Configurer le & Dépannage des licences unifiées et Smart Catalyst 9800 avec SLUP

Table des matières

Introduction

Ce document décrit comment configurer et dépanner Smart Licensing Using Policy (SLUP) sur le WLC Catalyst 9800.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Politique d'utilisation des licences Smart (SLUP)
- Contrôleur LAN sans fil (WLC) Catalyst 9800

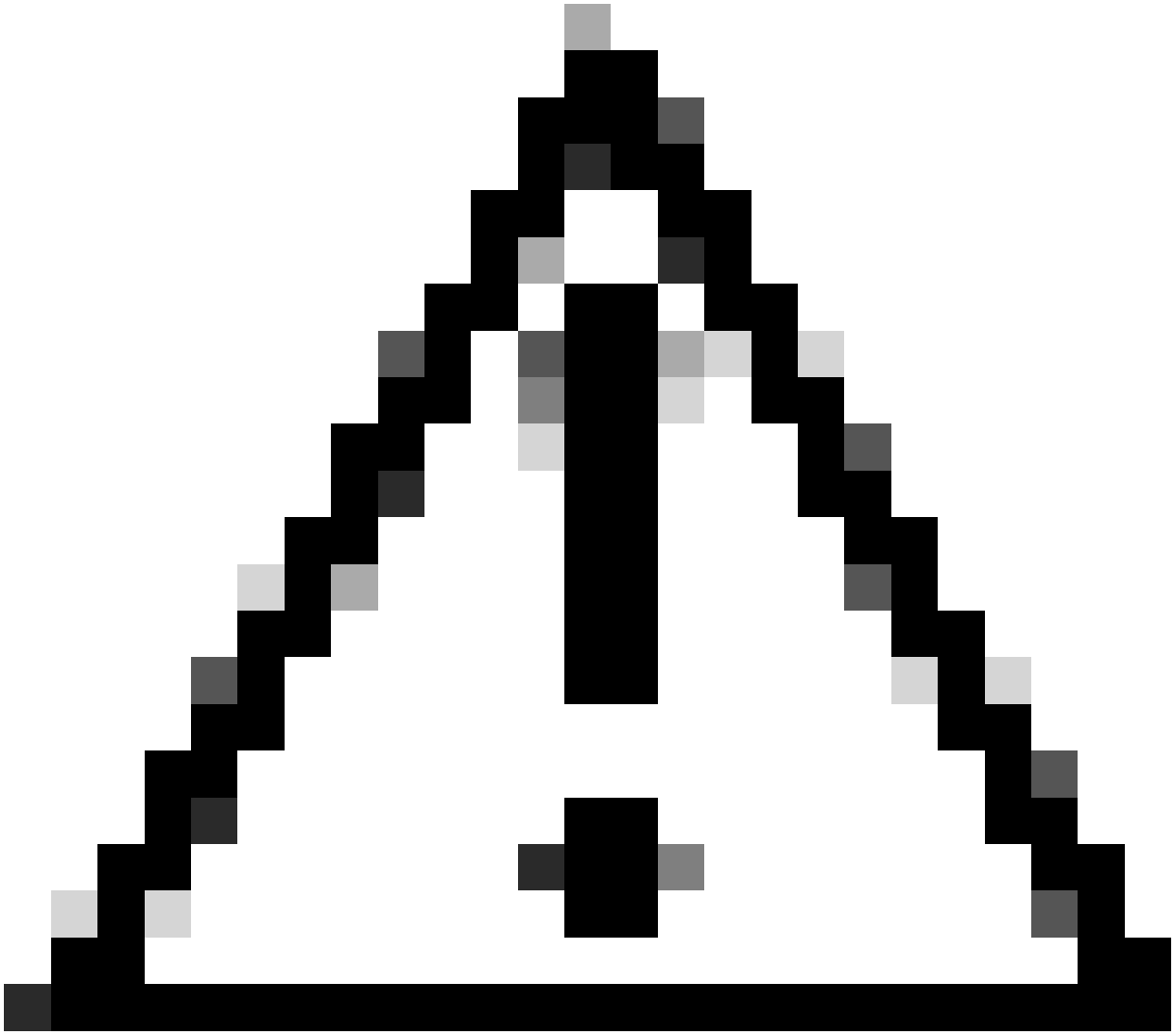
- Abonnement Cisco Networking

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

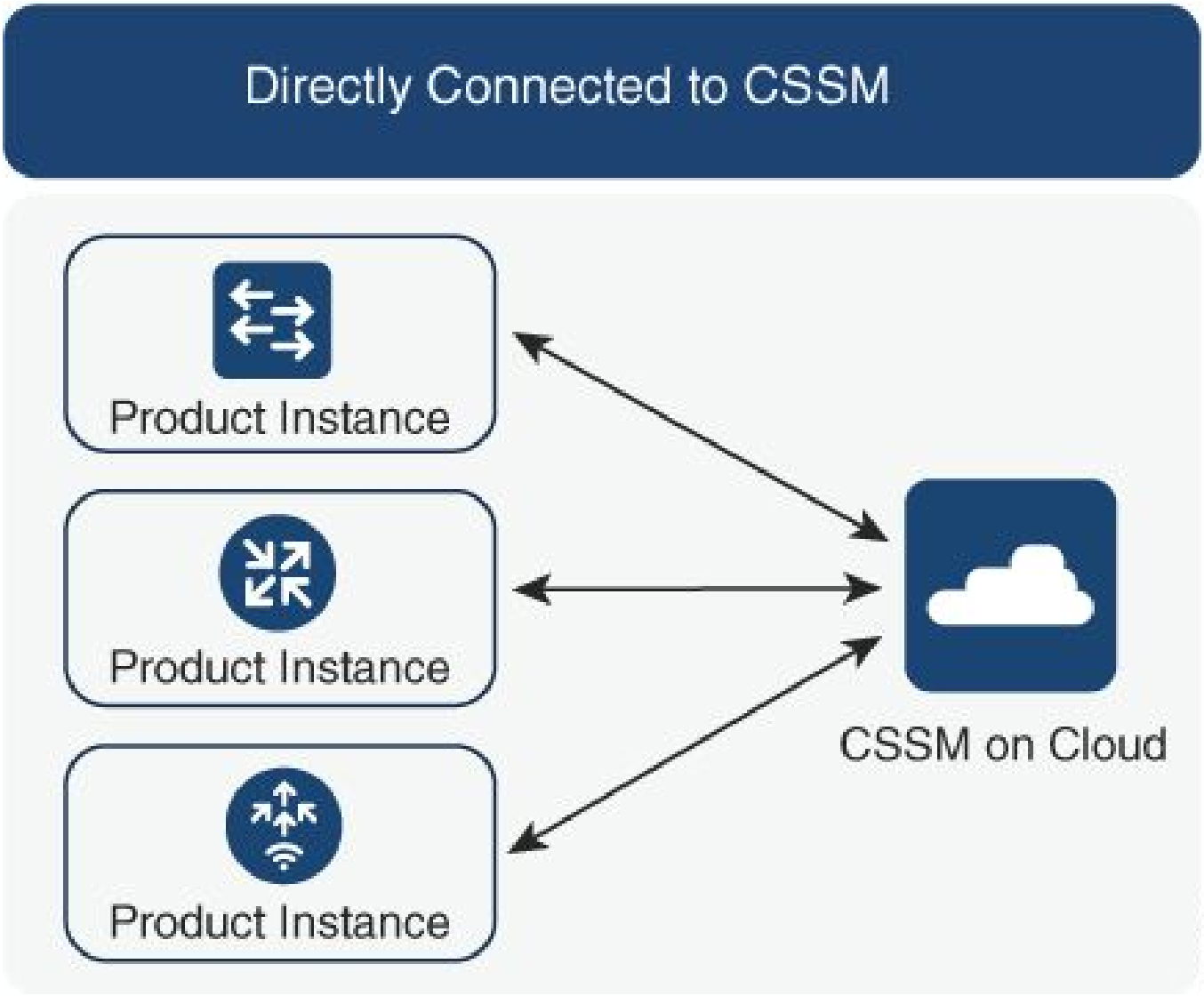
Informations générales



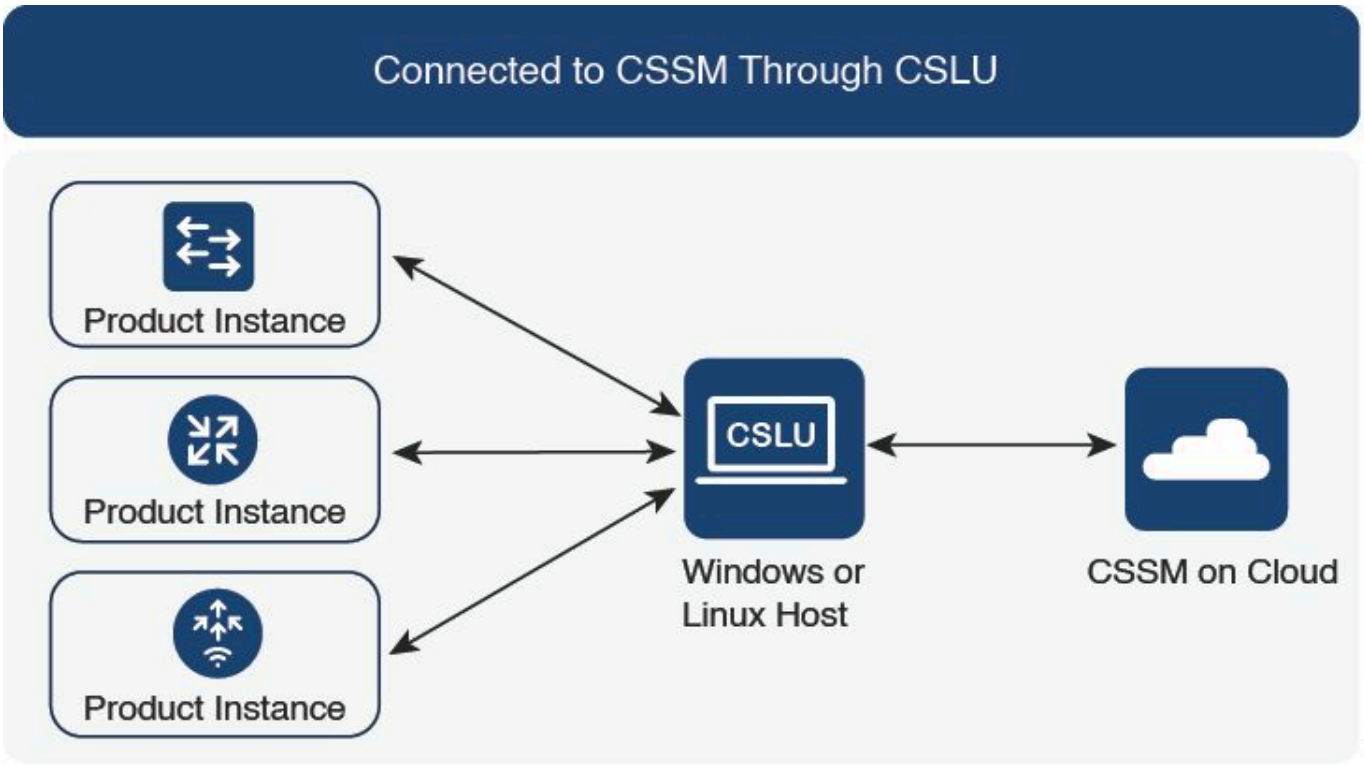
Mise en garde : Les notes de cet article contiennent des suggestions utiles ou des références à des éléments non couverts dans le document. Il est recommandé de lire chaque note.

1. Connexion directe au cloud Cisco Smart Software Manager (cloud CSSM)
2. Connecté à CSSM via CSLU (Cisco Smart License Utility Manager)
3. Connecté à CSSM via Smart Software Manager sur site (SSM sur site)

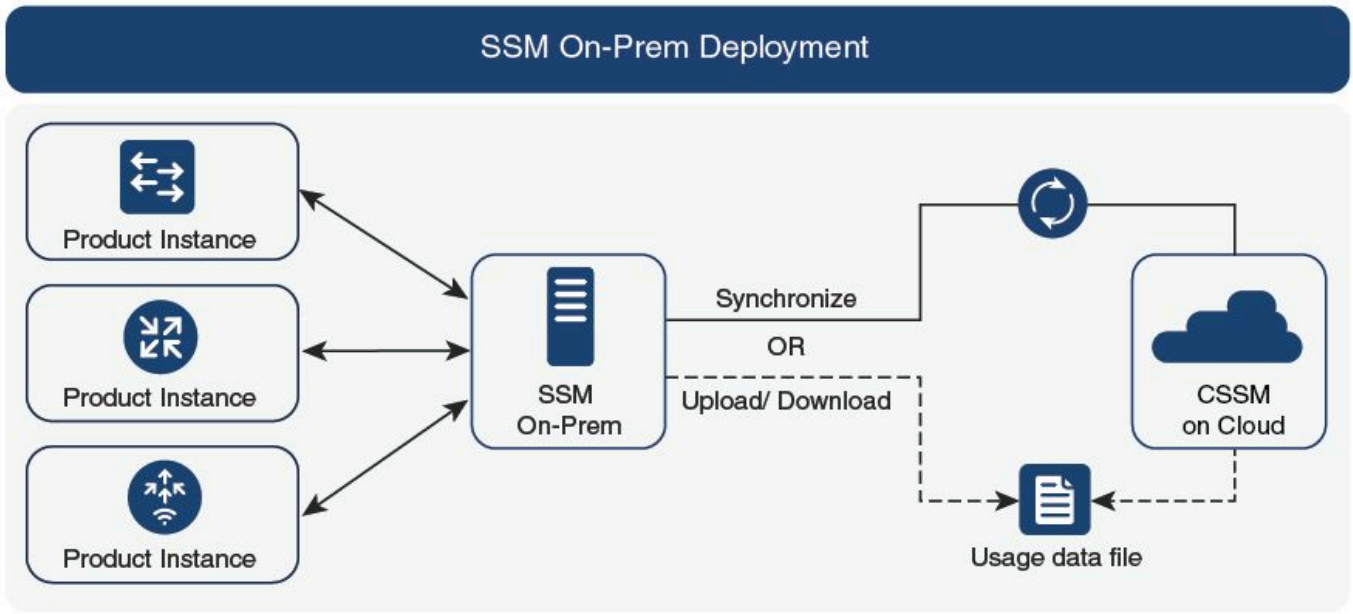
Cet article ne couvre pas tous les scénarios de licences Smart sur Catalyst 9800, référez-vous au Guide de configuration de licences Smart à l'aide de politiques pour plus d'informations. Cependant, cet article fournit une série de commandes utiles pour dépanner les problèmes de connexion directe, de CSLU et de gestion intelligente des licences SSM sur site à l'aide de la politique sur le Catalyst 9800.



Option 1. Connexion directe aux serveurs cloud Cisco Smart Licensing (CSSM)



Option 2. Connexion via CSLU



Option 3. Connexion via Smart Software Manager sur site (SSM sur site)

Remarque : Toutes les commandes mentionnées dans cet article s'appliquent uniquement aux WLC qui exécutent la version 17.3.2 ou ultérieure.

Licences unifiées, application et SLUP

La licence unifiée, disponible dans Cisco Networking Subscriptions, introduit l'application de la licence aux clients sur site.

- IOS XE 17.15.2 (décembre 2024) a été la première version prise en charge pour les licences unifiées et a introduit des rapports de licence par périphérique et l'état de conformité.
- Les futures versions d'IOS XE introduisent l'application Jour 0 pour les points d'accès sans licence et l'application Jour N pour les périphériques dont les licences ont expiré. sur les périphériques non conformes, l'application a lieu lorsque l'image logicielle est mise à jour.

Il est essentiel de suivre les étapes de ce guide pour vous assurer que vos périphériques sont configurés correctement à l'aide du protocole SLUP, afin qu'ils ne soient pas soumis à l'application lors de la mise à niveau de l'image logicielle IOS XE.

Vérification de la conformité AP sur Unified Licensing

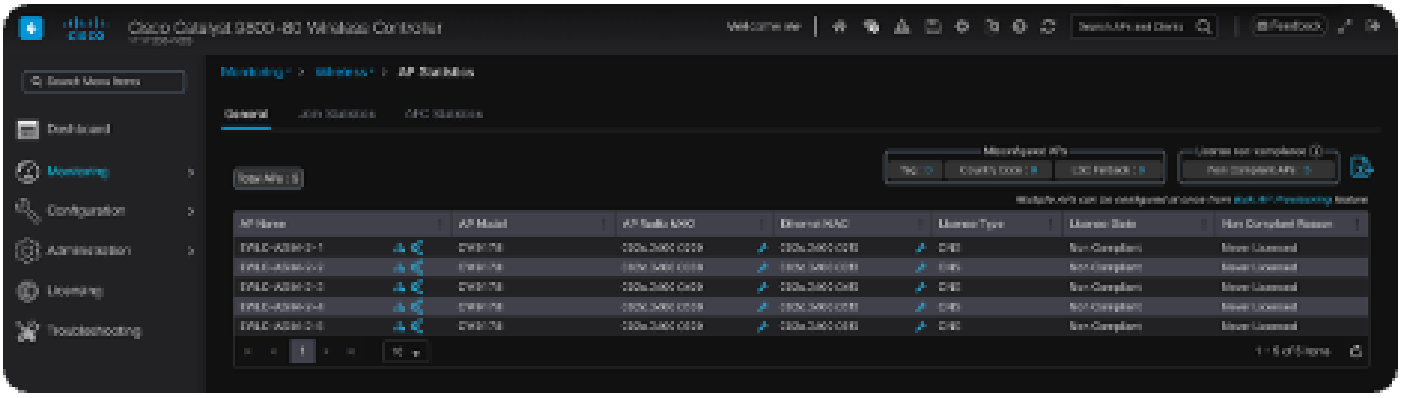


Figure 1 : Conformité AP de l'interface utilisateur Web (non conforme)

Les informations relatives à la conformité des points d'accès sont disponibles sur le contrôleur (tableau de bord Meraki, Catalyst Center 2.3.7.9) et sur le périphérique (interface utilisateur Web, CLI).

La Figure 1 présente un exemple d'informations de conformité AP sur l'interface utilisateur Web. Les points d'accès non conformes ont un état de licence non conforme, avec un raisonnement à condition que le point d'accès soit « Jamais sous licence ».

Une fois le SLUP correctement configuré, vos AP reflètent un état de conformité mis à jour.

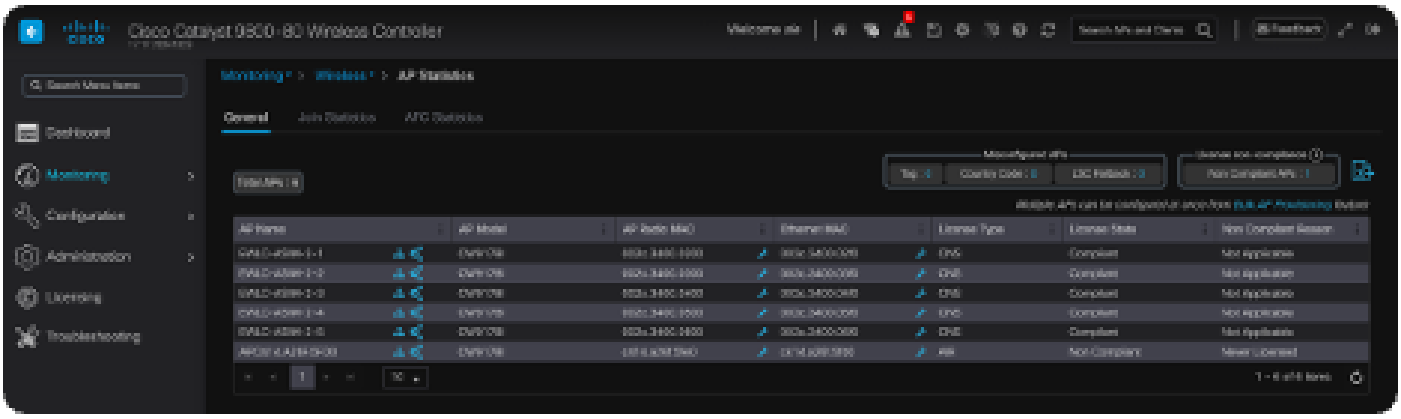


Figure 1 : Compatibilité AP avec interface utilisateur Web (conforme)

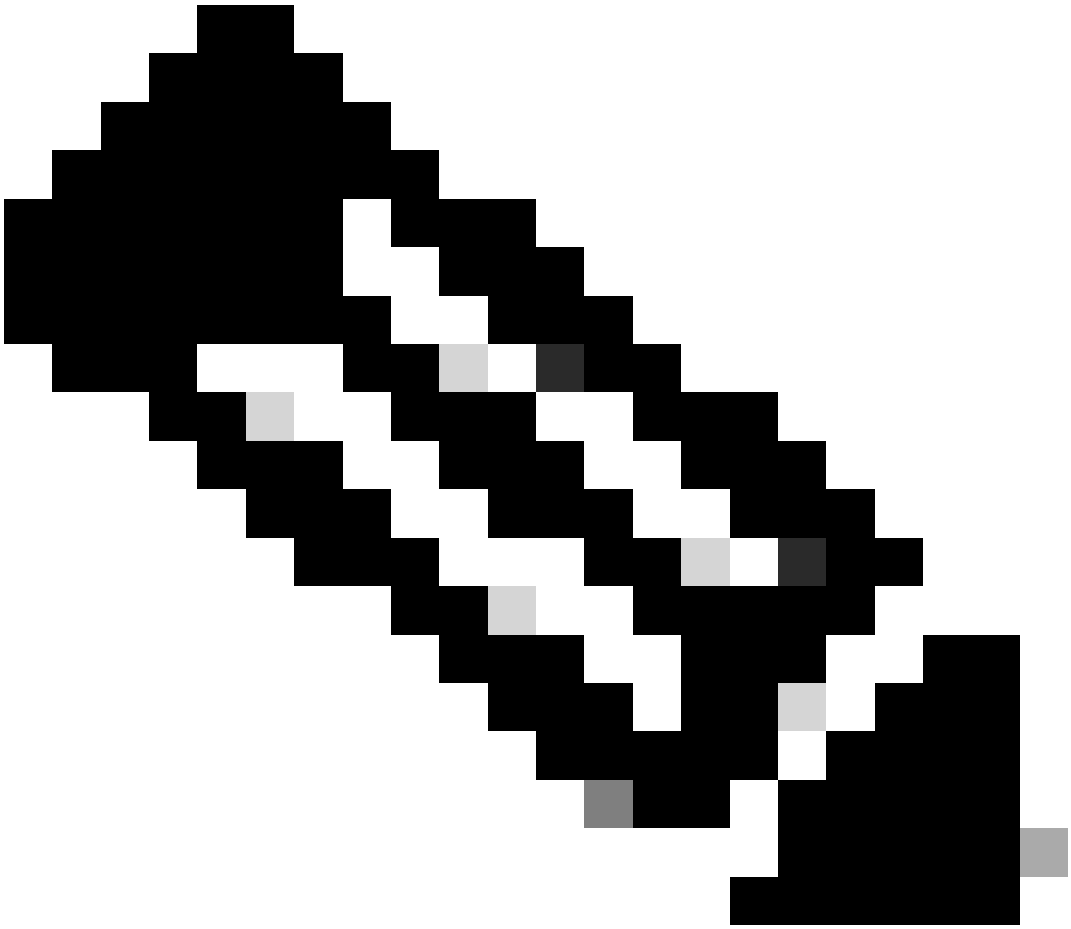
Remarque : si vous avez correctement configuré le SLUP et que l'état Non conforme est toujours

affiché sur vos points d'accès, vérifiez que vous avez acheté suffisamment de licences et que ces licences ont été déposées dans le compte Smart (SA) et le compte virtuel (VA) corrects.

Licences traditionnelles et SLUP

La fonctionnalité Smart Licensing Using Policy a été introduite dans le Catalyst 9800 avec la version de code 17.3.2. La version initiale 17.3.2 ne contient pas le menu de configuration SLUP dans l'interface utilisateur Web du WLC, qui a été introduite avec la version 17.3.3. Le SLUP diffère des licences Smart traditionnelles de plusieurs manières :

- WLC communique désormais avec CSSM via le domaine smartreceiver.cisco.com, au lieu du domaine tools.cisco.com.
- Au lieu de s'enregistrer, le WLC établit maintenant la confiance avec le CSSM ou le SSM sur site.
- Les commandes CLI ont été légèrement modifiées.
- Il n'y a plus de réservation de licences Smart (SLR). Au lieu de cela, vous pouvez régulièrement signaler votre utilisation manuellement.



Avertissement : Si vous utilisez un contrôleur sans fil Cisco Catalyst 9800-CL, assurez-vous que vous êtes familiarisé avec la condition ACK obligatoire qui commence par Cisco IOS® XE Cupertino 17.7.1. Reportez-vous à la section RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller.

Configuration

CSSM Direct Connect

Une fois que le jeton a été créé sur le CSSM, afin d'établir la confiance, ces commandes doivent être exécutées :

Remarque : Jeton max. Le nombre d'utilisations doit être d'au moins 2 dans un cas de WLC dans HA SSO.

```
configure terminal
ip http client source-interface



ip http client secure-trustpoint



license smart transport smart
license smart url default
exit
write memory
terminal monitor
license smart trust idtoken


          all force
```

- La commande ip http client source-interface spécifie l'interface de couche 3 à partir de laquelle les paquets associés à la licence vont provenir
- La commande ip http client secure-trustpoint spécifie quel trustpoint/certificate est utilisé pour la communication CSSM. Le nom du point de confiance peut être trouvé en utilisant la commande show crypto pki trustpoints. Il est recommandé d'utiliser un certificat auto-signé

TP-self-signed-xxxxxxxx ou un certificat installé par le fabricant (également appelé MIC, disponible uniquement sur les modèles 9800-40, 9800-80 et 9800-L), généralement appelé CISCO_IDEVID_SUDI.

- La commande Terminal monitor permet au WLC d'imprimer les journaux sur la console et de confirmer que la confiance a été établie avec succès. Il peut être désactivé à l'aide de terminal no monitor.
- Le mot clé all dans la dernière commande indique à tous les WLC dans le cluster HA SSO d'établir la confiance avec le CSSM.
- Le mot clé force indique au WLC de remplacer n'importe laquelle des approbations précédemment établies et d'en tenter une nouvelle.

Remarque : Si l'approbation n'est pas établie, le 9800 réessaie 1 minute plus tard après l'exécution de la commande, puis ne réessaie pas pendant un certain temps. Entrez à nouveau la commande token pour forcer un nouvel établissement de confiance.

Connecté à CSLU

Cisco Smart License Utility Manager (CSLU) est une application Windows (également disponible sur Linux) qui permet aux clients d'administrer les licences et les instances de produit associées depuis leurs locaux, au lieu de devoir connecter directement leurs instances de produit compatibles avec la licence Smart à Cisco Smart Software Manager (CSSM).

Cette section couvre uniquement la configuration sans fil 9800. Il existe d'autres étapes à effectuer pour configurer la licence avec CSLU (telles que l'installation de CSLU, la configuration du logiciel CSLU, etc.), qui est traitée dans les Guides de configuration .Si vous souhaitez mettre en oeuvre une méthode de communication initiée par une instance de produit ou par CSLU, ou terminer la séquence de tâches correspondante.

Initié par une instance de produit

1. Garantir l'accessibilité du réseau du contrôleur à CSLU
2. Assurez-vous que le type de transport est défini sur cslu :

```
(config)#license smart transport cslu
(config)#exit
#copy running-config startup-config
```

3. Si vous voulez que CSLU soit découvert par le contrôleur, vous devez effectuer l'action. Si vous voulez que CSLU soit découvert à l'aide du DNS, aucune action n'est requise. Si vous souhaitez le découvrir à l'aide d'une URL, saisissez la commande suivante :

```
(config)#license smart url cslu http://

         :8182/cslu/v1/pi
(config)#exit
```

```
#copy running-config startup-config
```

initié par CSLU

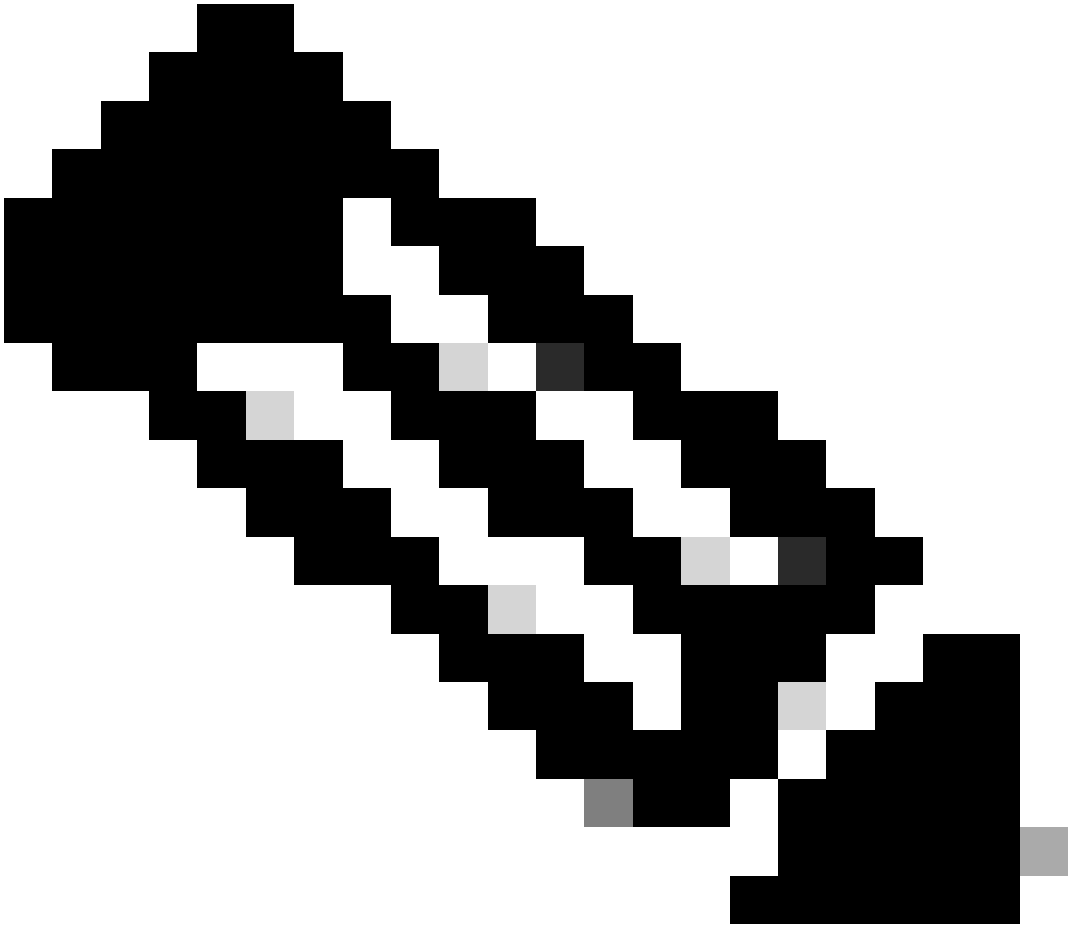
Lorsque vous configurez une communication initiée par CSLU, la seule action nécessaire est de vérifier et de garantir l'accessibilité du réseau vers CSLU à partir du contrôleur.

Connecté à SSM On-prem

La configuration avec le module SSM sur site est assez similaire à la connexion directe. On-prem doit exécuter la version 8-202102 ou ultérieure. Pour les versions SLUP (17.3.2 et ultérieures), il est conseillé d'utiliser l'URL CSLU et le type de transport. L'URL peut être obtenue à partir de l'interface WebUI sur site sous **Smart Licensing > Inventory > <Virtual Account> > General** section.

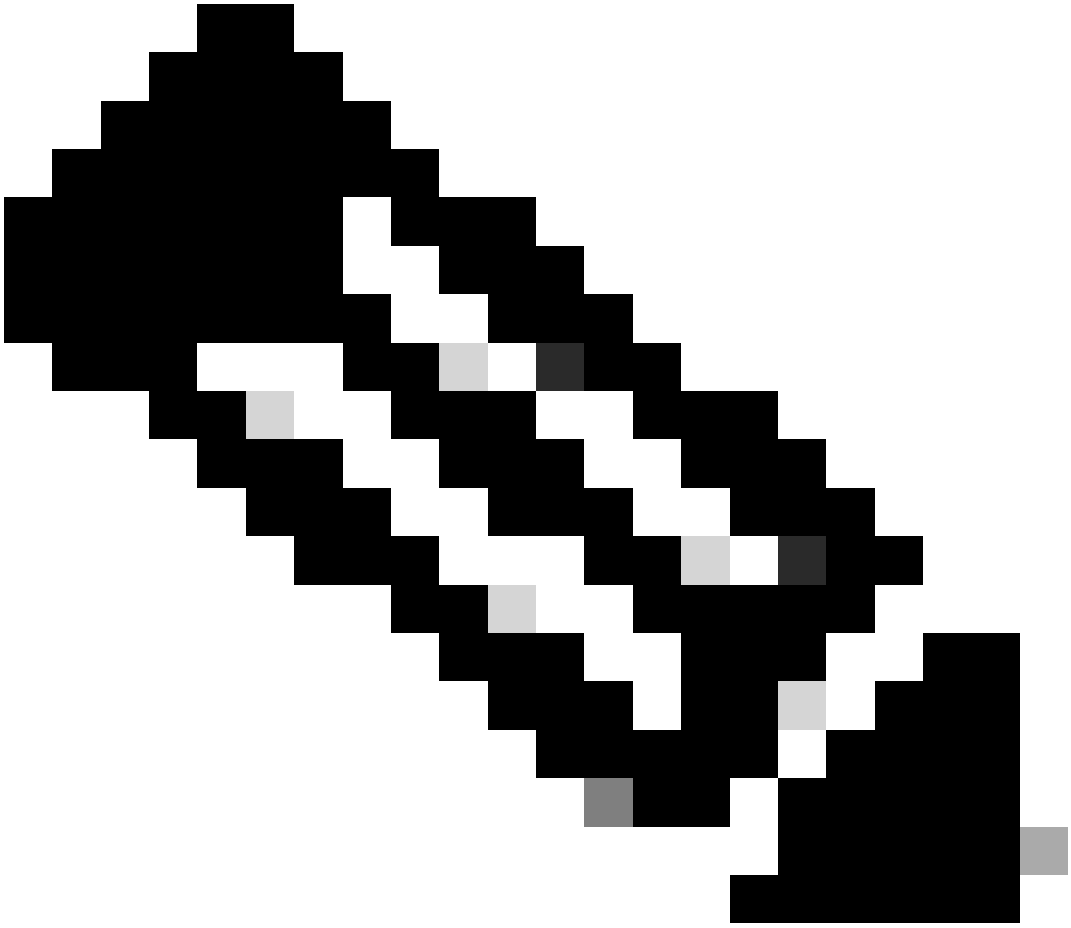
```
configure terminal
 ip http client source-interface



 ip http client secure-trustpoint



 license smart transport cslu
 license smart url cslu http://


         /cslu/v1/pi/


           (see previous paragraph on how to get exact URL)
 crypto pki trustpoint SLA-TrustPoint
  revocation-check none
 exit
write memory
terminal monitor
```

Le module SSM sur site ne nécessite pas l'utilisation d'un jeton de confiance.



Remarque : Si vous recevez le message, %PKI-3-CRL_FETCH_FAIL: Échec de la récupération de la liste de révocation de certificats pour trustpoint SLA-TrustPoint, car vous n'avez pas configuré revocation-check none sous SLA-TrustPoint. Il s'agit du point de confiance utilisé pour les licences Smart. Dans le cas d'un certificat On-prem, le certificat sur le serveur de licences est le plus souvent un certificat auto-signé pour lequel la vérification de la liste de révocation de certificats n'est pas possible, d'où la nécessité de configurer aucune vérification de révocation.

Configuration de Smart Transport via un proxy HTTPS



Remarque : Les proxies authentifiés ne sont pas encore pris en charge à partir de la version de code 17.9.2. Si vous utilisez des proxies authentifiés dans votre infrastructure, envisagez d'utiliser Cisco Smart License Utility Manager (CSLU), il prend en charge ce type de serveurs.

Pour utiliser un serveur proxy pour communiquer avec CSSM lorsque vous utilisez le mode de transport intelligent, procédez comme suit :

```
configure terminal
  ip http client source-interface



  ip http client secure-trustpoint
```

```
  license smart transport smart
  license smart url default
  license smart proxy address




  license smart proxy port




exit
write memory
terminal monitor
license smart trust idtoken



            all force
```

Fréquence De Communication

L'intervalle de rapport que vous pouvez configurer dans l'interface CLI ou GUI est sans effet.

Le WLC 9800 communique avec CSSM ou Smart Software Manager sur site toutes les 8 heures, quel que soit l'intervalle de rapport configuré via l'interface Web ou l'interface de ligne de commande. Cela signifie que les points d'accès nouvellement joints peuvent apparaître sur le CSSM jusqu'à 8 heures après leur adhésion initiale.

Vous pouvez déterminer la prochaine fois que les licences sont calculées et rapportées avec la commande show license air entities summary. Cette commande ne fait pas partie de la sortie typique show tech ou show license all :

<#root>

WLC#

```
show license air entities summary


Last license report time.....................: 07:38:15.237 UTC Fri Aug 27 2021
Upcoming license report time..................: 15:38:15.972 UTC Fri Aug 27 2021
```

```
No. of APs active at last report.................: 3
No. of APs newly added with last report.........: 0
No. of APs deleted with last report..............: 0
```

Licence Factory Reset

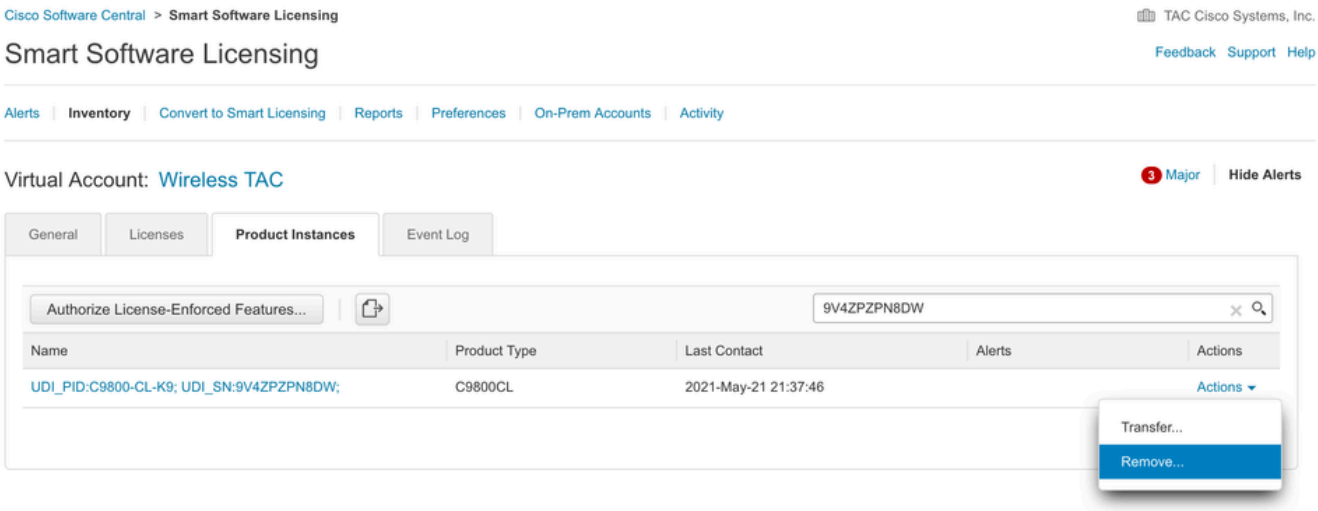
Le WLC du Catalyst 9800 peut avoir toute sa configuration de licence et faire confiance à la réinitialisation d'usine tout en conservant toutes les autres configurations. Cela nécessite un rechargement WLC :

```
WLC-1#license smart factory reset
%Warning: reload required after "license smart factory reset" command
```

Il est important de noter qu'après la réinitialisation d'une usine de licences, vous devez attendre une heure avant de renouveler la licence du WLC au cas où il serait en mode AirGap.

En cas de RMA ou de remplacement de matériel

Si le WLC 9800 doit être remplacé, le nouveau périphérique doit s'enregistrer auprès de CSSM/On-prem Smart Software Manager et il est perçu comme un nouveau périphérique. La libération du nombre d'homologations de l'instrument précédent nécessite une suppression manuelle sous Instances de produit :



Mise à niveau à partir d'un enregistrement de licence spécifique (SLR)

Les versions plus anciennes de WLC, antérieures à 17.3.2, utilisaient une méthode de licence hors ligne spéciale appelée SLR (Specific License Registration). Cette méthode de licence a été déconseillée dans les versions utilisant SLUP (17.3.2 et ultérieures).

Si vous mettez à niveau un contrôleur 9800 qui utilisait SLR vers une version 17.3.2 ou 17.4.1, il

est recommandé de passer à la création de rapports SLUP hors ligne plutôt que de vous fier aux commandes SLR. Enregistrez le fichier RUM d'utilisation des licences et enregistrez-le sur le portail Smart Licensing. Comme le SLR n'existe plus dans les versions récentes, cela indique le nombre correct de licences et libère toute licence inutilisée. Les licences ne sont plus bloquées, mais le nombre exact d'utilisations est indiqué.

Dépannage

Accès Internet, vérifications de port et requêtes ping

Au lieu de l'tools.cisco.com que les licences Smart traditionnelles utilisaient, le nouveau SLUP utilise le domaine smartreceiver.cisco.com pour établir la confiance. Au moment de la rédaction de cet article, ce domaine est résolu en plusieurs adresses IP différentes. Toutes ces adresses ne peuvent pas faire l'objet d'une requête ping. Les requêtes ping ne doivent pas être utilisées comme test d'accessibilité Internet à partir du WLC. Le fait de ne pas pouvoir envoyer de requête ping à ces serveurs ne signifie pas qu'ils ne fonctionnent pas correctement.

Au lieu des requêtes ping, Telnet sur le port 443 doit être utilisé comme test d'accessibilité. Telnet peut être comparé au domaine smartreceiver.cisco.com ou directement aux adresses IP du serveur. Si le trafic n'est pas bloqué, le port doit apparaître comme ouvert dans le résultat :

```
WLC-1#telnet smartreceiver.cisco.com 443
Trying smartreceiver.cisco.com (192.330.220.90, 443)... Open <-------
[Connection to 192.330.220.90 closed by foreign host]
```

Syslog

Si la commande terminal monitor est activée pendant que le jeton est en cours de configuration, le WLC imprime les journaux appropriés dans la CLI. Ces messages peuvent également être obtenus si vous exécutez la commande show logging. Les journaux d'une approbation établie avec succès ressemblent à ceci :

```
WLC-1#license smart trust idtoken <token> all force
Aug 22 12:13:08.425: %CRYPTO_ENGINE-5-KEY_DELETED: A key named SLA-KeyPair has been removed from key st
Aug 22 12:13:08.952: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named SLA-KeyPair has been generated or impor
Aug 22 12:13:08.975: %PKI-6-CONFIGAUTOSAVE: Running configuration saved to NVRAM
Aug 22 12:13:11.879: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was successfully in
```

Journaux d'un WLC sans serveur DNS défini ou avec un serveur DNS qui ne fonctionne pas :

```
Aug 23 09:19:43.486: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart Software Man
```

Dans ce cas, vérifiez qu'un serveur DNS valide est configuré. N'hésitez pas à utiliser toutes les adresses IP de serveur DNS public disponibles :

```
ip name-server
```

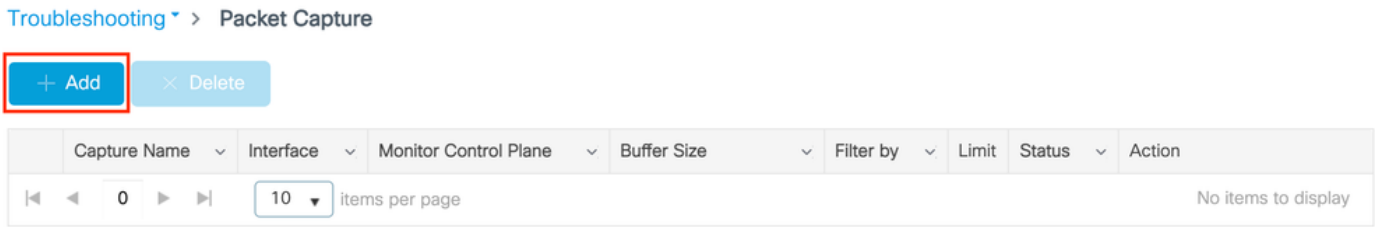
Journaux d'un WLC avec un serveur DNS fonctionnel, mais sans accès à Internet :

```
Aug 23 09:23:30.701: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart Software Man
```

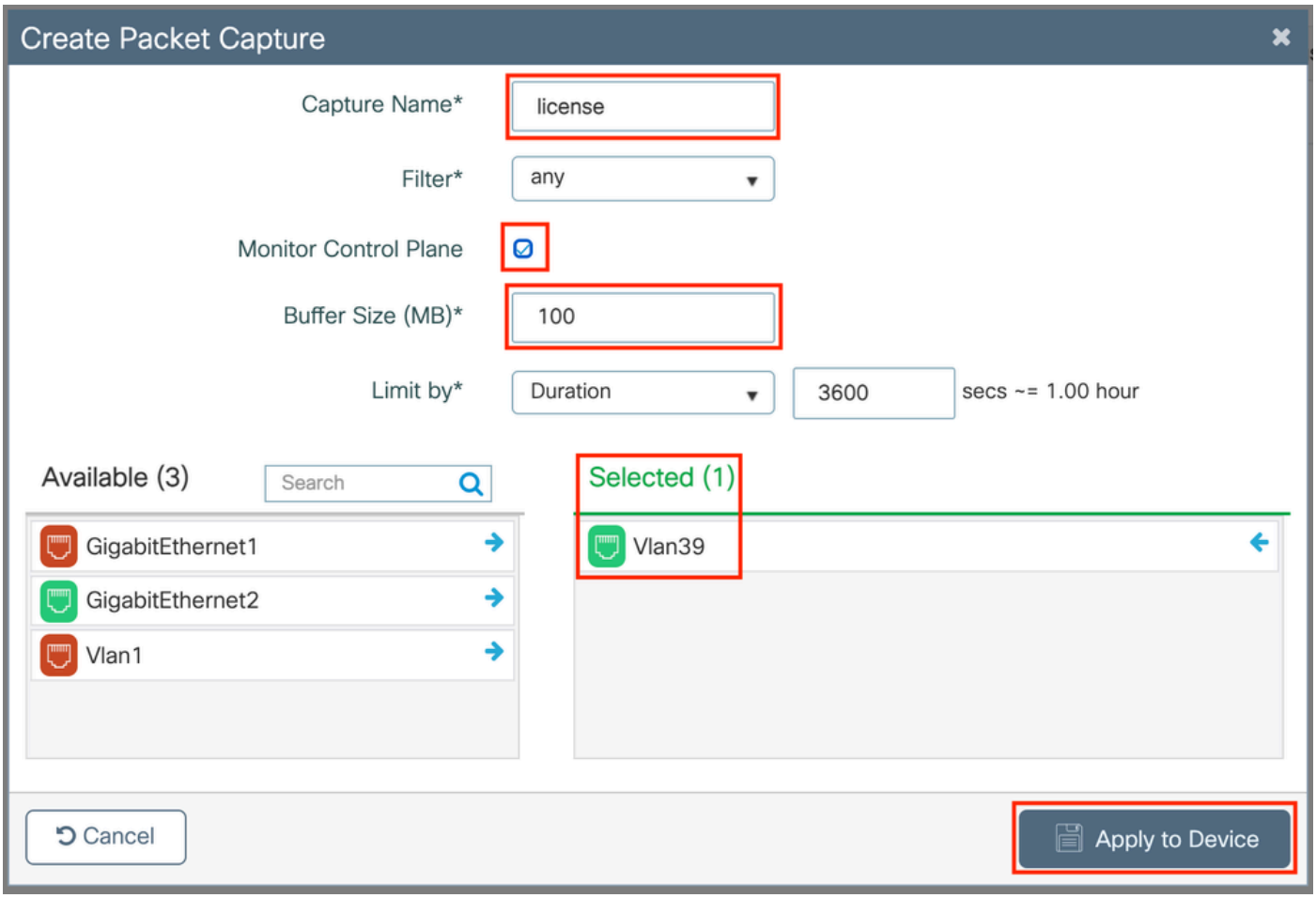
Captures de paquets

Même si la communication entre WLC et CSSM/SSM sur site est chiffrée et passe par HTTPS, l'exécution de captures de paquets peut révéler ce qui fait que la confiance n'est pas établie. La façon la plus simple de collecter des captures de paquets est par l'interface Web du WLC.

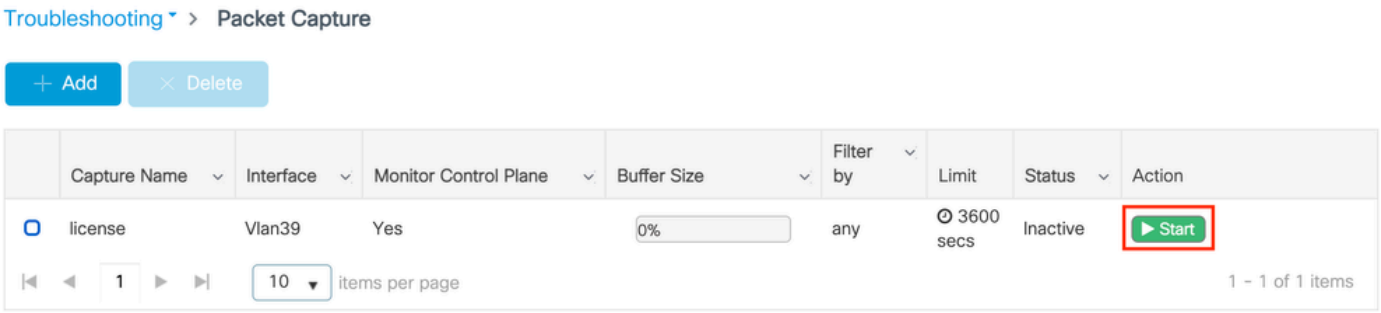
Accédez à Troubleshooting > Packet Capture. Créez un nouveau point de capture :



Assurez-vous que la case Monitor Control Plane est cochée. Augmentez la taille de la mémoire tampon à 100 Mo maximum. Ajoutez l'interface qui doit être capturée. Le trafic de licences Smart provient par défaut de l'interface de gestion sans fil ou de l'interface définie avec la commande ip http client source-interface :



Démarrez les captures et exécutez la commande license smart trust idtoken <token> all force :



Les captures de paquets d'un établissement de confiance doivent contenir les étapes suivantes :

1. Établissement de session TCP à l'aide de la séquence SYN, SYN-ACK et ACK
2. Établissement de session TLS avec échange de certificats serveur et client. L'établissement se termine par le paquet New Session Ticket
3. Échange de paquets chiffrés (trames de données d'application) où WLC signale l'utilisation de licence
4. Fin de session TCP via la séquence FIN-PSH-ACK, FIN-ACK et ACK

Remarque : Les captures de paquets contiennent beaucoup plus de trames, y compris des multiples de trames de mise à jour de fenêtre TCP et de données d'application

---

Étant donné que le cloud CSSM utilise 3 adresses IP publiques différentes, afin de filtrer toutes les captures de paquets entre WLC et CSSM, utilisez ces filtres Wireshark :

```
ip.addr==172.163.15.144 or ip.addr==192.168.220.90 or ip.addr==172.163.15.144
```

Si vous utilisez un module SSM sur site, filtrez l'adresse IP du module SSM :

```
ip.addr==
```

Exemple : Captures de paquets d'un établissement de confiance réussi avec CSSM connecté directement avec toutes les captures de paquets importantes filtrées :

No.	Arrival Time	Source	Destination	Protocol	Info
559	Aug 23, 2021 11:31:13.35…	192.168.10.150	192.133.220.90	TCP	22425 → 443 [SYN] Seq=0 Win=4128 Len=0 MSS=536
576	Aug 23, 2021 11:31:13.46…	192.133.220.90	192.168.10.150	TCP	443 → 22425 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1390
578	Aug 23, 2021 11:31:13.46…	192.168.10.150	192.133.220.90	TCP	22425 → 443 [ACK] Seq=1 Ack=1 Win=4128 Len=0
580	Aug 23, 2021 11:31:13.46…	192.168.10.150	192.133.220.90	TLSv1.2	Client Hello
608	Aug 23, 2021 11:31:13.58…	192.133.220.90	192.168.10.150	TLSv1.2	Server Hello
612	Aug 23, 2021 11:31:13.58…	192.168.10.150	192.133.220.90	TCP	[TCP Window Update] 22425 → 443 [ACK] Seq=168 Ack=537 Win=4128 Len=0
614	Aug 23, 2021 11:31:13.58…	192.133.220.90	192.168.10.150	TCP	443 → 22425 [ACK] Seq=537 Ack=168 Win=31953 Len=536 [TCP segment of a reassembled PDU]
673	Aug 23, 2021 11:31:13.70…	192.133.220.90	192.168.10.150	TLSv1.2	Certificate [TCP segment of a reassembled PDU]
675	Aug 23, 2021 11:31:13.70…	192.133.220.90	192.168.10.150	TLSv1.2	Server Key Exchange [TCP segment of a reassembled PDU]
695	Aug 23, 2021 11:31:13.71…	192.133.220.90	192.168.10.150	TLSv1.2	Certificate Request, Server Hello Done
711	Aug 23, 2021 11:31:13.85…	192.168.10.150	192.133.220.90	TLSv1.2	Certificate, Client Key Exchange
718	Aug 23, 2021 11:31:14.01…	192.168.10.150	192.133.220.90	TLSv1.2	Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
737	Aug 23, 2021 11:31:14.13…	192.133.220.90	192.168.10.150	TLSv1.2	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
745	Aug 23, 2021 11:31:14.13…	192.168.10.150	192.133.220.90	TLSv1.2	Application Data
747	Aug 23, 2021 11:31:14.13…	192.168.10.150	192.133.220.90	TLSv1.2	Application Data
749	Aug 23, 2021 11:31:14.13…	192.168.10.150	192.133.220.90	TLSv1.2	Application Data, Application Data
22…	Aug 23, 2021 11:31:45.00…	192.168.10.150	192.133.220.90	TCP	22425 → 443 [FIN, PSH, ACK] Seq=4306 Ack=9738 Win=3625 Len=0
22…	Aug 23, 2021 11:31:45.11…	192.133.220.90	192.168.10.150	TCP	443 → 22425 [FIN, ACK] Seq=9738 Ack=4307 Win=31250 Len=0
22…	Aug 23, 2021 11:31:45.11…	192.168.10.150	192.133.220.90	TCP	22425 → 443 [ACK] Seq=4307 Ack=9739 Win=3625 Len=0

Commandes show

Ces commandes show contiennent des informations utiles sur l'établissement de la confiance :

```
show license status
show license summary
show tech-support license
show license tech-support
show license air entities summary

show license history message (useful to see the history and content of messages sent to SL)

show tech wireless (actually gets show log and show run on top of the rest which can be useful)
```

La commande show license history message est l'une des commandes les plus utiles puisqu'elle peut afficher les messages réels envoyés par le WLC et reçus en retour de CSSM.

Un établissement de confiance qui a réussi a les deux « DEMANDE : Aug 23 10:18:08 2021

Central" et "RÉPONSE : Aug 23 10:18:10 2021 Central" messages imprimés. S'il n'y a rien après la ligne RESPONSE, cela signifie que le WLC n'a pas reçu de réponse du CSSM.

Voici un exemple de la sortie du message show license history pour un établissement d'approbation réussi :

```
REQUEST: Aug 23 10:18:08 2021 Central
{"request":"{\"header\":{\"request_type\":\"POLL_REQ\",\"sudi\":{\"udi_pid\":\"C9800-CL-K9\",\"udi_seri
NB\"},\"version\":\"1.3\",\"locale\":\"en_US.UTF-8\",\"signing_cert_serial_number\":\"3\",\"id_cert_ser
\",\"product_instance_identifier\":\"\",\"connect_info\":{\"name\":\"C_agent\",\"version\":\"5.0.9_rel/
e,\"additional_info\":\"\",\"capabilities\":[\"UTILITY\",\"DLC\",\"AppHA\",\"MULTITIER\",\"EXPORT_2\",\
Y_USAGE\"]}},\"request_data\":\"{\\\"sudi\\\":{\\\"udi_pid\\\":\\\"C9800-CL-K9\\\",\\\"udi_serial_numbe
\"},\\\"timestamp\\\":1629713888600,\\\"nonce\\\":\\\"11702702165338740293\\\",\\\"product_instance_ide
\"original_request_type\\\":\\\"LICENSE_USAGE\\\",\\\"original_piid\\\":\\\"2e84a42f-c903-44c5-83b2-e62
":7898262236}\"}","signature":{"type":"SHA256","key":"59152896","value":"eiJ7IuQaTCFxgUkwls76WZxa5DRI5A
OgMqQd5POU6VNsH2j9dHco4T1NJ/aCMbR1MRmkfxyVSWsx4lmjJL1lmpOSi3ZS4FBMvlF/EBOUfowREe2oz2lrQp1cAFpPn5SlaFezW
/Nu6SQZfIW+IdF+2qnJeNFAIZbNpgOB5d5HIJvDmDImvDu3bMRHhQAWr2KKzGFr6jPzOhs7bGY/+FlfTLQk5LFEUaKTNH/tuxJPFHlF
h9//uhsd+NaQyfdRFludkbfUBTFkvPxHW9/5w=="}}

  RESPONSE: Aug 23 10:18:10 2021 Central
{"signature":{"type":"SHA256","value":"TXZE034fqAul2jy9V4+HoB2hDShl9au/5sgodiCVatmu671/6MyN7kZfEzREufY8
SLrjTfO4grGeQTcH7yEjOD+gztWXCOu8RBT7/Bo9aBs\n4x1iOE6flPB3BP6yu7KIEUQZ8yHzlwDT+mVtJGi6TRrtYnV3KQMpCUmF5F
wOksf3SfXreNZJuzWXzjHvtmlusCQXw7ZTBzffYsNKOOlkJlr\nvgB2PkV7JUlsA481kpIvlPul6IiJXqk+2PC2IzCrCLG57lVN3XgX
1pEl2SHyQ/DAw==","piid":null,"cert_sn":null},"response":"{\"header\":{\"version\":\"1.3\",\"locale\":\"
mp\":1629713890172,\"nonce\":null,\"request_type\":\"POLL_REQ\",\"sudi\":{\"udi_pid\":\"C9800-CL-K9\",\
9PJK8D7OCNB\"},\"agent_actions\":null,\"connect_info\":{\"name\":\"SSM\",\"version\":\"1.3\",\"producti
s\":[\"DLC\",\"AppHA\",\"EXPORT_2\",\"POLICY_USAGE\",\"UTILITY\"],\"additional_info\":\"\"},\"signing_c
\",\"id_cert_serial_number\":\"59152896\",\"product_instance_identifier\":\"\"},\"status_code\":\"FAILE
\"Invalid ProductInstanceIdentifier: 2e84a42f-c903-44c5-83b2-e62e258c780f provided in the polling reque
262236\",\"retry_time_seconds\":0,\"response_data\":\"\"}","sch_response":null}
```

Débogages/btrace

Exécutez cette commande quelques minutes après une tentative d'établissement de confiance à l'aide d'une commande license smart trust idtoken all force. Les journaux IOSRP sont extrêmement verbeux. Ajouter | incluez « smart-agent » à la commande pour obtenir uniquement les journaux de licences smart.

```
show logging process iosrp start last 5 minutes
show logging process iosrp start last 5 minutes | include smart-agent
```

Vous pouvez également exécuter ces débogages, puis reconfigurer les commandes de licence pour forcer une nouvelle connexion :

```
debug license events
debug license errors
debug license agent all
```

Problèmes courants

WLC n'a pas d'accès Internet ou pare-feu bloque/modifie le trafic

Les captures de paquets intégrées sur le WLC sont un moyen facile de voir si le WLC reçoit quelque chose en retour du CSSM ou du SSM sur site. En l'absence de réponse, il est probable que le pare-feu bloque quelque chose.

La commande show license history message imprime une réponse vide 1 seconde après l'envoi de la demande si aucune réponse n'a été reçue du cloud CSSM ou du SSM sur site.

Par exemple, cela peut vous faire croire qu'une réponse vide a été reçue, mais en réalité il n'y a pas eu de réponse du tout :

```
REQUEST: Jun 29 11:12:39 2021 CET
{"request":"{\"header\":{\"request_type\":\"ID_TOKEN_TRUST\",\"sudi\":{\"udi_pid\":\"C9800-CL-K9\",\"ud
RESPONSE: Jun 29 11:12:40 2021 CET
```

Remarque : Il y a actuellement une demande d'amélioration de l'ID de bogue Cisco CSCvy84684 qui fait afficher le message d'historique de licence et imprimer une réponse vide quand il n'y a pas de réponse. Ceci permet d'améliorer le résultat de la commande show license history message

---

Alerte CA inconnue dans les captures de paquets

La communication avec le module CSSM ou le module SSM local nécessite un certificat correct côté 9800. Il peut être auto-signé, mais il ne peut pas être non valide ou expiré. Dans ce cas, une capture de paquet affiche une alerte TLS pour une CA inconnue envoyée par CSSM lorsque le certificat client HTTP 9800 a expiré.

La gestion de licences Smart utilise la configuration ip http client, qui est différente du serveur ip http que l'interface Web WLC utilise. Cela signifie que ces commandes doivent être configurées correctement :

```
ip http client source-interface
```

```
ip http client secure-trustpoint
```

Le nom du point de confiance peut être trouvé avec la commande show crypto pki trustpoints. Il est recommandé d'utiliser un certificat auto-signé TP-self-signed-xxxxxxxx ou un certificat installé par le fabricant (MIC), généralement appelé CISCO_IDEVID_SUDI et disponible uniquement sur les modèles 9800-80, 9800-40 et 9800-L.

Il est important de noter que les périphériques qui effectuent une interception TLS, tels qu'un pare-feu avec la fonctionnalité de déchiffrement SSL, peuvent empêcher le C9800 d'établir une connexion réussie avec le serveur de licences Cisco, car le certificat HTTPS présenté est le certificat de pare-feu au lieu du certificat du serveur de licences Cisco.

Remarque : Assurez-vous de configurer les commandes source-interface et secure-trustpoint. Une commande source-interface est nécessaire même si WLC n'a qu'une seule interface L3.

Informations connexes

- Licence Smart avec mode Air Gap sur le 9800
- Assistance technique de Cisco et téléchargements

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.