Utiliser l'enregistrement des licences Smart FMC et FTD et les problèmes courants pour le dépannage

Table des matières

Introduction

Ce document décrit la configuration d'enregistrement de licence Smart de Firepower Management Center sur les périphériques gérés par Firepower Threat Defense.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

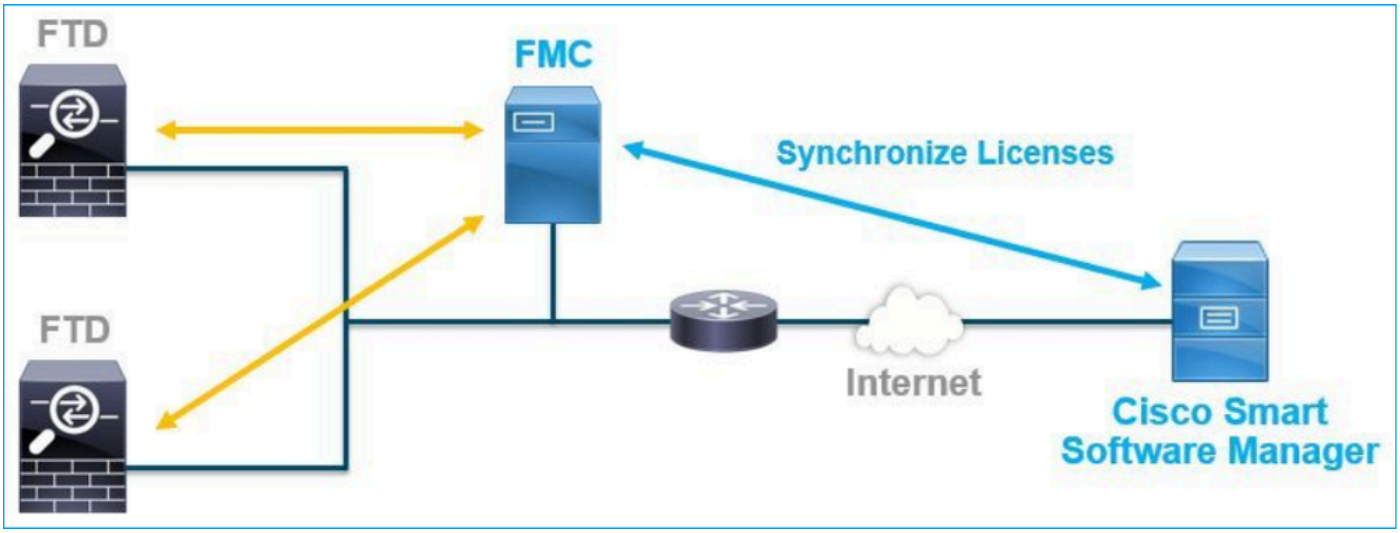
Composants utilisés

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

Enregistrement des licences FMC, FTD et Smart.

L'enregistrement des licences Smart s'effectue sur le centre de gestion Firepower (FMC). Le FMC communique avec le portail Cisco Smart Software Manager (CSSM) via Internet. Dans le CSSM, l'administrateur du pare-feu gère le compte Smart et ses licences. Le FMC peut librement attribuer et supprimer des licences aux périphériques Firepower Threat Defense (FTD) gérés. En d'autres termes, le FMC gère de manière centralisée les licences pour les périphériques FTD.



Une licence supplémentaire est requise pour utiliser certaines fonctionnalités des périphériques FTD. Les types de licences Smart que les clients peuvent attribuer à un périphérique FTD sont documentés dans Types et restrictions de licences FTD.

La licence de base est incluse dans le périphérique FTD. Cette licence est automatiquement enregistrée dans votre compte Smart lorsque le FMC est enregistré auprès de CSSM.
Les licences à durée limitée : Threat, Malware et URL Filtering sont facultatives. Pour utiliser les fonctions associées à une licence, une licence doit être attribuée au périphérique FTD.

Pour utiliser un FMCv (Firepower Management Center Virtual) pour la gestion FTD, une licence de périphérique Firepower MCv dans CSSM est également nécessaire pour le FMCv.

La licence FMCv est incluse dans le logiciel et elle est perpétuelle.

En outre, des scénarios sont fournis dans ce document pour aider à dépanner les erreurs courantes d'enregistrement de licence qui peuvent se produire.

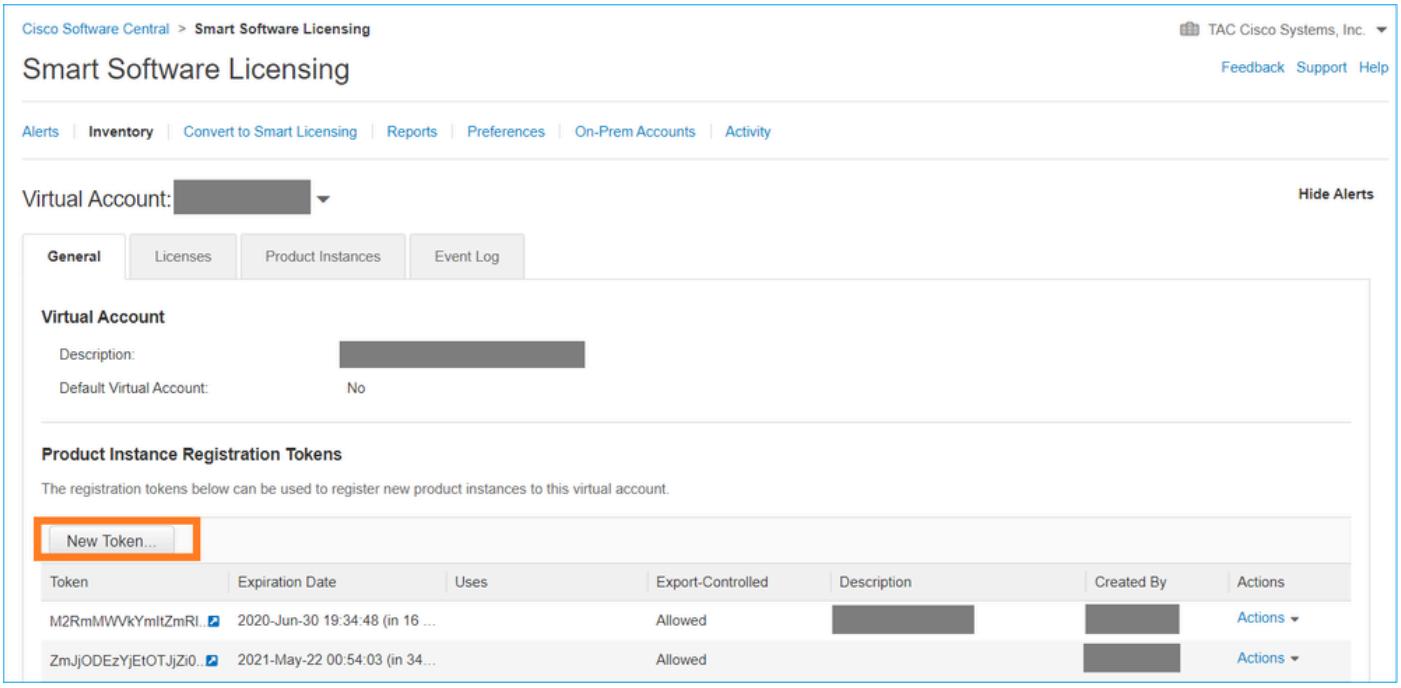
Pour plus d'informations sur les licences, consultez Licences de fonctions Cisco Firepower System et Foire aux questions (FAQ) sur les licences Firepower.

Inscription de licence Smart FMC

Conditions préalables

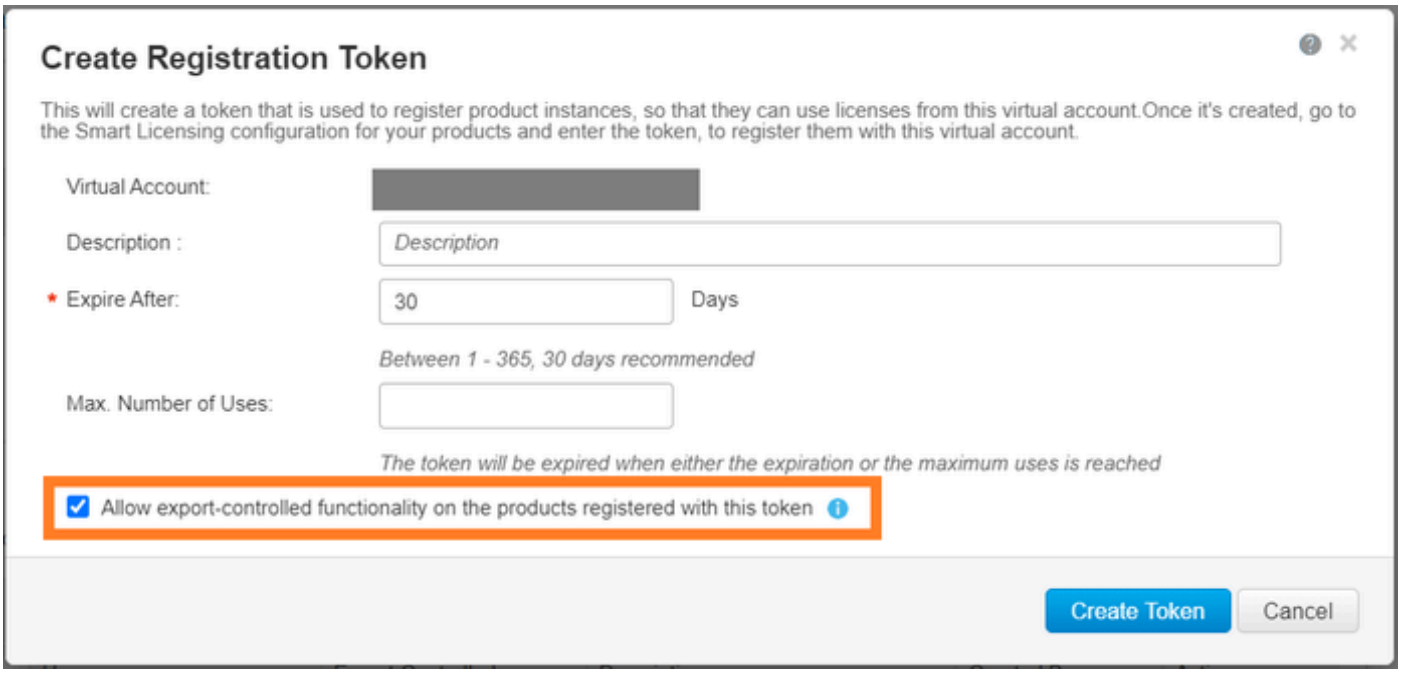
1. Pour l'enregistrement de la licence Smart, le FMC doit accéder à Internet. Étant donné que le certificat est échangé entre le FMC et le nuage de licences Smart avec HTTPS, assurez-vous qu'aucun périphérique dans le chemin d'accès ne peut affecter/modifier la communication. (par exemple, pare-feu, proxy, périphérique de décodage SSL, etc.).

2. Accédez au CSSM et émettez un ID de jeton à partir du bouton Inventory > General > New Token, comme illustré dans cette image.



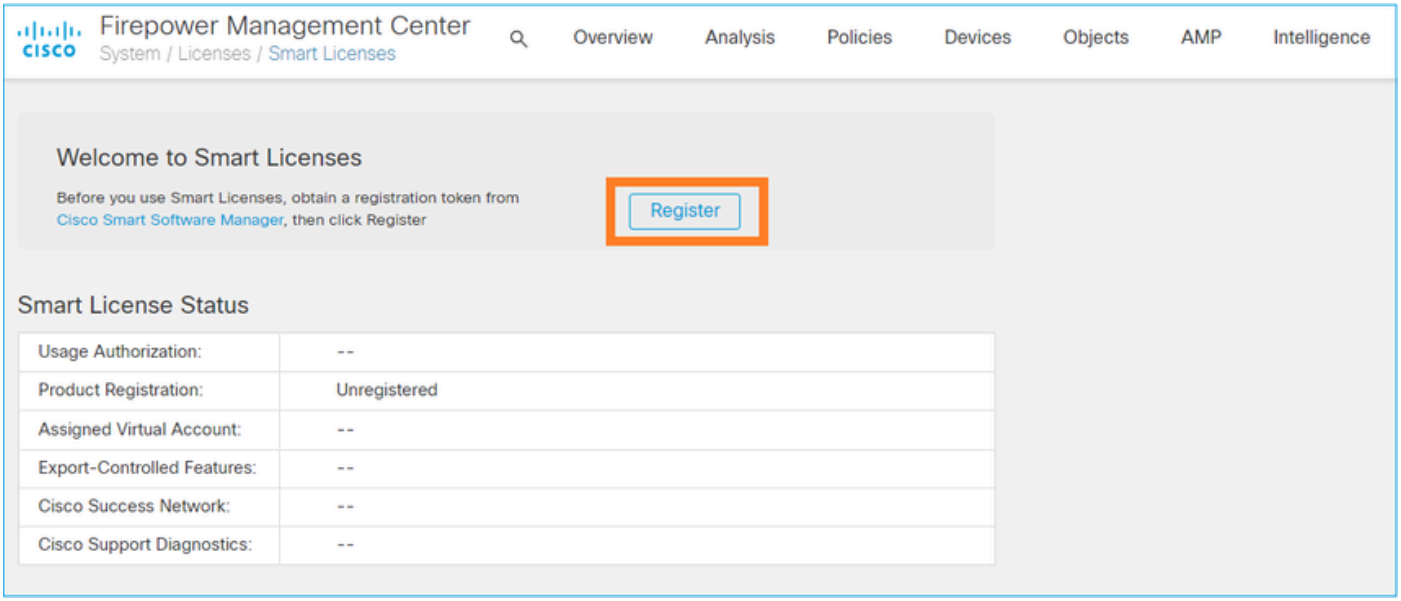
Pour utiliser le chiffrement fort, activez l'option Autoriser la fonctionnalité de contrôle des exportations sur les produits enregistrés avec ce jeton. Lorsque cette option est activée, une coche s'affiche dans la case.

3. Sélectionnez Créer un jeton.

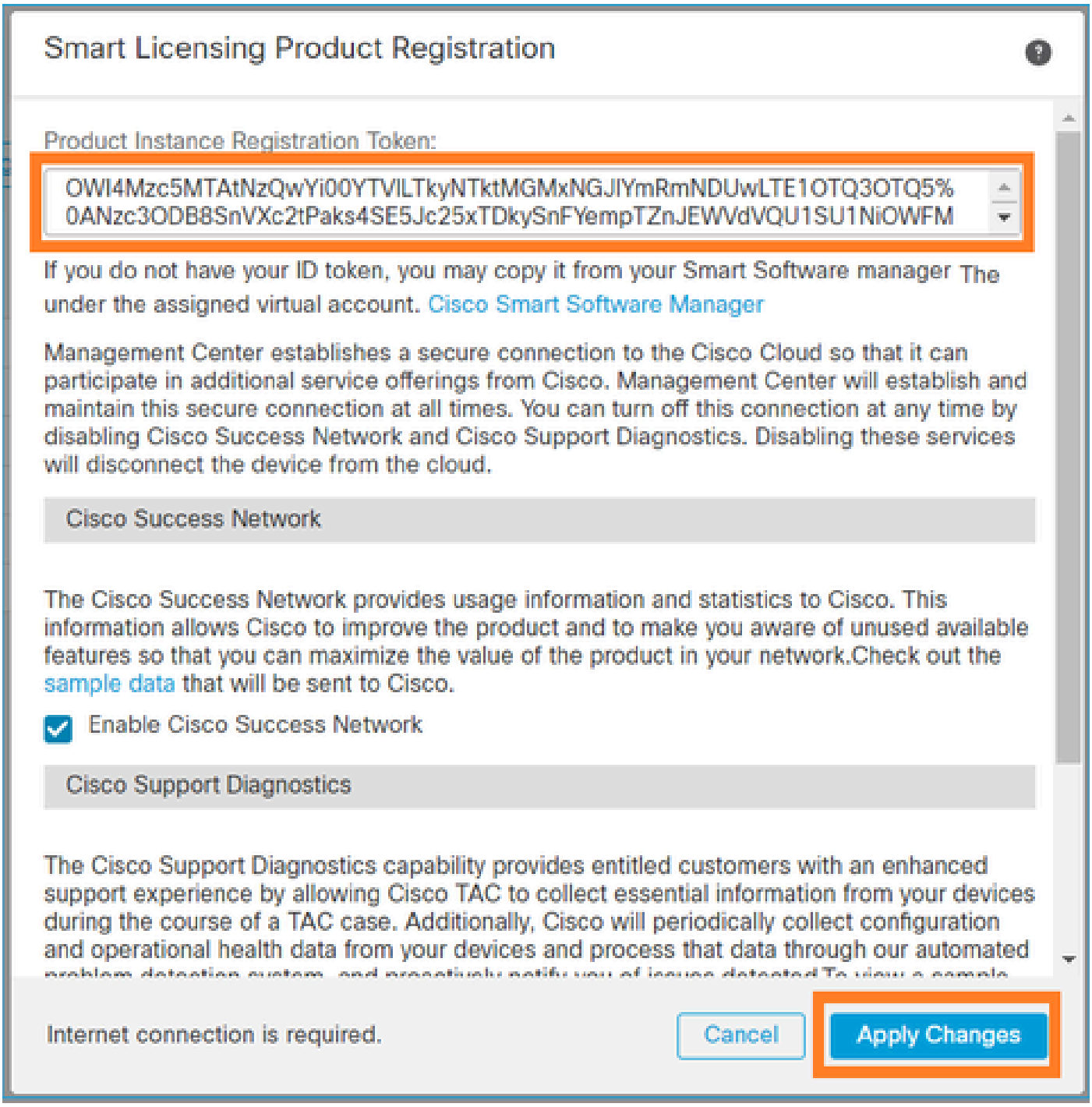


Inscription de licence Smart FMC

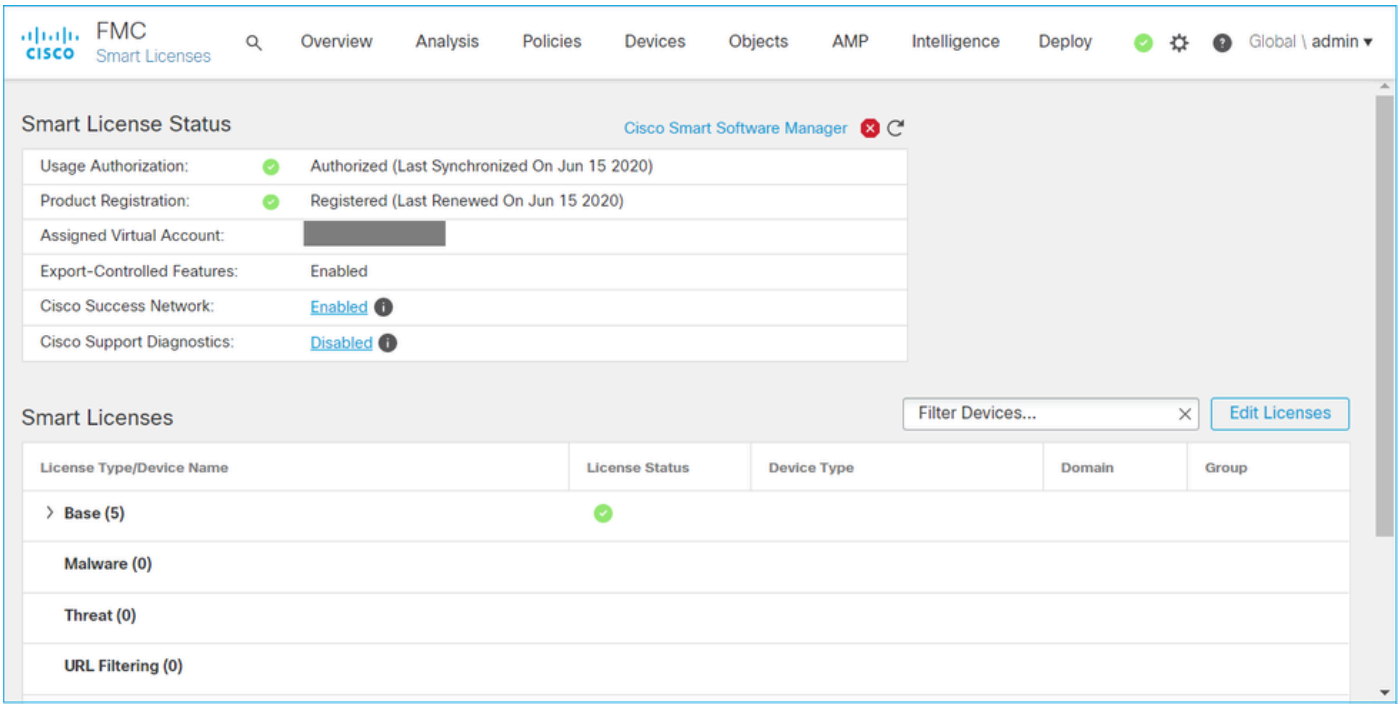
Accédez à System > Licenses > Smart Licenses sur le FMC, et sélectionnez le bouton Register, comme illustré dans cette image.



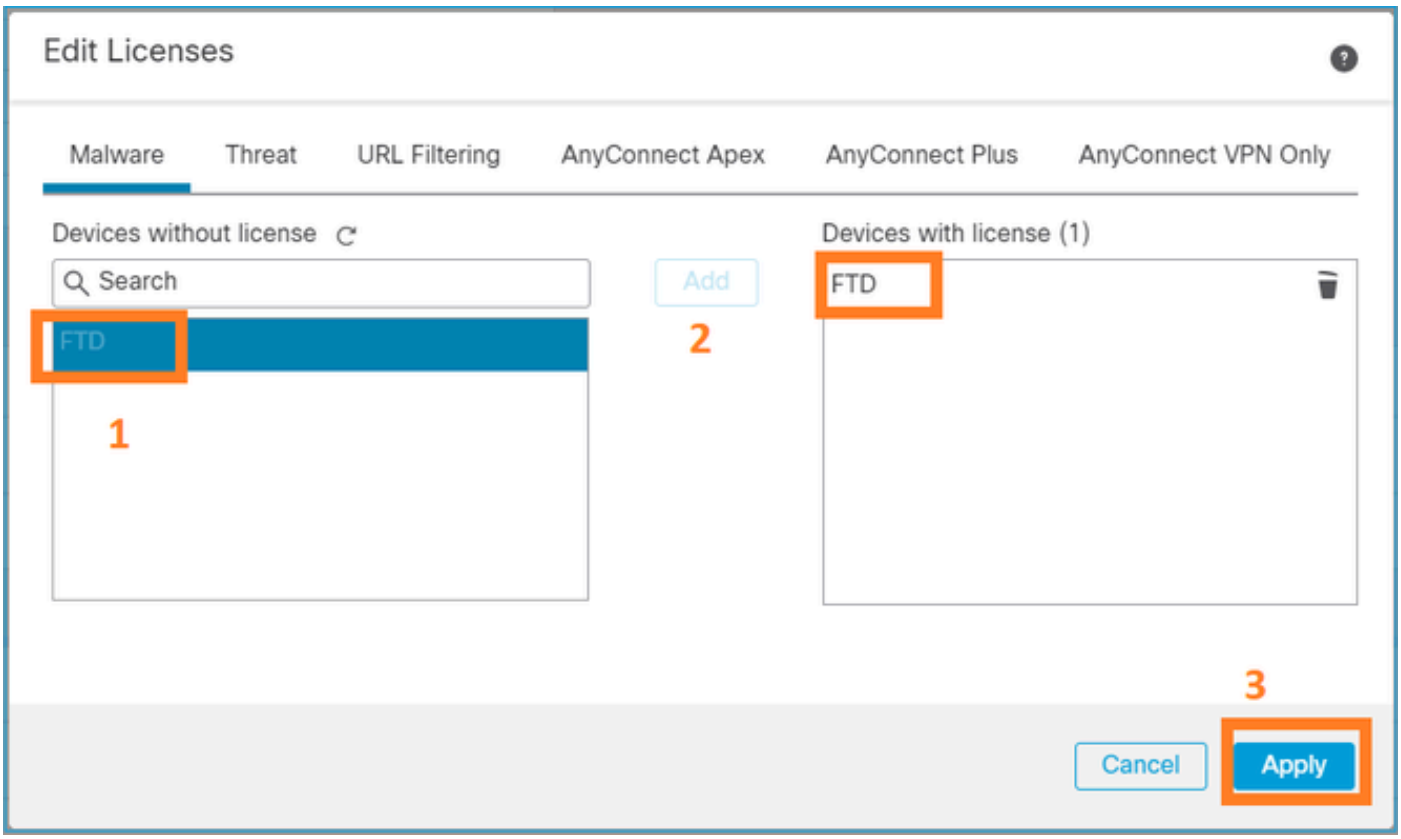
Saisissez l'ID de jeton dans la fenêtre Enregistrement du produit de licence Smart et sélectionnez Apply Changes, comme illustré dans cette image.



Si l'enregistrement de la licence Smart a réussi, l'état d'enregistrement du produit affiche Registered, comme illustré dans cette image.

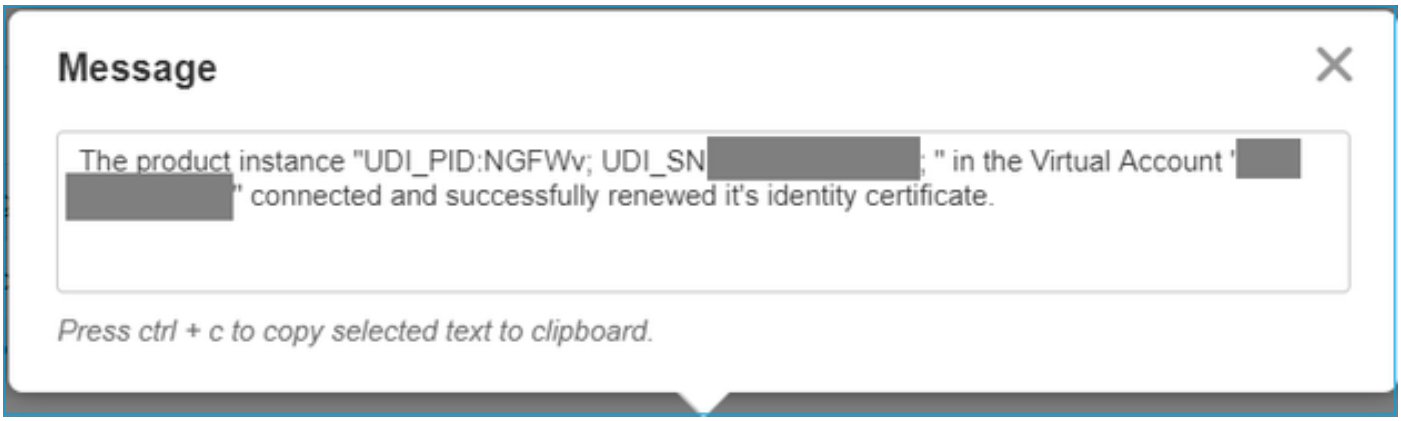


Pour attribuer une licence à durée déterminée au périphérique FTD, sélectionnez Edit Licenses (Modifier les licences). Ensuite, sélectionnez et ajoutez un périphérique géré à la section Périphériques avec licence. Enfin, sélectionnez le bouton Apply comme illustré dans cette image.



Confirmation côté Smart Software Manager (SSM)

La réussite de l'enregistrement de la licence Smart FMC peut être confirmée à partir de Inventory > Event Log dans CSSM, comme illustré dans cette image.

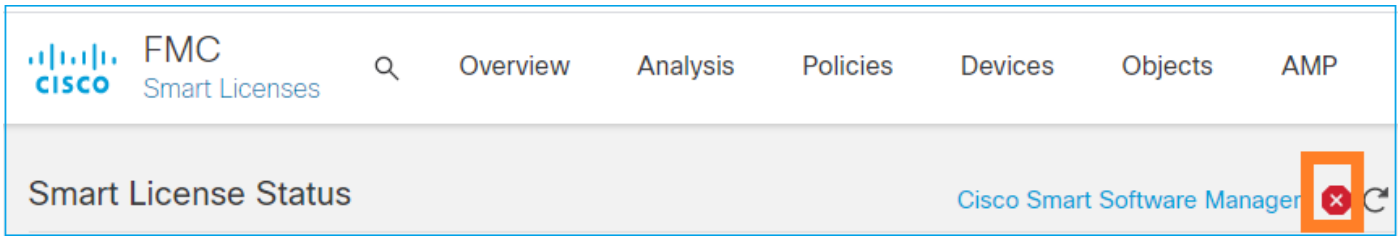


L'état d'enregistrement du FMC peut être confirmé à partir de Inventory > Product Instances. Consultez le journal des événements dans l'onglet Journal des événements. L'enregistrement et l'état d'utilisation des licences Smart peuvent être vérifiés dans l'onglet Inventory > Licenses. Vérifiez que la licence à durée déterminée achetée est utilisée correctement et qu'aucune alerte n'indique que les licences sont insuffisantes.

Désenregistrement de la licence Smart FMC

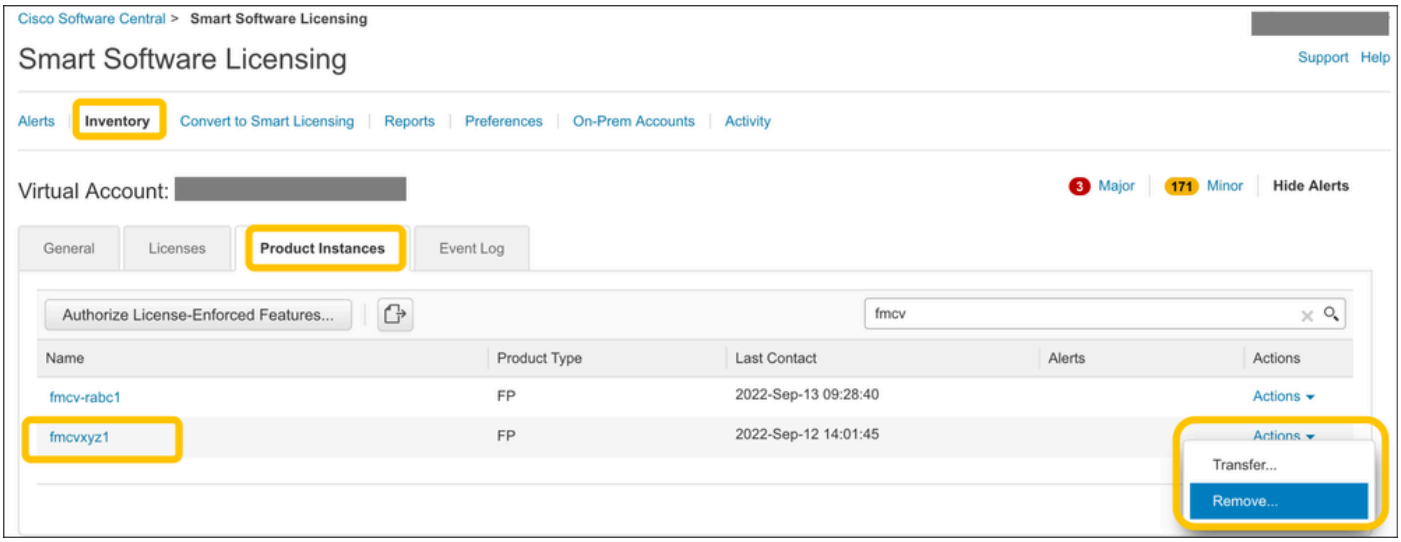
Désinscription du FMC du module Cisco SSM

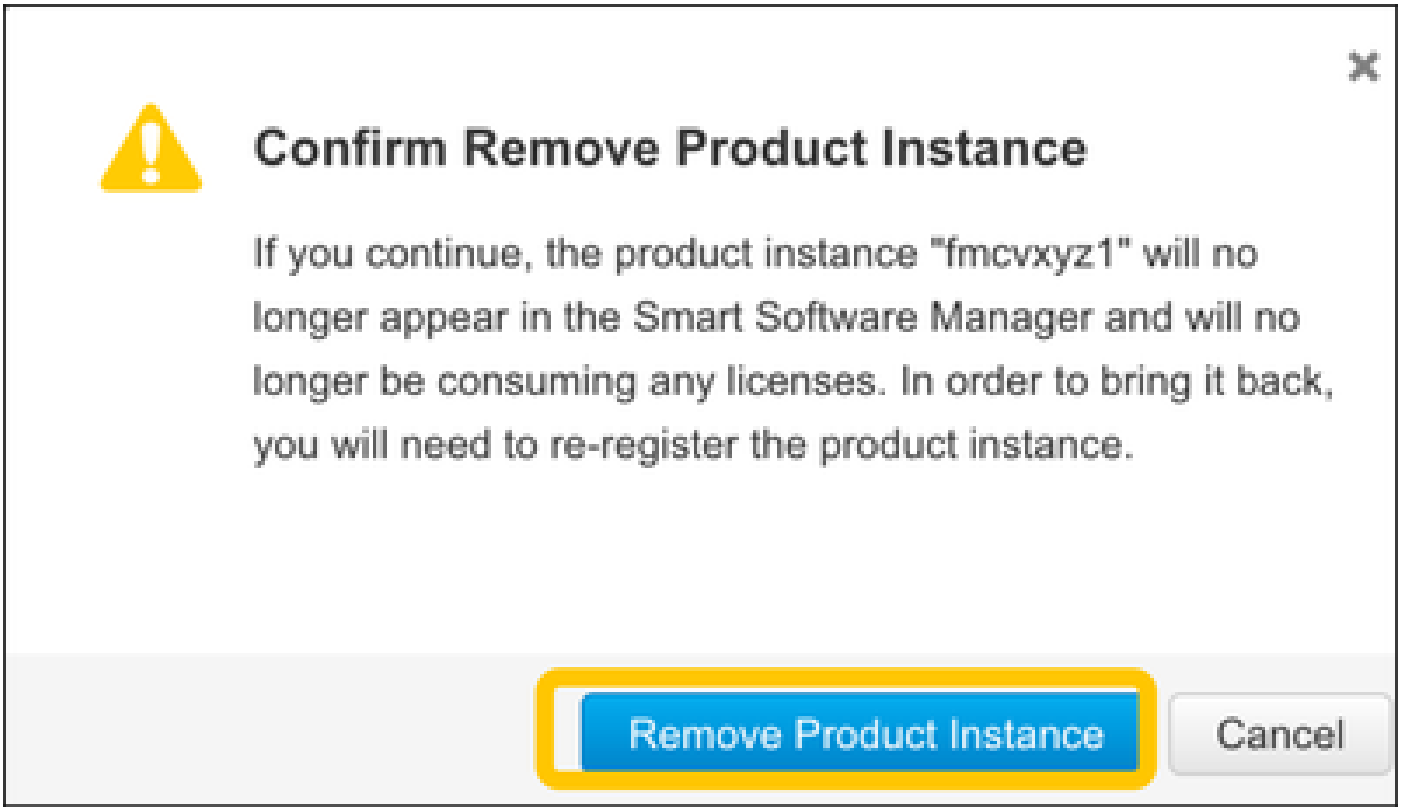
Pour libérer la licence pour une raison quelconque ou utiliser un jeton différent, accédez à System > Licenses > Smart Licenses et sélectionnez le bouton de désinscription, comme illustré dans cette image.



Supprimer l'enregistrement côté SSM

Accédez à Smart Software Manager (Cisco Smart Software Manager) et, dans Inventaire > Instances de produit, sélectionnez Supprimer sur le FMC cible. Sélectionnez ensuite Remove Product Instance pour supprimer le FMC et libérer les licences allouées, comme illustré dans cette image.





RMA

Si le FMC est renvoyé, annulez l'enregistrement du FMC à partir de Cisco Smart Software Manager (CSSM) en suivant les étapes de la section Désenregistrement de la licence Smart FMC > Supprimer l'enregistrement du côté SSM et réenregistrez le FMC avec CSSM en suivant les étapes de la section Enregistrement de la licence Smart FMC.

Dépannage

Vérification de synchronisation temporelle

Accédez à l'interface de ligne de commande du contrôleur FMC (par exemple, SSH) et assurez-vous que l'heure est correcte et qu'elle est synchronisée avec un serveur NTP approuvé. Étant donné que le certificat est utilisé pour l'authentification de licence Smart, il est important que le FMC dispose des informations d'heure correctes :

<#root>

```
admin@FMC:~$
```

date
Thu

```
 Jun 14 09:18:47 UTC 2020
admin@FMC:~$
admin@FMC:~$
```

ntpq -pn

```
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.0.0.2        171.68.xx.xx     2 u  387 1024  377    0.977    0.469   0.916
 127.127.1.1     .SFCL.          13 l    -   64    0    0.000    0.000   0.000
```

À partir de l'interface utilisateur FMC, vérifiez les valeurs du serveur NTP à partir de System > Configuration > Time Synchronization.

Activer la résolution de noms et vérifier l'accessibilité à tools.cisco.com (smartreceiver.cisco.com à partir de FMC 7.3+)

Assurez-vous que le FMC peut résoudre un nom de domaine complet et qu'il est accessible à tools.cisco.com (smartreceiver.cisco.com) à partir de FMC 7.3 selon l'ID de bogue Cisco CSCwj95397

<#root>

```
>
```

expert
admin@FMC2000-2:~$

sudo su

```
Password:
root@FMC2000-2:/Volume/home/admin# ping tools.cisco.com
PING tools.cisco.com (173.37.145.8) 56(84) bytes of data.
64 bytes from tools2.cisco.com (173.37.145.8): icmp_req=1 ttl=237 time=163 ms
64 bytes from tools2.cisco.com (173.37.145.8): icmp_req=2 ttl=237 time=163 ms
```

À partir de l'interface utilisateur FMC, vérifiez l'adresse IP de gestion et l'adresse IP du serveur DNS à partir de System > Configuration > Management Interfaces.

Vérifiez l'accès HTTPS (TCP 443) de FMC à tools.cisco.com (smartreceiver.cisco.com de FMC 7.3+)

Utilisez la commande Telnet ou curl pour vous assurer que le FMC a un accès HTTPS à tools.cisco.com (smartreceiver.cisco.com à partir de FMC 7.3+). Si la communication TCP 443 est interrompue, vérifiez qu'elle n'est pas bloquée par un pare-feu et qu'il n'y a pas de périphérique de déchiffrement SSL dans le chemin.

<#root>

```
root@FMC2000-2:/Volume/home/admin#

 telnet tools.cisco.com 443

Trying 72.163.4.38...

Connected to tools.cisco.com.

Escape character is '^]'.
^CConnection closed by foreign host.

 <--- Press Ctrl+C
```

Essai de boucle :

<#root>

```
root@FMC2000-2:/Volume/home/admin#

curl -vvk https://tools.cisco.com

*

Trying 72.163.4.38...

* TCP_NODELAY set

* Connected to tools.cisco.com (72.163.4.38) port 443 (#0)

* ALPN, offering http/1.1
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/certs/ca-certificates.crt
  CApath: none
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / AES128-GCM-SHA256
* ALPN, server accepted to use http/1.1
* Server certificate:
*  subject: C=US; ST=CA; L=San Jose; O=Cisco Systems, Inc.; CN=tools.cisco.com
```

```
*  start date: Sep 17 04:00:58 2018 GMT
*  expire date: Sep 17 04:10:00 2020 GMT
*  issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID SSL ICA G2
*  SSL certificate verify ok.
> GET / HTTP/1.1
> Host: tools.cisco.com
> User-Agent: curl/7.62.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Wed, 17 Jun 2020 10:28:31 GMT
< Last-Modified: Thu, 20 Dec 2012 23:46:09 GMT
< ETag: "39b01e46-151-4d15155dd459d"
< Accept-Ranges: bytes
< Content-Length: 337
< Access-Control-Allow-Credentials: true
< Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
< Access-Control-Allow-Headers: Content-type, fromPartyID, inputFormat, outputFormat, Authorization, Co
< Content-Type: text/html
< Set-Cookie: CP_GUTC=10.163.4.54.1592389711389899; path=/; expires=Mon, 16-Jun-25 10:28:31 GMT; domain=
< Set-Cookie: CP_GUTC=10.163.44.92.1592389711391532; path=/; expires=Mon, 16-Jun-25 10:28:31 GMT; domai
< Cache-Control: max-age=0
< Expires: Wed, 17 Jun 2020 10:28:31 GMT
<
<html>
<head>
<script language="JavaScript">

var input = document.URL.indexOf('intellishield');
if(input != -1) {
 window.location="https://intellishield.cisco.com/security/alertmanager/";
}
else {
 window.location="http://www.cisco.com";
};

</script>
</head>

<body>
<a href="http://www.cisco.com">www.cisco.com</a>
</body>
</html>
* Connection #0 to host tools.cisco.com left intact
root@FMC2000-2:/Volume/home/admin#
```

Vérification DNS

Vérifiez la résolution vers tools.cisco.com (smartreceiver.cisco.com à partir de FMC 7.3+) :

<#root>

```
root@FMC2000-2:/Volume/home/admin#

nslookup tools.cisco.com

Server:         192.0.2.100
Address:        192.0.2.100#53
```

```
Non-authoritative answer:

Name:   tools.cisco.com
Address: 72.163.4.38
```

Vérification du proxy

Si apProxy est utilisé, vérifiez les valeurs sur le FMC et sur le serveur proxy. Sur le FMC, vérifiez que le FMC utilise l'adresse IP et le port corrects du serveur proxy.

<#root>

```
root@FMC2000-2:/Volume/home/admin#

cat /etc/sf/smart_callhome.conf


KEEP_SYNC_ACTIVE:1
PROXY_DST_URL:https://tools.cisco.com/its/service/oddce/services/DDCEService

PROXY_SRV:192.0.xx.xx

PROXY_PORT:80
```

Dans l'interface utilisateur de FMC, les valeurs de proxy peuvent être confirmées à partir de System > Configuration > Management Interfaces.

Si les valeurs côté FMC sont correctes, vérifiez les valeurs côté serveur proxy (par exemple, si le serveur proxy autorise l'accès depuis le FMC et vers tools.cisco.com. En outre, autorisez le trafic et l'échange de certificats via le proxy. Le FMC utilise un certificat pour l'enregistrement de la licence Smart).

ID de jeton expiré

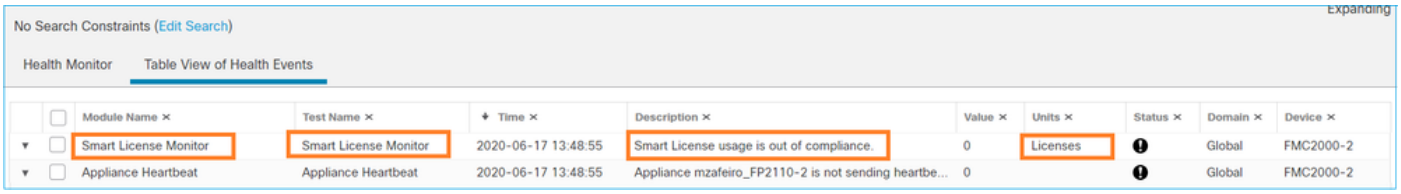
Vérifiez que l'ID de jeton émis n'a pas expiré. Si elle a expiré, demandez à l'administrateur Smart Software Manager d'émettre un nouveau jeton et de réenregistrer la licence Smart avec le nouvel ID de jeton.

Modification de la passerelle FMC

Il peut arriver que l'authentification de la licence Smart ne puisse pas être effectuée correctement en raison des effets d'un proxy relais ou d'un périphérique de déchiffrement SSL. Si possible, changez la route pour l'accès Internet FMC pour éviter ces périphériques, puis recommencez l'enregistrement de la licence Smart.

Vérifiez les événements d'intégrité sur FMC

Sur le FMC, accédez à System > Health > Events et vérifiez l'état du module Smart License Monitor pour les erreurs. Par exemple, si la connexion échoue en raison d'un certificat expiré ; une erreur, telle que id certificate expiré est générée, comme illustré dans cette image.



Vérifiez le journal des événements côté SSM

Si le FMC peut se connecter au CSSM, vérifiez le journal des événements de la connectivité dans Inventory > Event Log. Vérifiez s'il existe de tels journaux d'événements ou d'erreurs dans le CSSM. S'il n'y a pas de problème avec les valeurs/le fonctionnement du site FMC, et s'il n'y a pas de journal des événements du côté du CSSM, il est possible qu'il y ait un problème avec la route entre le FMC et le CSSM.

Problèmes courants

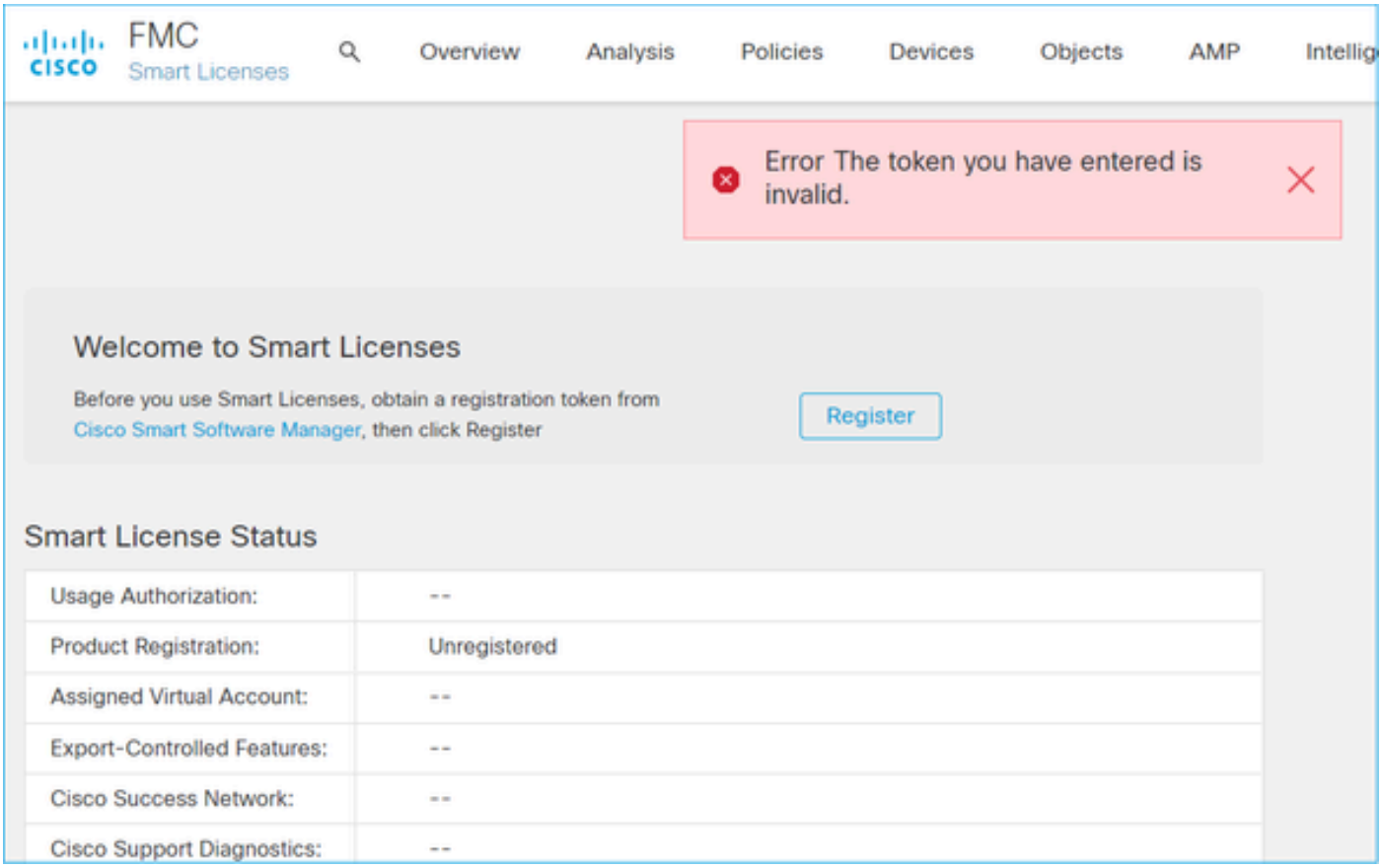
Résumé des États d'enregistrement et d'autorisation :

État d'enregistrement du produit	État autorisation utilisation	Commentaires
Non Enregistré	—	Le FMC n'est ni en mode enregistré ni en mode d'évaluation. Il s'agit de l'état initial après l'installation de FMC ou après l'expiration de la licence d'évaluation de 90 jours.
Enregistré	Autorisé	Le FMC est enregistré auprès de Cisco Smart Software Manager (CSSM) et des périphériques FTD sont enregistrés avec un abonnement valide.
Enregistré	Autorisation expirée	Le FMC n'a pas pu communiquer avec le serveur principal de licences Cisco pendant plus de 90 jours.
Enregistré	Non Enregistré	Le FMC est enregistré auprès de Cisco Smart Software Manager (CSSM), mais aucun périphérique FTD n'est enregistré sur le FMC.
Enregistré	Non-conformité	Le FMC est enregistré auprès de Cisco Smart Software Manager (CSSM), mais des périphériques FTD sont enregistrés avec un ou plusieurs abonnements non valides.

		Par exemple, un périphérique FTD (FP4112) utilise un abonnement THREAT, mais avec Cisco Smart Software Manager (CSSM), aucun abonnement THREAT n'est disponible pour FP4112.
Évaluation (90 jours)	S/O	La période d'évaluation est en cours d'utilisation, mais aucun périphérique FTD n'est enregistré sur le FMC.

Étude de cas 1. Jeton non valide

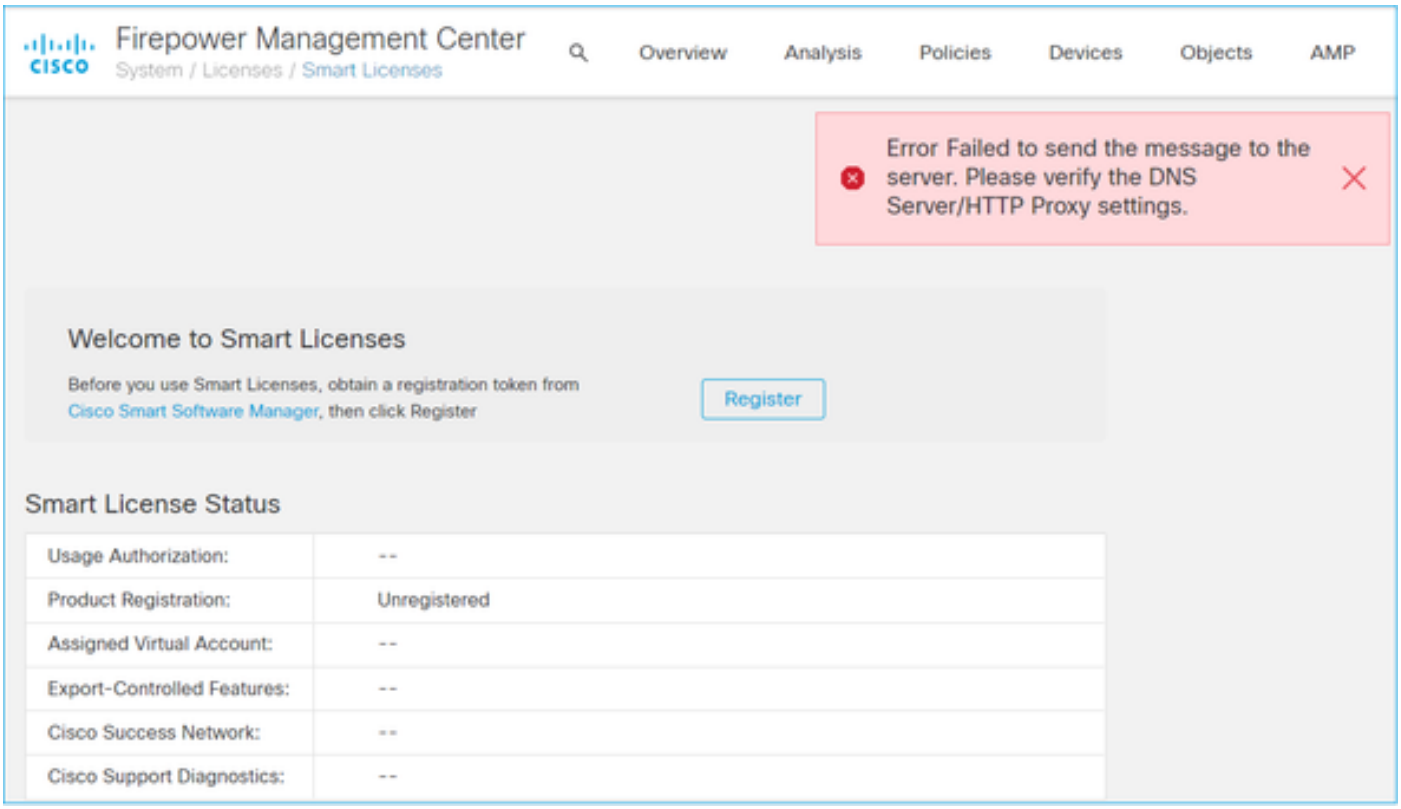
Symptôme : l'enregistrement au CSSM échoue rapidement (~10 s) en raison d'un jeton non valide, comme illustré dans cette image.



Résolution : utilisez un jeton valide.

Étude de cas 2. DNS non valide

Symptôme : échec de l'inscription au CSSM après un certain temps (~25 s), comme illustré dans cette image.



Vérifiez le fichier /var/log/process_stdout.log. Le problème DNS est visible :

<#root>

```
root@FMC2000-2:/Volume/home/admin#
```

cat /var/log/process_stdout.log

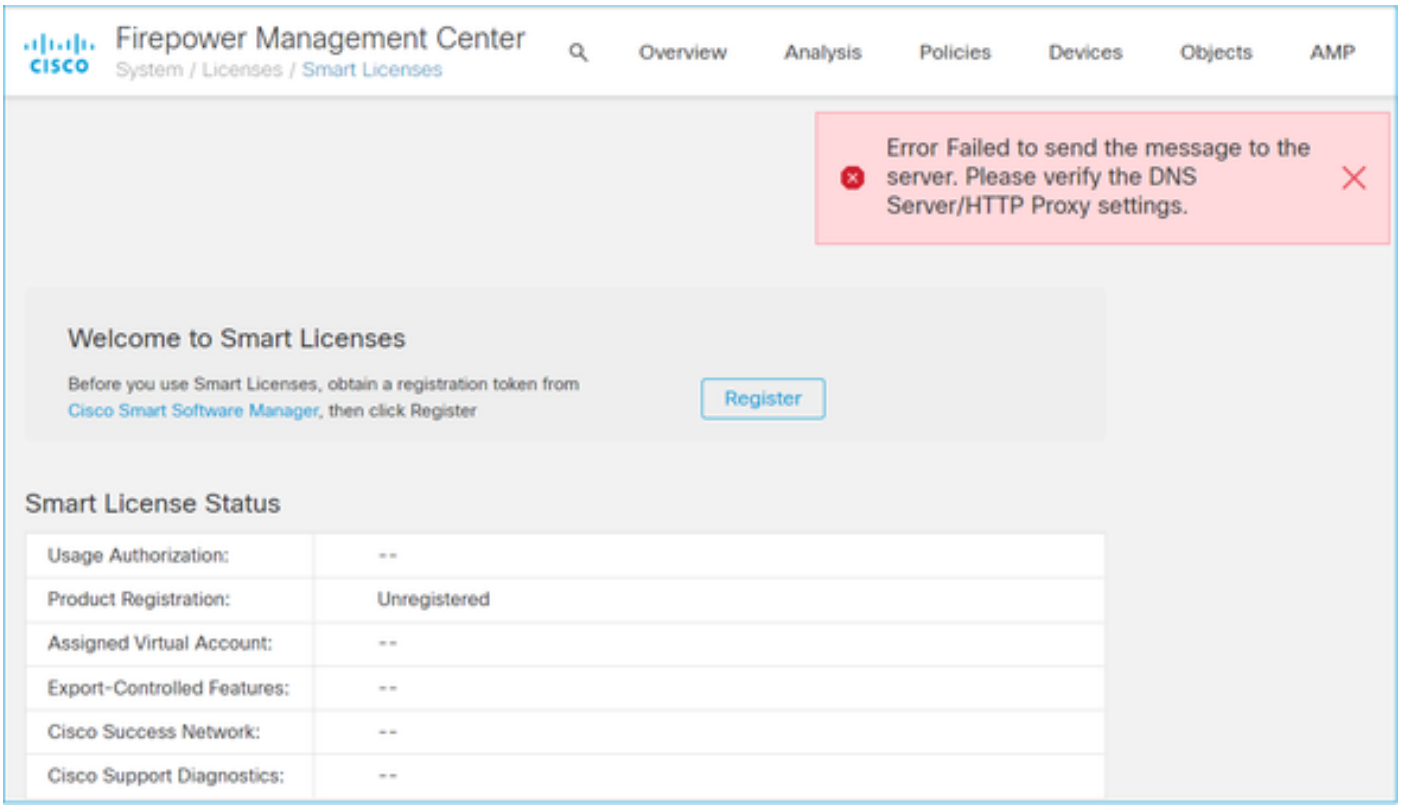
```
2020-06-25 09:05:21 sla[24043]: *Thu Jun 25 09:05:10.989 UTC: CH-LIB-ERROR: ch_pf_curl_send_msg[494],
failed to perform, err code 6, err string
```

"Couldn't resolve host name"

Résolution : échec de la résolution du nom d'hôte CSSM. La résolution consiste à configurer le DNS, s'il n'est pas configuré, ou à résoudre les problèmes DNS.

Étude de cas 3. Valeurs temporelles non valides

Symptôme : échec de l'inscription au CSSM après un certain temps (~25 s), comme illustré dans cette image.



Vérifiez le fichier /var/log/process_stdout.log. Les problèmes de certificat sont les suivants :

<#root>

```
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_curl_request_init[59]
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_curl_post_prepare[299
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_curl_post_prepare[302
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_curl_head_init[110],
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-ERROR: ch_pf_curl_send_msg[494],

failed to perform, err code 60, err string "SSL peer certificate or SSH remote key was not OK"

2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-TRACE: ch_pf_http_unlock[330], unl
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-TRACE: ch_pf_send_http[365], send
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-TRACE: ch_pf_curl_is_cert_issue[51

cert issue checking, ret 60, url https://tools.cisco.com/its/service/oddce/services/DDCEService
```

Vérifiez la valeur de temps FMC :

<#root>

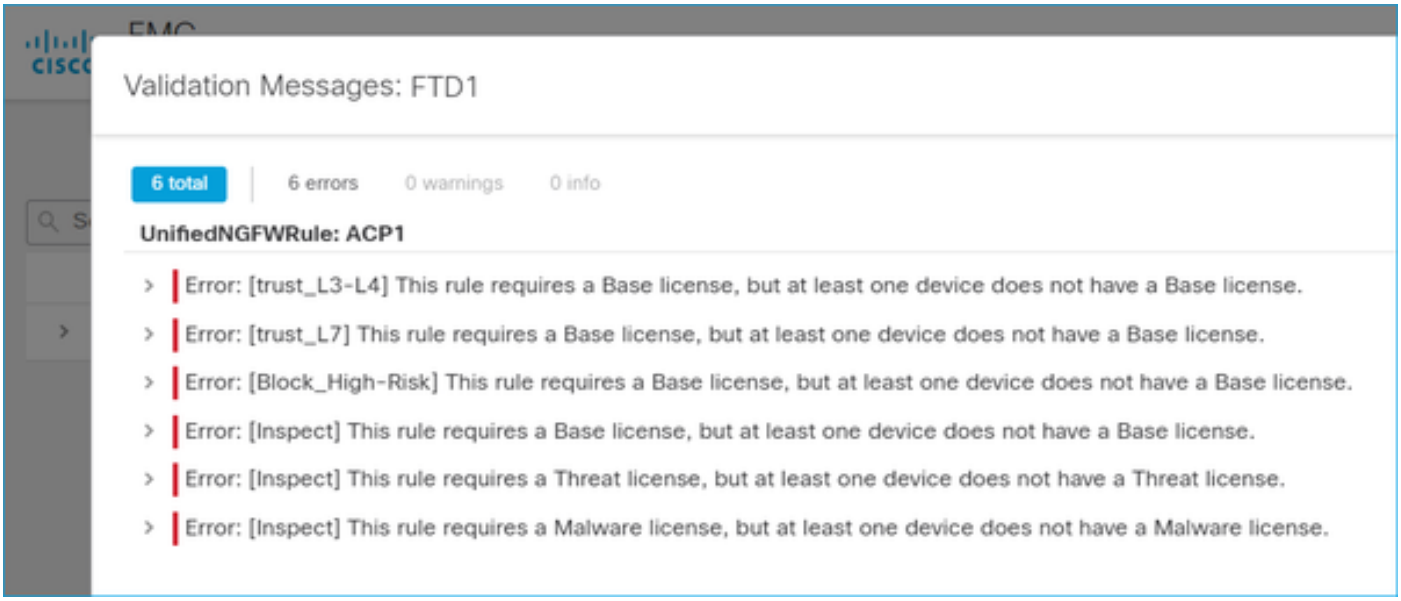
```
root@FMC2000-2:/Volume/home/admin#

date

Fri Jun 25 09:27:22 UTC 2021
```

Étude de cas 4. Aucun abonnement

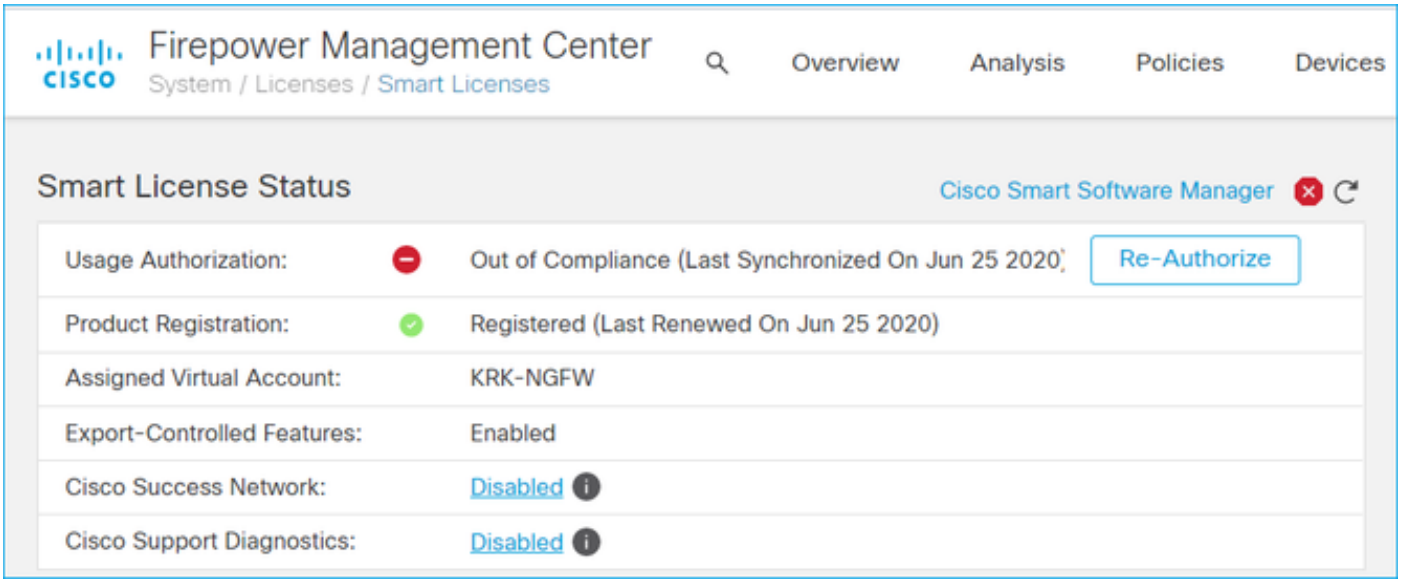
S'il n'y a pas d'abonnement de licence pour une fonctionnalité spécifique, le déploiement FMC n'est pas possible :



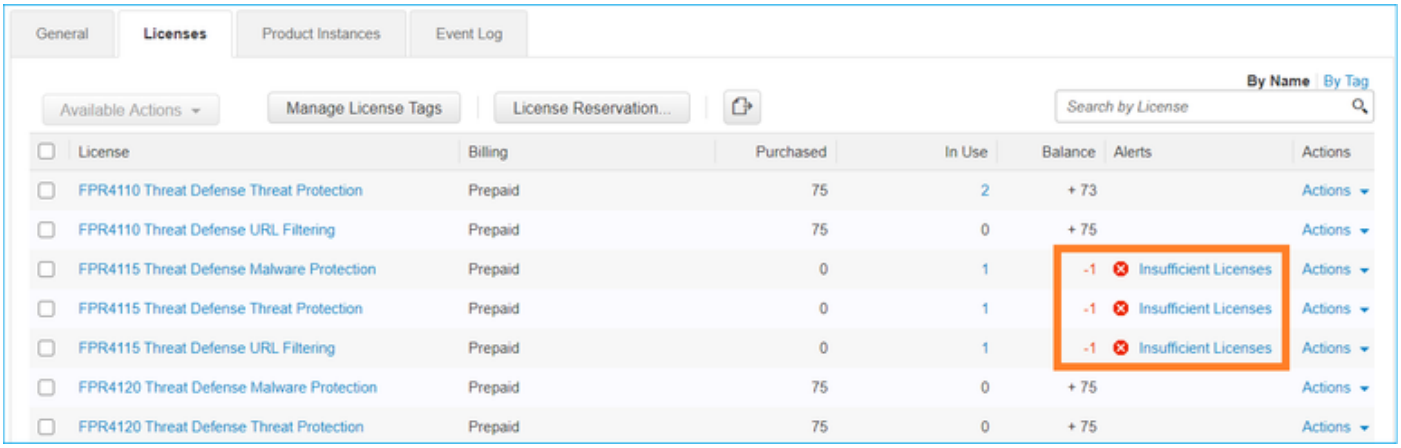
Résolution : il est nécessaire d'acheter et d'appliquer l'abonnement requis au périphérique.

Étude de cas 5. Non-conformité (OOC)

S'il n'y a aucun droit pour les abonnements FTD, la licence Smart FMC passe à l'état de non-conformité (OOC) :

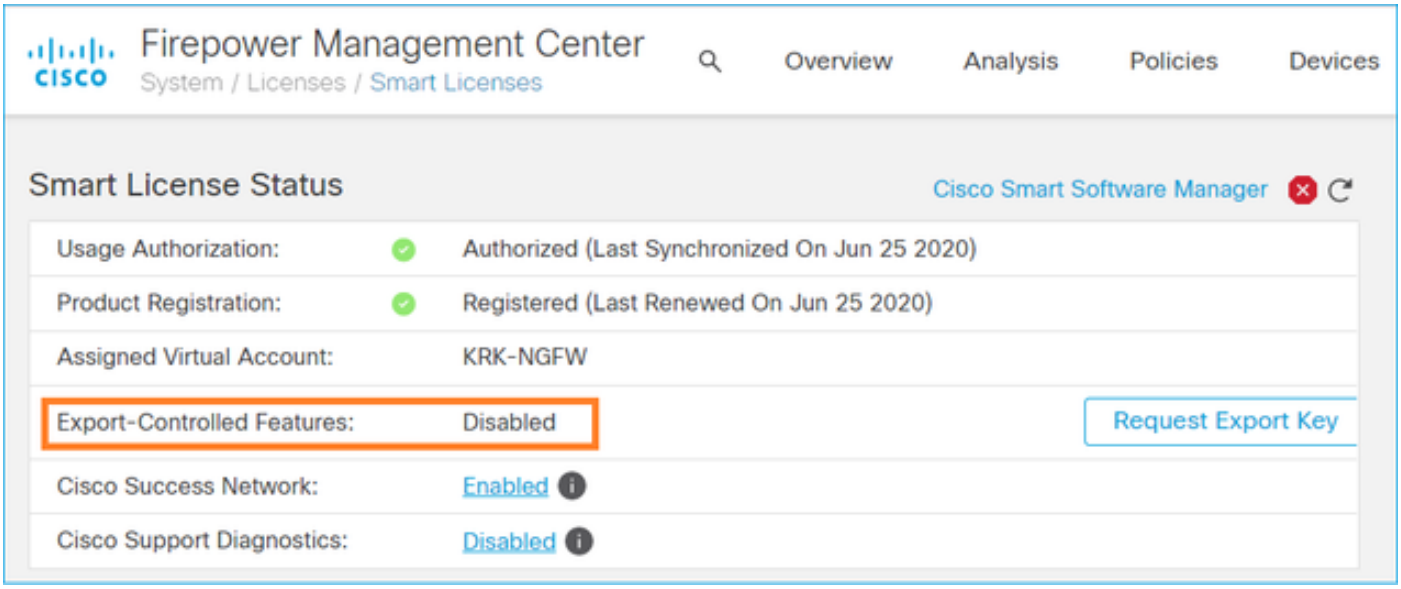


Dans le CSSM, recherchez les erreurs dans les alertes :



Étude de cas 6. Aucun chiffrement fort

Si seule la licence de base est utilisée, le cryptage DES (Data Encryption Standard) est activé dans le moteur FTD LINA. Dans ce cas, les déploiements tels que le réseau privé virtuel L2L (VPN) avec des algorithmes plus puissants échouent :



Résolution : enregistrez le FMC sur le CSSM et activez un attribut de chiffrement fort.

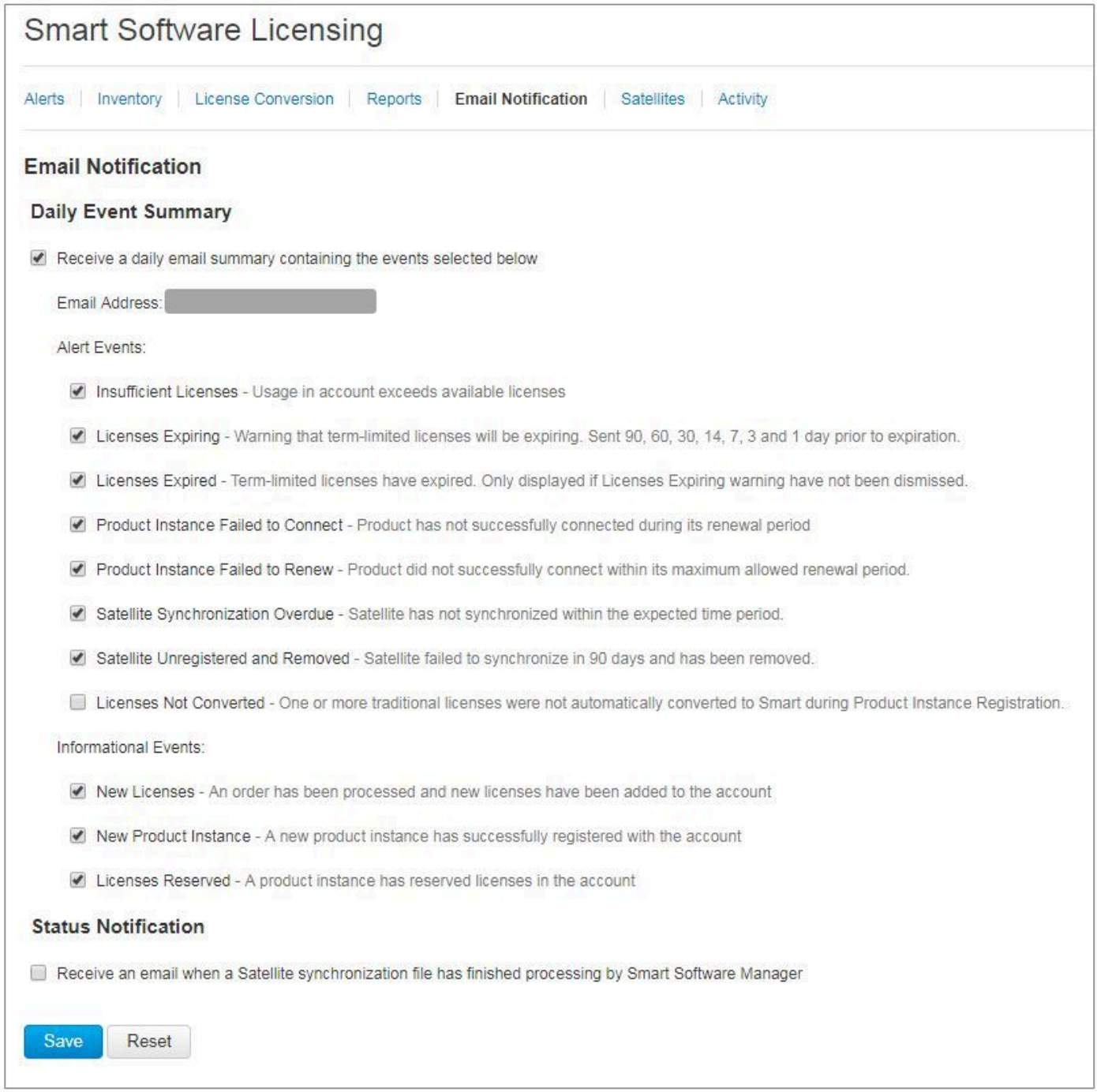
Notes supplémentaires

Définir la notification d'état de licence Smart

Notification par e-mail par SSM

Du côté SSM, la notification par e-mail SSM permet la réception d'e-mails récapitulatifs pour divers événements. Par exemple, une notification pour un manque de licence ou pour des licences qui sont sur le point d'expirer. Des notifications de connexion d'instance de produit ou d'échec de mise à jour peuvent être reçues.

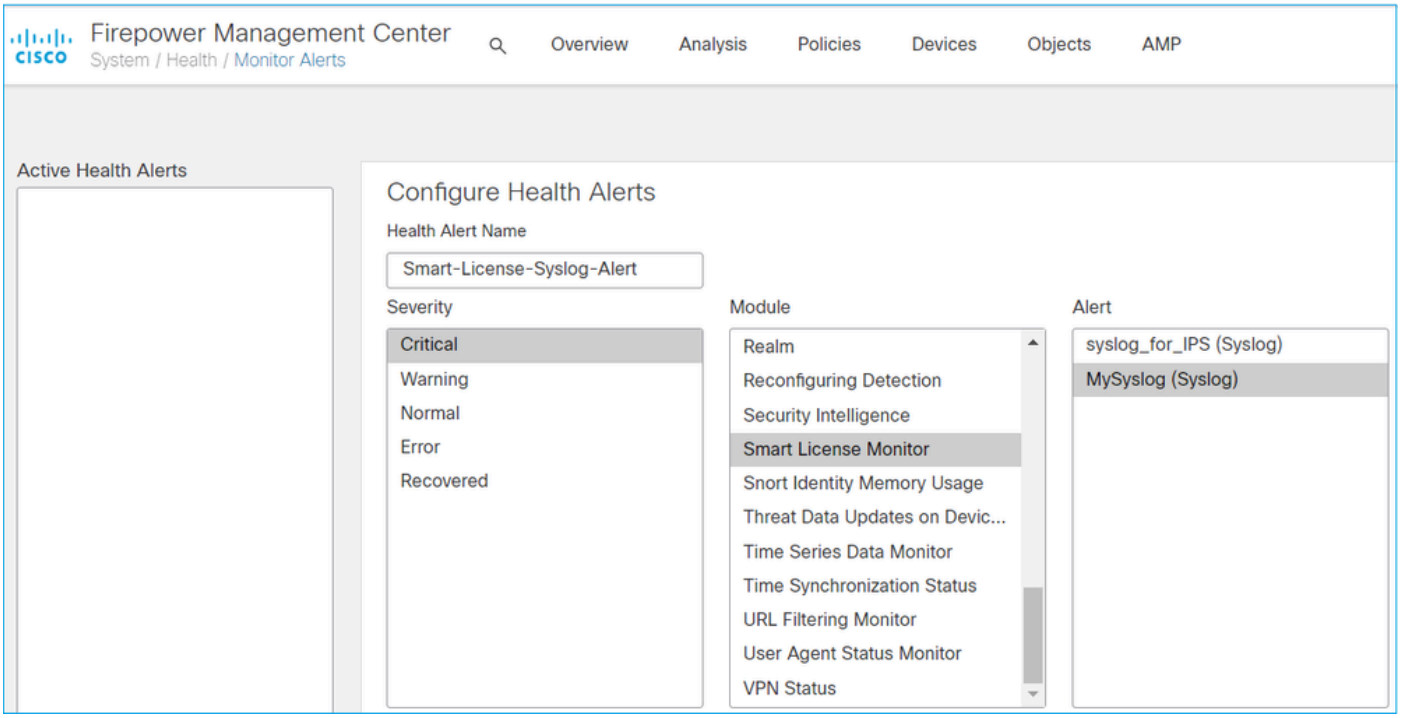
Cette fonction est très utile pour signaler et empêcher l'apparition de restrictions fonctionnelles dues à l'expiration de la licence.



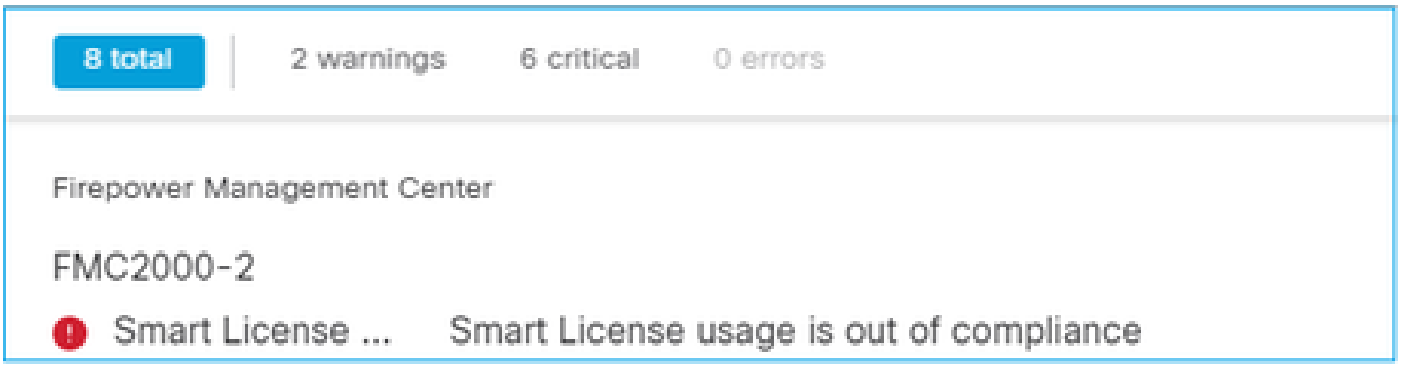
Obtenir des notifications d'alerte d'intégrité du FMC

Côté FMC, il est possible de configurer une alerte Health Monitor et de recevoir une notification d'alerte d'un événement d'intégrité. Le module Smart License Monitor est disponible pour vérifier l'état de la licence Smart. L'alerte de surveillance prend en charge les déroutements Syslog, Email et SNMP.

Voici un exemple de configuration pour obtenir un message Syslog lorsqu'un événement Smart License monitor se produit :



Voici un exemple d'alerte d'état de santé :



Le message Syslog généré par le FMC est le suivant :

<#root>

```
Mar 13 18:47:10 xx.xx.xx.xx Mar 13 09:47:10 FMC :
```

`HMNOTIFY: Smart License Monitor (Sensor FMC)`

```
: Severity: critical: Smart License usage is out of compliance
```

Reportez-vous à la Surveillance de l'état pour plus de détails sur les alertes de la Surveillance de l'état.

Plusieurs FMC sur le même compte Smart

Lorsque plusieurs FMC sont utilisés sur le même compte Smart, chaque nom d'hôte FMC doit être unique. Lorsque plusieurs FMC sont gérés dans CSSM, pour distinguer chaque FMC, le nom d'hôte de chaque FMC doit être unique. Ceci est utile pour la maintenance de la licence Smart FMC en cours d'utilisation.

FMC doit maintenir la connectivité Internet

Après l'enregistrement, le FMC vérifie le cloud de licences Smart et l'état des licences tous les 30 jours. Si le FMC ne peut pas communiquer pendant 90 jours, la fonction sous licence est conservée, mais elle conserve l'état Authorization Expired. Même dans cet état, le FMC tente en permanence de se connecter au cloud de licences Smart.

Déployer plusieurs FMCv

Lorsque le système Firepower est utilisé dans un environnement virtuel, le clonage (à chaud ou à froid) n'est pas officiellement pris en charge. Chaque FMCv (Firepower Management Center virtual) est unique car il contient des informations d'authentification. Pour déployer plusieurs FMCv, le FMCv doit être créé un par un à partir du fichier OVF (Open Virtualization Format). Pour plus d'informations sur cette limitation, reportez-vous au Guide de démarrage rapide du déploiement de Cisco Firepower Management Center Virtual pour VMware.

Foire aux questions (FAQ)

Dans FTD HA, combien de licences de périphériques sont nécessaires ?

Lorsque deux FTD sont utilisés en haute disponibilité, une licence est requise pour chaque périphérique. Par exemple, deux licences Threat and Malware sont nécessaires si les fonctionnalités Intrusive Protection System (IPS) et Advanced Malware Protection (AMP) sont utilisées sur la paire FTD HA.

Pourquoi aucune licence AnyConnect n’est-elle utilisée par FTD ?

Après l'enregistrement FMC sur le compte Smart, assurez-vous que la licence AnyConnect est activée. Pour activer la licence, accédez àFMC > Devices, sélectionnez votre périphérique, puis License. Sélectionnez l'icône Crayon, choisissez la licence qui est déposée dans le compte Smart, puis sélectionnez Enregistrer.

Pourquoi une seule licence AnyConnect est-elle « En cours d'utilisation » dans le compte Smart lorsque 100 utilisateurs sont connectés ?

Ce comportement est normal, car le compte Smart effectue le suivi du nombre d'appareils pour lesquels cette licence est activée et qui n'ont pas d'utilisateurs actifs connectés.

Pourquoi y a-t-il une erreur Device does not have the AnyConnect License après la configuration et le déploiement d'un VPN d'accès à distance par le FMC ?

Assurez-vous que le FMC est enregistré dans le cloud de licences Smart. Le comportement attendu est que la configuration d'accès à distance ne peut pas être déployée lorsque le FMC n'est pas enregistré ou en mode Évaluation. Si le FMC est enregistré, assurez-vous que la licence AnyConnect existe dans votre compte Smart et qu'elle est attribuée au périphérique.

Pour attribuer une licence, naviguer par Périphériques FMC, sélectionnez votre périphérique, Licence (icône Crayon). Sélectionnez la licence dans le compte Smart et sélectionnez Enregistrer.

Pourquoi y a-t-il une erreur Remote Access VPN with SSL cannot be deployed when Export-Controlled Features (Strong-crypto) are disabled lorsqu'il y a un déploiement d'une configuration VPN d'accès à distance ?

Le VPN d'accès à distance déployé sur le FTD nécessite une licence de cryptage fort pour être activé. EnAssurez-vous qu'une licence de cryptage fort est activée sur le FMC. Pour vérifier l'état de la licence de chiffrement fort, naviguer à la Système FMC > Licences > Licence Smartet vérifiez que les fonctionnalités d'exportation contrôlée sont activées.

Comment activer une licence de cryptage fort si Export-Controlled Features est désactivé ?

Cette fonctionnalité est activée automatiquement si l'option Autoriser la fonctionnalité de contrôle d'exportation sur les produits enregistrés avec cette fonctionnalité est activée pour le jeton utilisé lors de l'enregistrement du FMC sur le cloud de comptes Smart. Si cette option n'est pas activée pour le jeton, annulez l'enregistrement du FMC et réenregistrez-le avec cette option activée.

Que faire si l'option « Autoriser la fonctionnalité contrôlée par exportation sur les produits enregistrés avec ce jeton » n'est pas disponible lors de la génération du jeton ?

Contactez votre équipe de compte Cisco.

Pourquoi l'erreur « Strong crypto (c'est-à-dire que l'algorithme de chiffrement est supérieur à DES) pour la topologie VPN s2s n'est pas prise en charge » est-elle reçue ?

Cette erreur s'affiche lorsque le FMC utilise le mode Évaluation ou lorsque le compte de licence Smart n'a pas droit à une licence de chiffrement fort. VVérifiez que le FMC est enregistré auprès de l'autorité de licence et que la fonctionnalité d'autorisation d'exportation contrôlée sur les produits enregistrés avec ce jeton est activée. Si le compte Smart n'est pas autorisé à utiliser une licence de chiffrement fort, le déploiement de la configuration site à site VPN avec des chiffrements plus forts que DES n'est pas autorisé.

Pourquoi un état « Non conforme » sur le CSP est-il reçu ?

Le périphérique peut devenir non conforme lorsque l'un des périphériques gérés utilise des licences non disponibles.

Comment peut-on corriger l'état « Non conforme » ?

Suivez les étapes décrites dans le Guide de configuration de Firepower :

1. Consultez la section Licences Smart au bas de la page pour déterminer les licences nécessaires.

2. Achetez les licences requises par le biais de vos canaux habituels.

3. Dans Cisco Smart Software Manager (https://software.cisco.com/#SmartLicensing-Inventory), vérifiez que les licences apparaissent dans votre compte virtuel.

4. Dans le FMC, sélectionnez System > Licenses > Smart Licenses.

5. Sélectionnez Re-Authorize.

La procédure complète se trouve dans Licence du système Firepower.

Quelles sont les fonctionnalités de Firepower Threat Defense Base ?

La licence de base permet :

- Configuration des périphériques FTD pour commuter et router (qui inclut le relais DHCP et la NAT).
- Configuration des périphériques FTD en mode haute disponibilité (HA).
- Configuration des modules de sécurité en tant que cluster dans un châssis Firepower 9300 (cluster intra-châssis).
- Configuration des périphériques Firepower 9300 ou Firepower 4100 (FTD) en tant que cluster (cluster inter-châssis).
- Configuration du contrôle des utilisateurs et des applications et ajout de conditions d'utilisateur et d'application aux règles de contrôle d'accès

Comment peut-on obtenir la licence de fonctionnalités Firepower Threat Defense Base ?

Une licence de base est automatiquement incluse à chaque achat d'un périphérique virtuel Firepower Threat Defense ou Firepower Threat Defense. Il est automatiquement ajouté à votre compte Smart lorsque le FTD s'enregistre auprès du FMC.

Quelles adresses IP doivent être autorisées dans le chemin entre le FMC et le nuage de licences Smart ?

Le FMC utilise l’adresse IP sur le port 443 pour communiquer avec le cloud de licences Smart.

Cette adresse IP (https://tools.cisco.com)est résolu en ces adresses IP :

- 72.163.4.38
- 173.37.145.8

Pour les versions FMC supérieures à 7.3, il se connecte à https://smartreceiver.cisco.com qui se résout à ces adresses IP :

- 146,112,59,81

Informations connexes

- Guides de configuration de Firepower Management Center
- Présentation de Cisco Live Smart Licensing : BRKARC-2034
- Licences de fonctions Cisco Secure Firewall Management Center
- Foire aux questions (FAQ) sur les licences logicielles Cisco Smart

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.