support license
```

et valider la configuration/les journaux collectés (joignez cette sortie au cas où vous décideriez d'ouvrir le dossier du centre d'assistance technique Cisco pour une étude plus approfondie).

4. Activer les débogages

Activez ces débogages pour collecter des informations supplémentaires sur le processus de gestion des licences Smart.



> Remarque : après avoir activé les débogages, vous devez essayer d'enregistrer la licence à nouveau via CLi comme mentionné au point 4.1.

```
#debug call-home smart-licensing [all | trace | error]
#debug ip http client [all | api | cache | error | main | msg | socket]
```

Pour les débogages internes, activez et lisez les traces binaires :

```
! enable debug
#set platform software trace ios [switch] active R0 infra-sl debug
```

```
!
! read binary traces infra-sl process logs
#show platform software trace message ios [switch] active R0
```

Scénarios de défaillance courants

Cette section décrit quelques scénarios de défaillance courants pouvant survenir pendant ou après l'enregistrement d'un périphérique Cisco :

Scénario #1 : Enregistrement du commutateur « Motif de l'échec : produit déjà enregistré »

Extrait de « show license all » :

Inscription :

État : UNREGISTERED - REGISTRATION FAILED

Fonctionnalité d'exportation contrôlée : non autorisée

Enregistrement initial : ÉCHEC le 22 octobre 2018 à 14:25:31 HNE

Raison de l'échec : produit déjà enregistré

Prochaine tentative d'inscription : Oct 22 14:45:34 2018 EST

Étapes suivantes :

- Le périphérique Cisco doit être à nouveau enregistré.

- Si le périphérique Cisco apparaît dans le CSSM, le paramètre force doit être utilisé (c'est-à-dire, license smart register idtoken <TOKEN> force).

Remarque : la raison de l'échec peut également apparaître comme suit :
- Motif de l'échec : le produit <X> et le sudi contenant udiSerialNumber:<SerialNumber>,udiPid:<Product> ont déjà été enregistrés.
- Motif de l'échec : l'instance de produit existante a une consommation et l'indicateur Force est False

---

Scénario #2 : Enregistrement du commutateur « Échec Motif : Votre demande n'a pas pu être traitée pour le moment. Veuillez réessayer"

Extrait de « show license all » :

Inscription :

État : INSCRIPTION - INSCRIPTION EN COURS

Fonctionnalité d'exportation contrôlée : non autorisée

Inscription initiale : ÉCHEC le 24 octobre 2018 à 15:55:26 HNE

Raison de l'échec : votre demande n'a pas pu être traitée pour le moment. Veuillez réessayer

Prochaine tentative d'inscription : Oct 24 16:12:15 2018 EST

Étapes suivantes :

- Activez les débogages comme indiqué dans la section 4 pour obtenir plus d'informations sur le problème.

- Générez un nouveau jeton dans CSSM dans votre licence Smart et essayez à nouveau.

Scénario #3 : Motif de l'échec "La date 1526135268653 du périphérique est décalée au-delà de la limite de tolérance autorisée

Extrait de « show license all » :

Inscription :

État : INSCRIPTION - INSCRIPTION EN COURS

Fonctionnalité d'exportation contrôlée : non autorisée

Inscription initiale : ÉCHEC le 11 novembre 17:55:46 2018 HNE

Raison de l'échec : {"horodatage":["La date du périphérique '1526135268653' est décalée au-delà de la limite de tolérance autorisée."]}

Prochaine tentative d'inscription : Nov 11 18:12:17 2018 EST

Journaux visibles :

%PKI-3-CERTIFICATE_INVALID_NOT_YET_VALID : la validation de la chaîne de certificats a échoué. Le certificat (numéro de série : XXXXXX) n'est pas encore valide. La période de validité commence le 2018-12-12:43Z

Étapes suivantes :

- Vérifiez que l'horloge du périphérique Cisco indique l'heure correcte (show clock).

- Configurez le protocole NTP (Network Time Protocol), si possible, pour vous assurer que l'horloge est correctement réglée.

- Si le protocole NTP n'est pas possible, vérifiez que l'horloge manuellement définie (clock set) est correcte (show clock) et configurée en tant que source horaire approuvée en vérifiant que clock calendar-valid est configurée

Remarque : par défaut, l'horloge système n'est pas fiable. La valeur Clock Calendar-valid est requise.

Scénario #4 : Enregistrement du commutateur « Motif de l'échec : transport de communication non disponible ».

Extrait de « show license all » :

Inscription : état : NON INSCRIT - ÉCHEC DE L'INSCRIPTION

Fonctionnalité D'Exportation Contrôlée : Non Autorisée

Inscription initiale : ÉCHEC le 09 mars 21:42:02 2019 CST

Raison de l'échec : transport de communication non disponible.

Journaux visibles :

%CALL_HOME-3-CALL_HOME_FAILED_TO_ENABLE : échec de l'activation de call-home à partir de Smart Agent pour les licences : échec de l'activation de smart call home en raison d'un profil utilisateur actif existant. Si vous utilisez un profil utilisateur autre que le profil CiscoTAC-1 pour envoyer des données au serveur SCH dans Cisco, entrez reporting smart-licensing-data en mode profil pour configurer ce profil pour la licence Smart. Pour plus d'informations sur SCH, consultez le site http://www.cisco.com/go/smartcallhome
%SMART_LIC-3-AGENT_REG_FAILED : échec de Smart Agent pour l'enregistrement de licence avec Cisco Smart Software Manager ou satellite : transport de communication non disponible.
%SMART_LIC-3-COMM_FAILED : échec des communications avec Cisco Smart Software Manager ou satellite : transport des communications non disponible.

Étapes suivantes :

- Vérifiez que call-home est activé avec service call-home dans la sortie show running-config du périphérique Cisco.

- Assurez-vous que le profil call-home correct est actif.

- Vérifiez que les données Smart-licensing-data de rapport sont configurées sous le profil call-home actif.

Scénario #5 : Autorisation de licence de commutateur « Raison de l'échec : échec de l'envoi du message HTTP Call Home ».

Extrait de « show license all » :

Autorisation de licence :

État : NON CONFORME le 26 juillet 09:24:09 2018 UTC

Dernière tentative de communication : ÉCHEC le 02 août 14:26:23 2018 UTC

Raison de l'échec : échec de l'envoi du message HTTP Call Home.

Prochaine tentative de communication : Aug 02 14:26:53 2018 UTC

Date limite de communication : 25 oct. 09:21:38 2018 UTC

Les journaux possibles s'affichent :

%CALL_HOME-5-SL_MESSAGE_FAILED : échec de l'envoi du message Smart Licensing à : https://<ip>/its/service/oddce/services/DDCEService (ERR 205 : requête abandonnée)

%SMART_LIC-3-COMM_FAILED : échec des communications avec Cisco Smart Software Manager ou le satellite : échec de l'envoi du message HTTP Call Home.

%SMART_LIC-3-AUTH_RENEW_FAILED : Renouvellement de l'autorisation avec Cisco Smart Software Manager ou satellite : erreur d'envoi du message de communication pour le PID d'udi : XXX, SN : XXX

Étapes suivantes :

- Vérifiez que le périphérique Cisco peut envoyer une requête ping à tools.cisco.com.

- Si DNS n'est pas configuré, configurez un serveur DNS ou une instruction ip host pour l'adresse IP locale nslookup pour tools.cisco.com.

- Essayez d'établir une connexion Telnet entre le périphérique Cisco et tools.cisco.com sur le port TCP 443 (port utilisé par HTTPS).

- Vérifiez que l'interface source du client HTTP est définie et correcte.

- Vérifiez que l'URL/IP du profil call home est correctement définie sur le périphérique Cisco via show call-home profile all.

- Vérifiez que la route IP pointe vers le saut suivant correct.

- Assurez-vous que le port TCP 443 n'est pas bloqué sur le périphérique Cisco, le chemin vers Smart Call Home Server ou Cisco Smart Software Manager sur site (satellite).

- Vérifiez que l'instance VRF (Virtual Routing and Forwarding) correcte est configurée sous Call-Home, le cas échéant.

Scénario #6 : Motif de l'échec « Champ Numéro de série du certificat ID manquant ; Champ Numéro de série du certificat signature manquant ; Les données signées et le certificat ne correspondent pas » Journal

Ce comportement se produit lorsque vous travaillez avec un serveur CSSM sur site dont le certificat de chiffrement a expiré, comme indiqué dans le bogue Cisco ayant l'ID CSCvr41393. Ce comportement est attendu, car le CSSM sur site doit être autorisé à synchroniser et à renouveler son certificat afin d'éviter un problème de synchronisation de certification avec tout périphérique en cours d'enregistrement.

Extrait de « show license all » :

Inscription :
État : NON ENREGISTRÉ
Compte Smart : exemple de compte
Fonctionnalité d'exportation contrôlée : AUTORISÉE

Autorisation de licence :
État : MODE D'ÉVALUATION
Période d'évaluation restante : 65 jours, 18 heures, 43 minutes, 0 secondes

Journaux visibles :

Cette erreur apparaît sous show logging ou show license eventlog :
SAVET_DEREGISTER_STATUS msgStatus="LS_INVALID_DATA" error="Champ de numéro de série du certificat ID manquant ; Champ de numéro de série du certificat signature manquant ; Les données signées et le certificat ne correspondent pas"

Étapes suivantes :

- Vérifiez que le périphérique Cisco dispose d'une connectivité IP au serveur sur site CSSM.
- Si vous utilisez HTTPS, vérifiez que le nom C de certification est utilisé dans la configuration call-home des périphériques.
- Si un serveur DNS n'est pas disponible pour résoudre le nom C de certification, configurez une instruction ip host statique pour mapper le nom de domaine et l'adresse IP.

- Vérifiez que l'état du certificat sur CSSM sur site est toujours valide.
- Si le certificat CSSM sur site a expiré, utilisez l'une des solutions de contournement documentées dans l'ID de bogue Cisco CSCvr41393

Remarque : par défaut, HTTPS effectue un contrôle d'identité du serveur lors de la connexion SSL pour vérifier que l'URL ou l'IP est identique au certificat fourni par le serveur. Cela peut entraîner des problèmes lors de l'utilisation d'adresses IP au lieu d'une entrée DNS si le nom d'hôte et l'adresse IP ne correspondent pas. Si DNS n'est pas possible ou si une instruction ip host statique est utilisée, aucun contrôle d'identité de serveur sécurisé http ne peut être configuré pour désactiver ce contrôle de certification.

Scénario #7 : Autorisation de licence de commutateur « Motif de l'échec : attente de la réponse »

Extrait de « show license all » :

Autorisation de licence :
État : NON CONFORME le 26 juillet 09:24:09 2018 UTC
Dernière tentative de communication : EN ATTENTE le 02 août 14:34:51 2018 UTC
Motif de l'échec : attente de réponse
Prochaine tentative de communication : Aug 02 14:53:58 2018 UTC
Date limite de communication : 25 oct. 09:21:39 2018 UTC

Les journaux possibles s'affichent :

%PKI-3-CRL_FETCH_FAIL : échec de la récupération de la liste de révocation de certificats pour le point de confiance SLA-TrustPoint Raison : échec de la sélection du socket. Timeout : 5 (Connection timed out)
%PKI-3-CRL_FETCH_FAIL : échec de la récupération de la liste de révocation de certificats pour le point de confiance SLA-TrustPoint Raison : échec de la sélection du socket. Timeout : 5 (Connection timed out)

Étapes suivantes :

- Pour corriger ce problème, le SLA-TrustPoint doit être configuré sur none dans la configuration en cours

show running-config

<omis>

crypto pki trustpoint SLA-TrustPoint

revocation-check none

Qu'est-ce qu'une CRL ?

Une liste de révocation de certificats est une liste de certificats révoqués. La liste de révocation de certificats est créée et signée numériquement par l'autorité de certification qui a émis les certificats à l'origine. La liste de révocation de certificats contient les dates d'émission et d'expiration de chaque certificat. Pour plus d'informations sur les LCR, cliquez ici.

Scénario #8 : état de la licence « NON CONFORME »

Extrait de « show license all » :

Autorisation de licence :
État : NON CONFORME le 26 juillet 09:24:09 2018 UTC
Dernière tentative de communication : EN ATTENTE le 02 août 14:34:51 2018 UTC
Motif de l'échec : attente de réponse
Prochaine tentative de communication : Aug 02 14:53:58 2018 UTC
Date limite de communication : 25 oct. 09:21:39 2018 UTC

Les journaux possibles s'affichent :

%SMART_LIC-3-OUT_OF_COMPLIANCE : un ou plusieurs droits ne sont pas conformes.

Étapes suivantes :

- Vérifiez si le jeton du compte Smart Virtual approprié a été utilisé.

- Vérifiez le nombre de licences disponibles ici.

Scénario #9 : Autorisation de licence de commutateur « Motif de l'échec : les données et la signature ne correspondent pas »

Extrait de « show license all » :

Autorisation de licence :

Statut : AUTORISÉ le 12 mars 09:17:45 2020 HAE

Dernière tentative de communication : ÉCHEC le 12 mars 09:17:45 2020 EDT

Raison de l'échec : les données et la signature ne correspondent pas

Prochaine tentative de communication : mars 12 09:18:15 2020 EDT

Date limite de communication : 09 mai 21:22:43 2020 EDT

Les journaux possibles s'affichent :

%SMART_LIC-3-AUTH_RENEW_FAILED : Renouvellement de l'autorisation avec Cisco Smart Software Manager (CSSM) : erreur reçue de Smart Software Manager : les données et la signature ne correspondent pas pour l'ID d'audit PID : C9000, SN : XXXXXXXXXXX

Étapes suivantes :

- Désenregistrez le commutateur avec la licence smart deregister.

- Enregistrez ensuite le commutateur à l'aide d'un nouveau jeton avec la licence smart register idtoken <TOKEN> force.

Références

1) Page d'accueil de Cisco Smart Licensing

2) Communauté Cisco - Formations à la demande.

3) Compte Smart - portail de gestion : licences logicielles Smart

4) Compte Smart - créer de nouveaux comptes : comptes Smart

5) Guide de configuration (exemple) - System Management Configuration Guide, Cisco IOS XE Fuji 16.9.x (commutateurs Catalyst 9300)

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.