Dépannage de la licence Smart ASA sur les appliances FXOS Firepower

Table des matières

Introduction

Ce document décrit la fonction de licence intelligente de l'appliance de sécurité adaptative (ASA) sur Firepower eXtensible Operating System (FXOS).

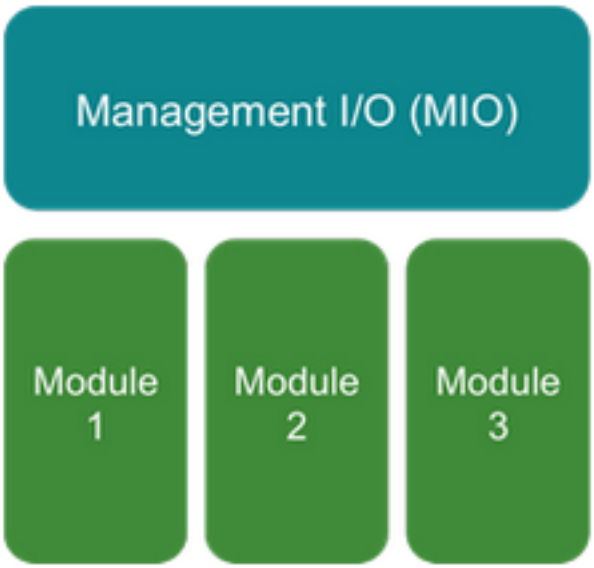
Informations générales

La licence Smart sur FXOS est utilisée lorsqu'un ASA est installé sur le châssis. Pour Firepower Threat Defense (FTD) et Firepower Management Center (FMC), vérifiez l'enregistrement et le dépannage des licences Smart FMC et FTD.

Ce document couvre principalement les scénarios où le châssis FXOS a un accès direct à Internet. Si votre châssis FXOS ne peut pas accéder à Internet, vous devez envisager un serveur satellite ou une réservation de licence permanente (PLR). Consultez le guide de configuration de FXOS pour plus de détails sur la gestion hors connexion.

Architecture de licences Smart

Présentation générale des composants du châssis :

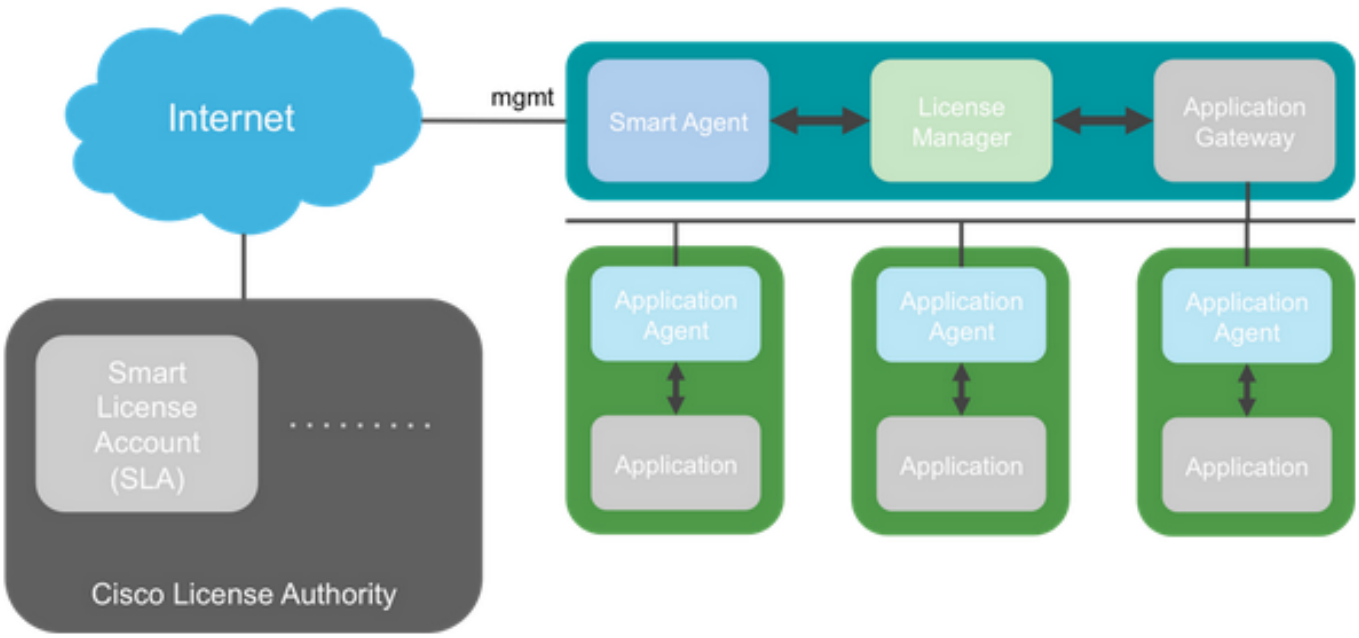


- Les modules MIO (Management Input/Output) et les modules individuels jouent un rôle dans la gestion des licences Smart
- MIO elle-même ne nécessite aucune licence pour son fonctionnement
- Les applications SA de chaque module doivent être sous licence

Le superviseur FXOS est le MIO. Le MIO comprend trois composants principaux :

- Agent intelligent
- Gestionnaire de licences
- AppAG

Architecture globale



Nomenclature

Terme	Description

Autorité de licence Cisco	Le serveur principal de licences Cisco pour les licences Smart. Conserve toutes les informations relatives aux licences de produits. Cela inclut les droits et les informations sur les périphériques.
Compte de licence Smart	Compte disposant de tous les droits pour l'appliance.
ID de jeton	Un identificateur est utilisé pour distinguer le compte de licence Smart lorsque l'appliance est enregistrée.
Droit	Équivalent à une licence. Correspond à une fonction individuelle ou à un niveau de fonction entier.
Clé d'activation de produit (PAK)	Ancien mécanisme de licence. Lié à un seul appareil.

États des agents Smart

Province	Description
Non Configuré	Les licences Smart ne sont pas activées.
Non Identifié	La licence Smart a été activée, mais Smart Agent n'a pas encore contacté Cisco pour s'enregistrer.
Enregistré	L'agent a contacté l'autorité de gestion des licences Cisco et s'est enregistré.
Autorisé	Lorsqu'un agent reçoit un état de non-conformité en réponse à une demande d'autorisation d'habilitation.
Non-conformité (OOC)	Lorsqu'un agent reçoit un état OOC en réponse à une demande d'autorisation d'habilitation.
Autorisation expirée	Si l'agent n'a pas communiqué avec Cisco depuis 90 jours.

Droits ASA

Voici les droits ASA pris en charge :

- Niveau standard
- Multicontexte
- Cryptage fort (3DES)
- Mobile/fournisseur de services (GTP)

Configuration

Suivez les instructions de ces documents :

- Licences logicielles intelligentes (ASAv, ASA sur Firepower)
- Gestion des licences pour l'ASA

Avant toute configuration de niveau de fonctionnalité :

```
asa(config-smart-lic)# show license all
Smart licensing enabled: Yes

Compliance status: In compliance
```

```
Overall licensed status: Invalid (0)

No entitlements in use

Serial Number:  FCH12345ABC

License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 1024
Inside Hosts                      : Unlimited
Failover                          : Active/Active
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Enabled
Security Contexts                 : 10
Carrier                           : Disabled
AnyConnect Premium Peers          : 20000
AnyConnect Essentials             : Disabled
Other VPN Peers                   : 20000
Total VPN Peers                   : 20000
AnyConnect for Mobile             : Enabled
AnyConnect for Cisco VPN Phone    : Enabled
Advanced Endpoint Assessment      : Enabled
Shared License                    : Disabled
Total TLS Proxy Sessions          : 15000
Cluster                           : Enabled

**************************************************************************
*                                WARNING                                 *
*                                                                        *
*    THIS DEVICE IS NOT LICENSED WITH A VALID FEATURE TIER ENTITLEMENT    *
*                                                                        *
**************************************************************************
```

Configurer le niveau standard :

```
asa(config)# license smart
INFO: License(s) corresponding to an entitlement will be activated only after an entitlement
request has been authorized.
asa(config-smart-lic)# feature tier standard
asa(config-smart-lic)# show license all

Smart licensing enabled: Yes

Compliance status: In compliance

Overall licensed status: Authorized (3)

Entitlement(s):

Feature tier:
Tag: regid.2015-10.com.cisco.FIREPOWER_4100_ASA_STANDARD,1.0_7d7f5ee2-1398-4b0e-aced-
b3f7fb1cacfc
Version: 1.0
Enforcement mode: Authorized
Handle: 1
Requested time: Tue, 04 Aug 2020 07:58:13 UTC
Requested count: 1
Request status: Complete
```

```
Serial Number: FCH12345ABC

License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces : Unlimited
Maximum VLANs : 1024
Inside Hosts : Unlimited
Failover : Active/Active
Encryption-DES : Enabled
Encryption-3DES-AES : Enabled
Security Contexts : 10
Carrier : Disabled
AnyConnect Premium Peers : 20000
AnyConnect Essentials : Disabled
Other VPN Peers : 20000
Total VPN Peers : 20000
AnyConnect for Mobile : Enabled
AnyConnect for Cisco VPN Phone : Enabled
Advanced Endpoint Assessment : Enabled
Shared License : Disabled
Total TLS Proxy Sessions : 15000
Clustetext
```

Basculement (haute disponibilité)

Comme indiqué dans le Guide de configuration ASA, chaque unité Firepower doit être enregistrée auprès de l'autorité de licence ou du serveur satellite. Vérification depuis l'interface CLI ASA :

```
asa# show failover | include host
        This host: Primary - Active
       Other host: Secondary - Standby Ready

asa# show license all

Smart licensing enabled: Yes

Compliance status: In compliance

Overall licensed status: Authorized (3)

Entitlement(s):

Feature tier:
       Tag: regid.2015-10.com.cisco.FIREPOWER_4100_ASA_STANDARD,1.0_7d7f5ee2-1398-4b0e-aced-
b3f7fb1cacfc
       Version: 1.0
       Enforcement mode: Authorized
       Handle: 1
       Requested time: Tue, 04 Aug 2020 07:58:13 UTC
       Requested count: 1
       Request status: Complete

Serial Number:  FCH12345ABC

License mode: Smart Licensing

Licensed features for this platform:
```

```
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 1024
Inside Hosts                      : Unlimited
Failover                          : Active/Active
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Enabled
Security Contexts                 : 10
Carrier                           : Disabled
AnyConnect Premium Peers          : 20000
AnyConnect Essentials             : Disabled
Other VPN Peers                   : 20000
Total VPN Peers                   : 20000
AnyConnect for Mobile             : Enabled
AnyConnect for Cisco VPN Phone    : Enabled
Advanced Endpoint Assessment      : Enabled
Shared License                    : Disabled
Total TLS Proxy Sessions          : 15000
Cluster                           : Enabled

Failover cluster licensed features for this platform:
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 1024
Inside Hosts                      : Unlimited
Failover                          : Active/Active
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Enabled
Security Contexts                 : 20
Carrier                           : Disabled
AnyConnect Premium Peers          : 20000
AnyConnect Essentials             : Disabled
Other VPN Peers                   : 20000
Total VPN Peers                   : 20000
AnyConnect for Mobile             : Enabled
AnyConnect for Cisco VPN Phone    : Enabled
Advanced Endpoint Assessment      : Enabled
Shared License                    : Disabled
Total TLS Proxy Sessions          : 15000
Cluster                           : Enabled
```

L'unité en veille :

```
asa# show failover | i host
       This host: Secondary - Standby Ready
       Other host: Primary - Active

asa# show license all

Smart licensing enabled: Yes

Compliance status: In compliance

Overall licensed status: Not applicable in standby state

No entitlements in use

Serial Number:  FCH12455DEF

License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited
```

```
Maximum VLANs                    : 1024
Inside Hosts                     : Unlimited
Failover                         : Active/Active
Encryption-DES                   : Enabled
Encryption-3DES-AES              : Disabled
Security Contexts                : 10
Carrier                          : Disabled
AnyConnect Premium Peers         : 20000
AnyConnect Essentials            : Disabled
Other VPN Peers                  : 20000
Total VPN Peers                  : 20000
AnyConnect for Mobile            : Enabled
AnyConnect for Cisco VPN Phone   : Enabled
Advanced Endpoint Assessment     : Enabled
Shared License                   : Disabled
Total TLS Proxy Sessions         : 15000
Cluster                          : Enabled

Failover cluster licensed features for this platform:
Maximum Physical Interfaces      : Unlimited
Maximum VLANs                    : 1024
Inside Hosts                     : Unlimited
Failover                         : Active/Active
Encryption-DES                   : Enabled
Encryption-3DES-AES              : Enabled
Security Contexts                : 20
Carrier                          : Disabled
AnyConnect Premium Peers         : 20000
AnyConnect Essentials            : Disabled
Other VPN Peers                  : 20000
Total VPN Peers                  : 20000
AnyConnect for Mobile            : Enabled
AnyConnect for Cisco VPN Phone   : Enabled
Advanced Endpoint Assessment     : Enabled
Shared License                   : Disabled
Total TLS Proxy Sessions         : 15000
Cluster                          : Enabled
```

Étude de cas : Licence ASA HA sur FP2100

- Sur le 2100, l'ASA communique avec le portail Cisco Smart Licensing (cloud) via les interfaces ASA, et non via la gestion FXOS
- Vous devez enregistrer les deux ASA sur le portail Cisco Smart Licensing (cloud)

Dans ce cas, l'authentification locale HTTP est utilisée sur une interface externe :

```
ciscoasa(config)# show run http
http server enable
http 0.0.0.0 0.0.0.0 outside
ciscoasa(config)# show run aaa
aaa authentication http console LOCAL
ciscoasa(config)# show run username
username cisco password ***** pbkdf2
```

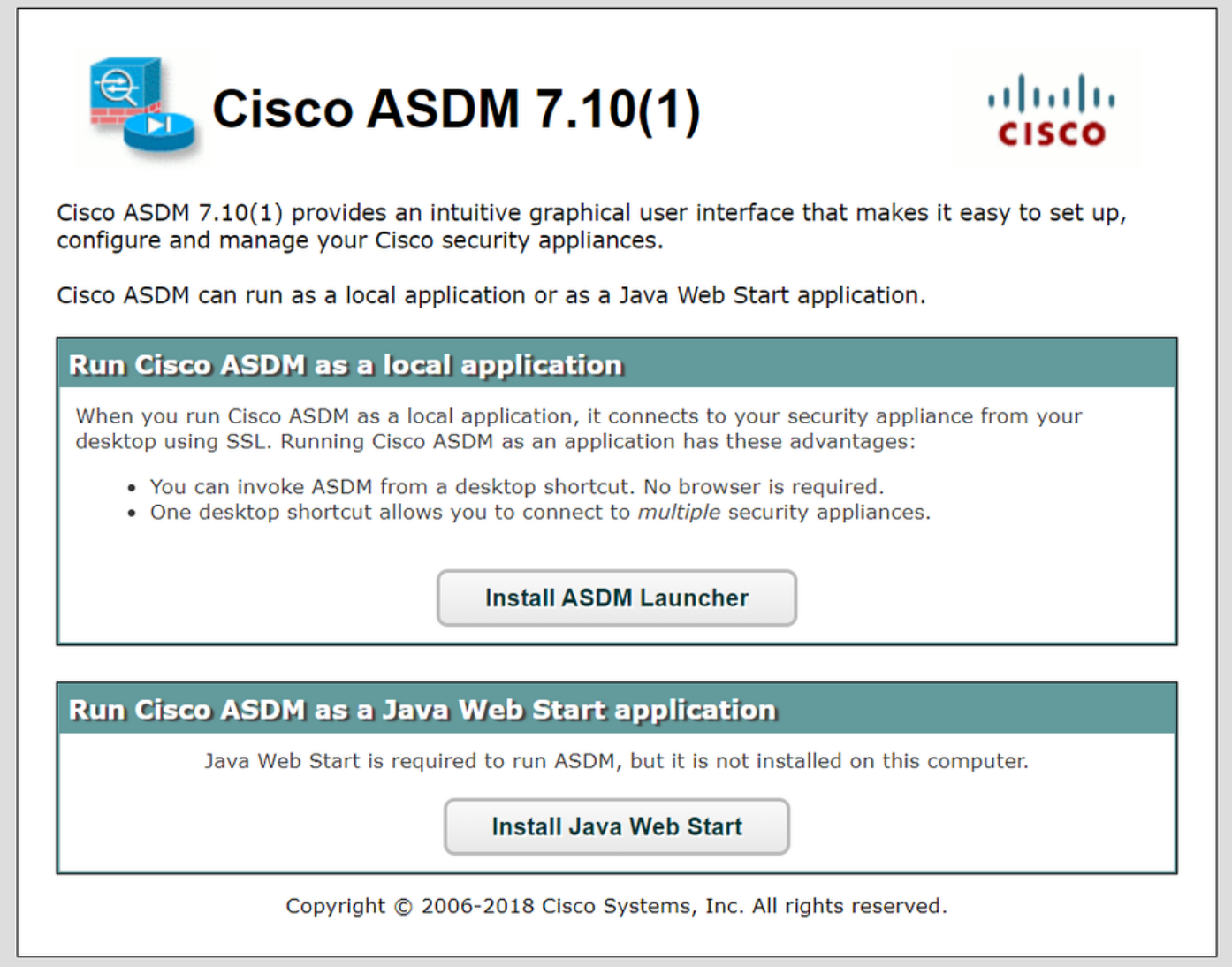
Vous ne pouvez vous connecter à l'ASA via l'ASDM que si une licence 3DES/AES est activée. Pour un ASA qui n'est pas déjà enregistré, cela est possible uniquement sur une interface qui est management-only. Selon le guide de configuration : « Strong Encryption (3DES/AES) est disponible pour les connexions de gestion avant de vous connecter à l'autorité de licence ou au serveur

satellite afin que vous puissiez lancer ASDM. Notez que l'accès ASDM est uniquement disponible sur les interfaces de gestion uniquement avec le cryptage par défaut. Le trafic prêt à l'emploi n'est pas autorisé tant que vous ne vous connectez pas et que vous n'obtenez pas la licence de chiffrement fort. Dans un autre cas, vous obtenez :

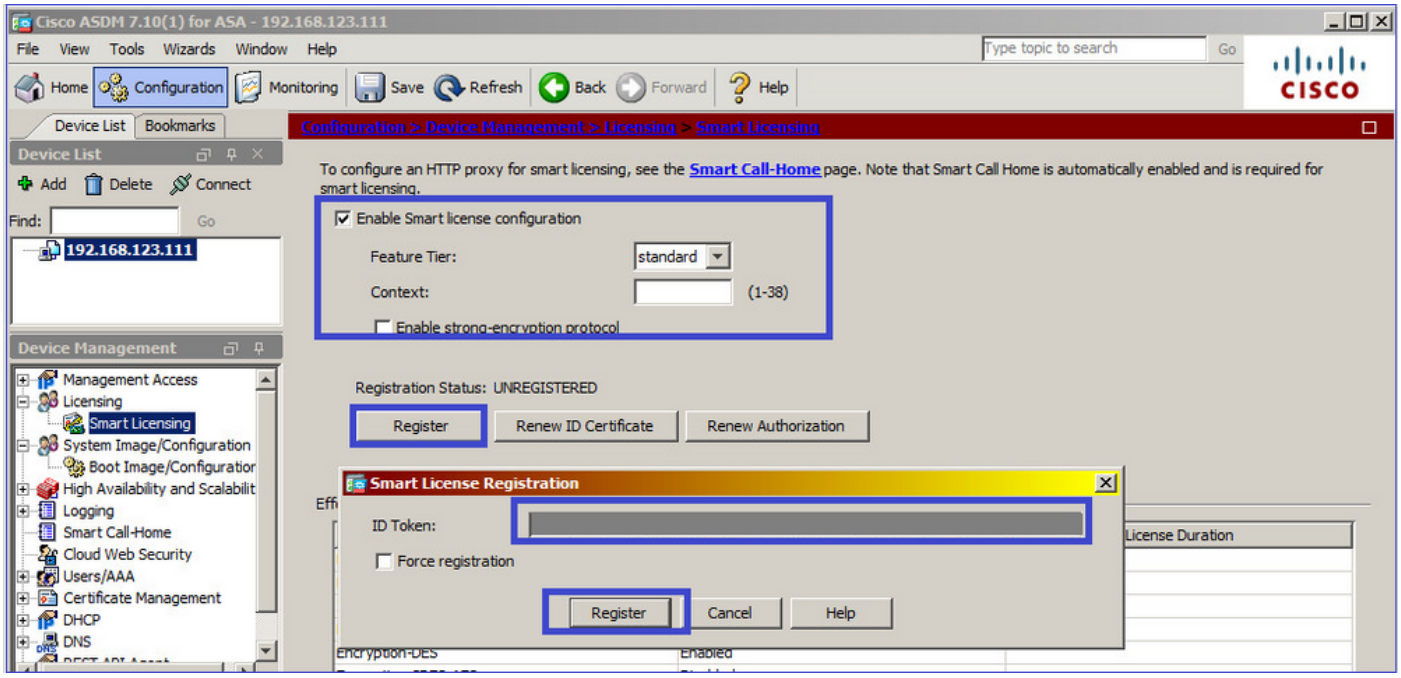
```
ciscoasa(config)# debug ssl 255
debug ssl enabled at level 255.
error:1408A0C1:SSL routines:ssl3_get_client_hello:no shared cipher
```

Pour contourner l'ASA a la gestion seulement configuré sur l'interface Internet et donc la connexion ASDM est possible :

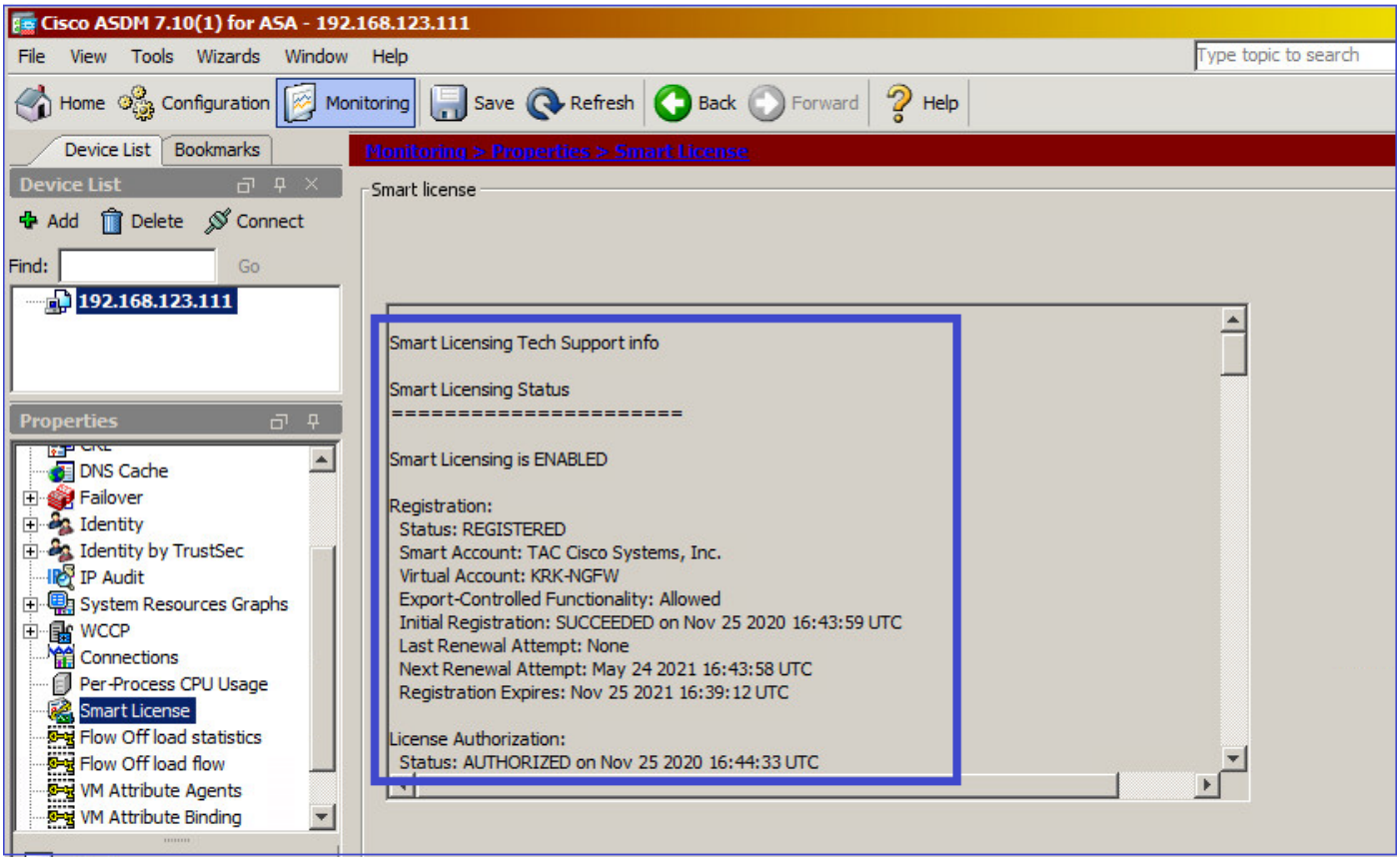
```
interface Ethernet1/2
management-only
nameif outside
security-level 100
ip address 192.168.123.111 255.255.255.0 standby 192.168.123.112
```



Configurez la licence Smart sur l'ASA principal :



Naviguez jusqu'à **Monitoring > Properties > Smart License** pour vérifier l'état de l'enregistrement :



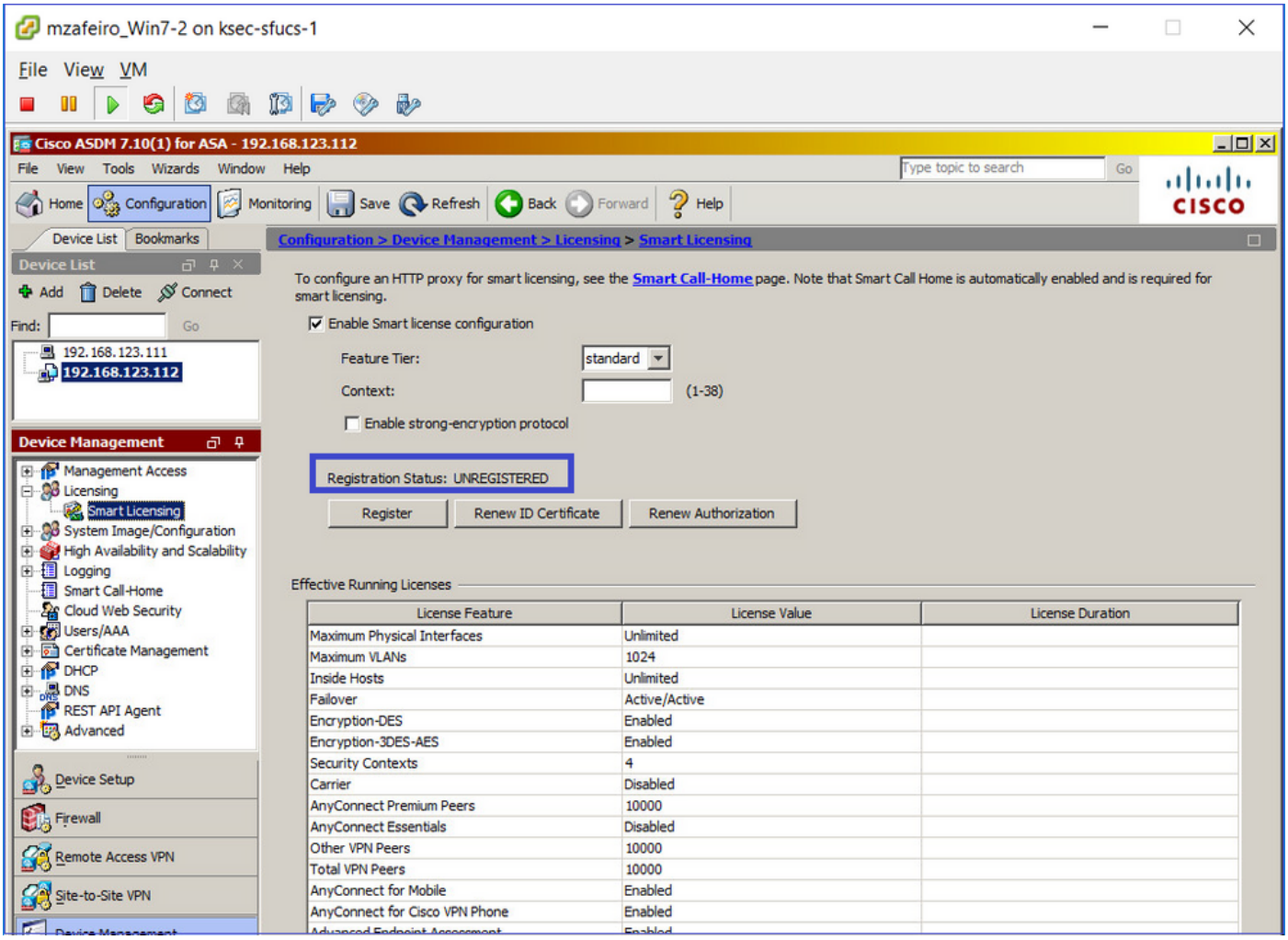
Vérification de l'interface CLI ASA principale :

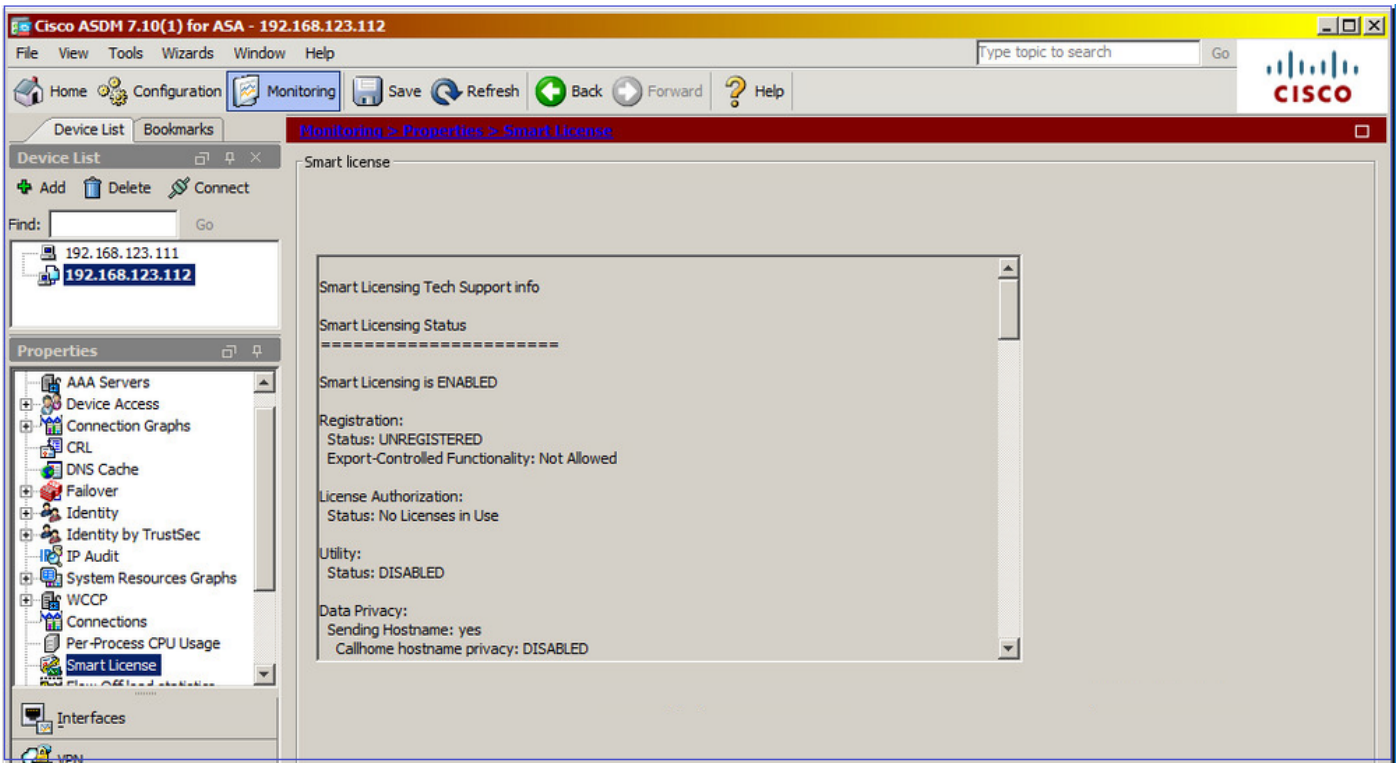
```
ciscoasa/pri/act# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED
```

```
Registration:
Status: REGISTERED
Smart Account: Cisco Systems, Inc.
Virtual Account: NGFW
Export-Controlled Functionality: Allowed
Initial Registration: SUCCEEDED on Nov 25 2020 16:43:59 UTC
Last Renewal Attempt: None
Next Renewal Attempt: May 24 2021 16:43:58 UTC
Registration Expires: Nov 25 2021 16:39:12 UTC

License Authorization:
Status: AUTHORIZED on Nov 25 2020 16:47:42 UTC
Last Communication Attempt: SUCCEEDED on Nov 25 2020 16:47:42 UTC
Next Communication Attempt: Dec 25 2020 16:47:41 UTC
Communication Deadline: Feb 23 2021 16:42:46 UTC

Utility:
Status: DISABLED

Data Privacy:
Sending Hostname: yes
Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
Type: Callhome

License Usage
==============

Firepower 2100 ASA Standard (FIREPOWER_2100_ASA_STANDARD):
Description: Firepower 2100 ASA Standard
Count: 1
Version: 1.0
Status: AUTHORIZED

Product Information
===================
UDI: PID:FPR-2140,SN:JAD12345ABC

Agent Version
=============
Smart Agent for Licensing: 4.3.6_rel/38

ciscoasa/pri/act# show run license
license smart
feature tier standard

ciscoasa/pri/act# show license features
Serial Number: JAD12345ABC
Export Compliant: YES

License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces : Unlimited
Maximum VLANs : 1024
Inside Hosts : Unlimited
Failover : Active/Active
Encryption-DES : Enabled
Encryption-3DES-AES : Enabled
```

```
Security Contexts : 2
Carrier : Disabled
AnyConnect Premium Peers : 10000
AnyConnect Essentials : Disabled
Other VPN Peers : 10000
Total VPN Peers : 10000
AnyConnect for Mobile : Enabled
AnyConnect for Cisco VPN Phone : Enabled
Advanced Endpoint Assessment : Enabled
Shared License : Disabled
Total TLS Proxy Sessions : 10000
Cluster : Disabled


Failover cluster licensed features for this platform:
Maximum Physical Interfaces : Unlimited
Maximum VLANs : 1024
Inside Hosts : Unlimited
Failover : Active/Active
Encryption-DES : Enabled
Encryption-3DES-AES : Enabled
Security Contexts : 4
Carrier : Disabled
AnyConnect Premium Peers : 10000
AnyConnect Essentials : Disabled
Other VPN Peers : 10000
Total VPN Peers : 10000
AnyConnect for Mobile : Enabled
AnyConnect for Cisco VPN Phone : Enabled
Advanced Endpoint Assessment : Enabled
Shared License : Disabled
Total TLS Proxy Sessions : 10000
Cluster : Disabled
```

Connectez-vous via l'ASDM à l'ASA de secours (cela n'est possible que si l'ASA a été configuré avec une adresse IP de secours). L'ASA de secours est représenté comme suit : UNREGISTERED et ceci est attendu car il n'a pas encore été enregistré sur le portail Smart Licensing :





L'interface CLI ASA en veille affiche :

```
ciscoasa/sec/stby# show license all
```

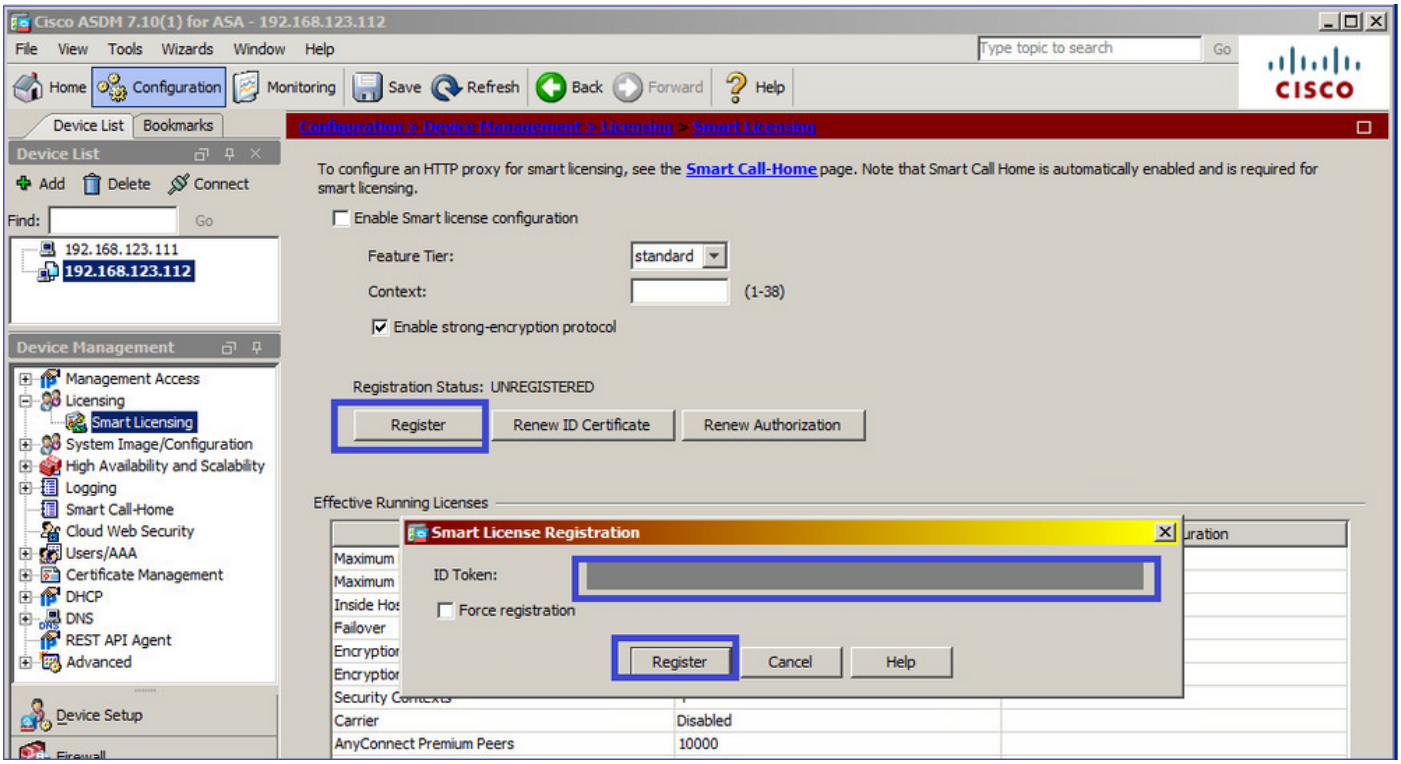
```
Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
Status: UNREGISTERED
Export-Controlled Functionality: Not Allowed

License Authorization:
Status: No Licenses in Use

Utility:
Status: DISABLED

Data Privacy:
Sending Hostname: yes
Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
Type: Callhome

License Usage
==============

No licenses in use

Product Information
===================
UDI: PID:FPR-2140,SN:JAD123456A

Agent Version
=============
Smart Agent for Licensing: 4.3.6_rel/38
ciscoasa/sec/stby# show run license
license smart
feature tier standard
```

Les fonctionnalités de licence activées sur l'ASA de secours :

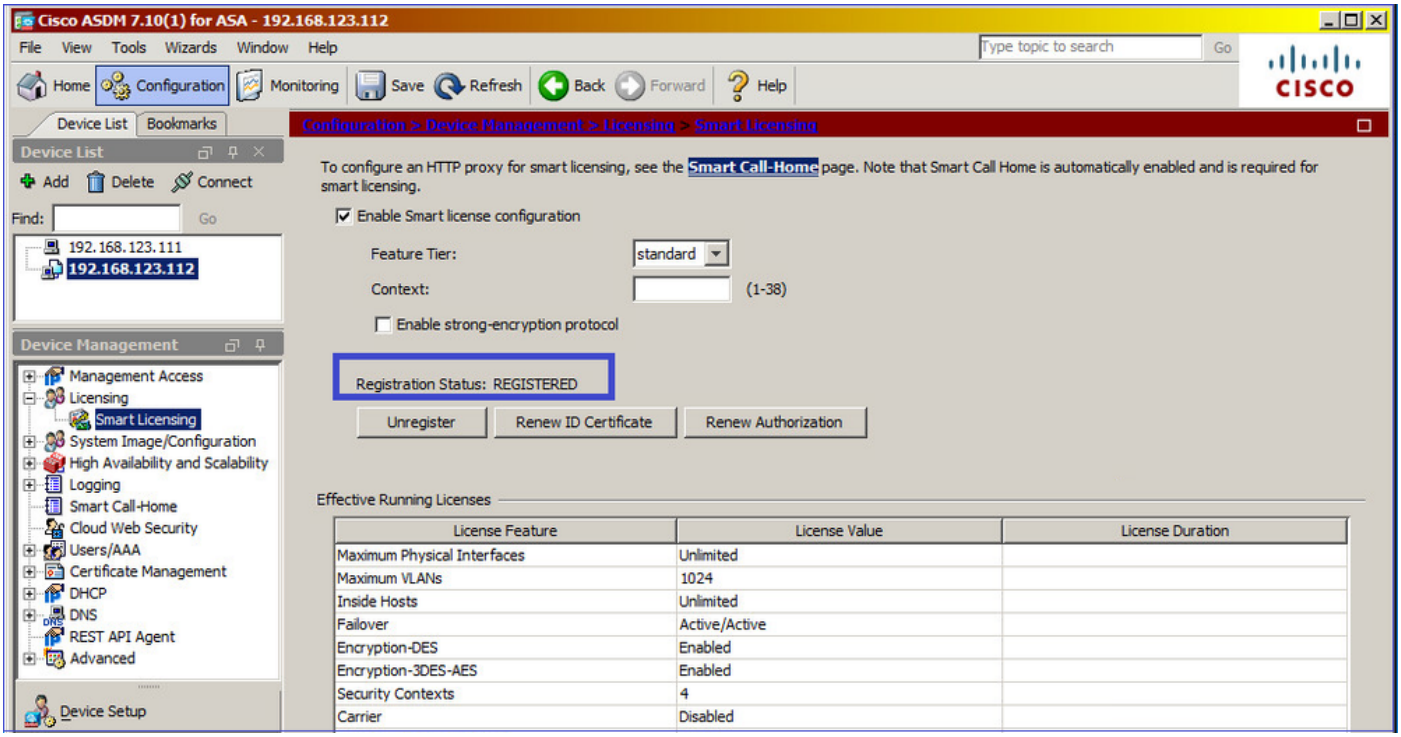
```
ciscoasa/sec/stby# show license features
Serial Number: JAD123456A
Export Compliant: NO

License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces : Unlimited
Maximum VLANs : 1024
Inside Hosts : Unlimited
Failover : Active/Active
Encryption-DES : Enabled
Encryption-3DES-AES : Disabled
Security Contexts : 2
Carrier : Disabled
AnyConnect Premium Peers : 10000
AnyConnect Essentials : Disabled
Other VPN Peers : 10000
Total VPN Peers : 10000
```

```
AnyConnect for Mobile : Enabled
AnyConnect for Cisco VPN Phone : Enabled
Advanced Endpoint Assessment : Enabled
Shared License : Disabled
Total TLS Proxy Sessions : 10000
Cluster : Disabled


Failover cluster licensed features for this platform:
Maximum Physical Interfaces : Unlimited
Maximum VLANs : 1024
Inside Hosts : Unlimited
Failover : Active/Active
Encryption-DES : Enabled
Encryption-3DES-AES : Enabled
Security Contexts : 4
Carrier : Disabled
AnyConnect Premium Peers : 10000
AnyConnect Essentials : Disabled
Other VPN Peers : 10000
Total VPN Peers : 10000
AnyConnect for Mobile : Enabled
AnyConnect for Cisco VPN Phone : Enabled
Advanced Endpoint Assessment : Enabled
Shared License : Disabled
Total TLS Proxy Sessions : 10000
Cluster : Disabled
```

Enregistrez l'ASA de secours :



Le résultat sur l'ASA en veille est qu'il est REGISTERED:



Vérification CLI sur ASA en veille :

```
ciscoasa/sec/stby# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
Status: REGISTERED
Smart Account: Cisco Systems, Inc.
Virtual Account: NGFW
Export-Controlled Functionality: Allowed
Initial Registration: SUCCEEDED on Nov 25 2020 17:06:51 UTC
Last Renewal Attempt: None
Next Renewal Attempt: May 24 2021 17:06:51 UTC
Registration Expires: Nov 25 2021 17:01:47 UTC

License Authorization:
Status: AUTHORIZED on Nov 25 2020 17:07:28 UTC
Last Communication Attempt: SUCCEEDED on Nov 25 2020 17:07:28 UTC
Next Communication Attempt: Dec 25 2020 17:07:28 UTC
Communication Deadline: Feb 23 2021 17:02:15 UTC

Utility:
Status: DISABLED

Data Privacy:
Sending Hostname: yes
Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
Type: Callhome
```

```
License Usage
==============

No licenses in use

Product Information
===================
UDI: PID:FPR-2140,SN:JAD123456AX

Agent Version
=============
Smart Agent for Licensing: 4.3.6_rel/38

ciscoasa/sec/stby# show license feature
Serial Number: JAD123456A
Export Compliant: YES

License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces : Unlimited
Maximum VLANs : 1024
Inside Hosts : Unlimited
Failover : Active/Active
Encryption-DES : Enabled
Encryption-3DES-AES : Enabled
Security Contexts : 2
Carrier : Disabled
AnyConnect Premium Peers : 10000
AnyConnect Essentials : Disabled
Other VPN Peers : 10000
Total VPN Peers : 10000
AnyConnect for Mobile : Enabled
AnyConnect for Cisco VPN Phone : Enabled
Advanced Endpoint Assessment : Enabled
Shared License : Disabled
Total TLS Proxy Sessions : 10000
Cluster : Disabled


Failover cluster licensed features for this platform:
Maximum Physical Interfaces : Unlimited
Maximum VLANs : 1024
Inside Hosts : Unlimited
Failover : Active/Active
Encryption-DES : Enabled
Encryption-3DES-AES : Enabled
Security Contexts : 4
Carrier : Disabled
AnyConnect Premium Peers : 10000
AnyConnect Essentials : Disabled
Other VPN Peers : 10000
Total VPN Peers : 10000
AnyConnect for Mobile : Enabled
AnyConnect for Cisco VPN Phone : Enabled
Advanced Endpoint Assessment : Enabled
Shared License : Disabled
Total TLS Proxy Sessions : 10000
Cluster : Disabled
```

Cluster ASA

Si la licence des périphériques ne correspond pas, le cluster n'est pas formé :

```
Cluster unit unit-1-1 transitioned from DISABLED to CONTROL
New cluster member unit-2-1 rejected due to encryption license mismatch
```

Une configuration de cluster réussie :

```
asa(config)# cluster group GROUP1
asa(cfg-cluster)# enable
Removed all entitlements except per-unit entitlement configuration before joining cluster as
data unit.

Detected Cluster Control Node.
Beginning configuration replication from Control Node.
.
Cryptochecksum (changed): ede485ad d7fb9644 2847deaf ba16830b
End configuration replication from Control Node.
```

Noeud de contrôle de cluster :

```
asa# show cluster info | i state
   This is "unit-1-1" in state CONTROL_NODE
   Unit "unit-2-1" in state DATA_NODE

asa# show license all

Smart licensing enabled: Yes

Compliance status: In compliance

Overall licensed status: Authorized (3)

Entitlement(s):

Feature tier:
       Tag: regid.2015-10.com.cisco.FIREPOWER_4100_ASA_STANDARD,1.0_7d7f5ee2-1398-4b0e-aced-
b3f7fb1cacfc
       Version: 1.0
       Enforcement mode: Authorized
       Handle: 2
       Requested time: Mon, 10 Aug 2020 08:12:38 UTC
       Requested count: 1
       Request status: Complete

Serial Number:  FCH12345ABC

License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 1024
Inside Hosts                      : Unlimited
Failover                          : Active/Active
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Enabled
```

```
Security Contexts                : 10
Carrier                          : Disabled
AnyConnect Premium Peers         : 20000
AnyConnect Essentials            : Disabled
Other VPN Peers                  : 20000
Total VPN Peers                  : 20000
AnyConnect for Mobile            : Enabled
AnyConnect for Cisco VPN Phone   : Enabled
Advanced Endpoint Assessment     : Enabled
Shared License                   : Disabled
Total TLS Proxy Sessions         : 15000
Cluster                          : Enabled

Failover cluster licensed features for this platform:
Maximum Physical Interfaces      : Unlimited
Maximum VLANs                    : 1024
Inside Hosts                     : Unlimited
Failover                         : Active/Active
Encryption-DES                   : Enabled
Encryption-3DES-AES              : Enabled
Security Contexts                : 20
Carrier                          : Disabled
AnyConnect Premium Peers         : 20000
AnyConnect Essentials            : Disabled
Other VPN Peers                  : 20000
Total VPN Peers                  : 20000
AnyConnect for Mobile            : Enabled
AnyConnect for Cisco VPN Phone   : Enabled
Advanced Endpoint Assessment     : Enabled
Shared License                   : Disabled
Total TLS Proxy Sessions         : 15000
Cluster                          : Enabled
```

Unité de données de cluster :

```
asa# show cluster info | i state
   This is "unit-2-1" in state DATA_NODE
   Unit "unit-1-1" in state CONTROL_NODE

asa# show license all

Smart licensing enabled: Yes

Compliance status: In compliance

Overall licensed status: Authorized (3)

Entitlement(s):

Strong encryption:
       Tag: regid.2015-10.com.cisco.FIREPOWER_4100_ASA_ENCRYPTION,1.0_052986db-c5ad-40da-97b1-
ee0438d3b2c9
       Version: 1.0
       Enforcement mode: Authorized
       Handle: 3
       Requested time: Mon, 10 Aug 2020 07:29:45 UTC
       Requested count: 1
       Request status: Complete

Serial Number:  FCH12345A6B
```

```
License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 1024
Inside Hosts                      : Unlimited
Failover                          : Active/Active
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Enabled
Security Contexts                 : 10
Carrier                           : Disabled
AnyConnect Premium Peers          : 20000
AnyConnect Essentials             : Disabled
Other VPN Peers                   : 20000
Total VPN Peers                   : 20000
AnyConnect for Mobile             : Enabled
AnyConnect for Cisco VPN Phone    : Enabled
Advanced Endpoint Assessment      : Enabled
Shared License                    : Disabled
Total TLS Proxy Sessions          : 15000
Cluster                           : Enabled

Failover cluster licensed features for this platform:
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 1024
Inside Hosts                      : Unlimited
Failover                          : Active/Active
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Enabled
Security Contexts                 : 20
Carrier                           : Disabled
AnyConnect Premium Peers          : 20000
AnyConnect Essentials             : Disabled
Other VPN Peers                   : 20000
Total VPN Peers                   : 20000
AnyConnect for Mobile             : Enabled
AnyConnect for Cisco VPN Phone    : Enabled
Advanced Endpoint Assessment      : Enabled
Shared License                    : Disabled
Total TLS Proxy Sessions          : 15000
Cluster                           : Enabled
```

Vérification et débogage

Résumé des commandes de vérification du châssis (MIO) :

```
FPR4125# show license all
FPR4125# show license techsupport
FPR4125# scope monitoring
FPR4125 /monitoring # scope callhome
FPR4125 /monitoring/callhome # show expand
FPR4125# scope system
FPR4125 /system # scope services
FPR4125 /system/services # show dns
FPR4125 /system/services # show ntp-server
FPR4125# scope security
FPR4125 /security # show trustpoint
FPR4125# show clock
```

```
FPR4125# show timezone
FPR4125# show license usage
```

Vérification de la configuration :

```
FPR4125-1# scope system
FPR4125-1 /system # scope services
FPR4125-1 /system/services # show configuration
```

Récapitulatif des commandes de vérification ASA :

```
asa# show run license
asa# show license all
asa# show license entitlement
asa# show license features
asa# show tech-support license
asa# debug license 255
```

Exemples de résultats de commandes de vérification du châssis (MIO)

```
FPR4125-1# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
 Status: REGISTERED
 Smart Account: TAC Cisco Systems, Inc.
 Virtual Account: EU TAC
 Export-Controlled Functionality: ALLOWED
 Initial Registration: SUCCEEDED on Dec 10 2018 23:30:02 UTC
 Last Renewal Attempt: SUCCEEDED on Mar 12 2020 23:16:11 UTC
 Next Renewal Attempt: Sep 08 2020 23:16:10 UTC
 Registration Expires: Mar 12 2021 23:11:09 UTC

License Authorization:
 Status: AUTHORIZED on Aug 04 2020 07:58:46 UTC
 Last Communication Attempt: SUCCEEDED on Aug 04 2020 07:58:46 UTC
 Next Communication Attempt: Sep 03 2020 07:58:45 UTC
 Communication Deadline: Nov 02 2020 07:53:44 UTC

License Conversion:
 Automatic Conversion Enabled: True
 Status: Not started

Export Authorization Key:
 Features Authorized:
   <none>

Utility:
 Status: DISABLED
```

```
Data Privacy:
 Sending Hostname: yes
   Callhome hostname privacy: DISABLED
   Smart Licensing hostname privacy: DISABLED
 Version privacy: DISABLED

Transport:
 Type: Callhome

License Usage
==============

Firepower 4100 ASA Standard (FIREPOWER_4100_ASA_STANDARD):
 Description: Firepower 4100 ASA Standard
 Count: 1
 Version: 1.0
 Status: AUTHORIZED
 Export status: NOT RESTRICTED

Product Information
===================
UDI: PID:FPR-4125-SUP,SN:JAD12345678

Agent Version
=============
Smart Agent for Licensing: 4.6.9_rel/104

Reservation Info
================
License reservation: DISABLED

FPR4125-1# scope monitoring
FPR4125-1 /monitoring # scope callhome
FPR4125-1 /monitoring/callhome # show expand

Callhome:
Admin State: Off
Throttling State: On
Contact Information:
Customer Contact Email:
From Email:
Reply To Email:
Phone Contact e.g., +1-011-408-555-1212:
Street Address:
Contract Id:
Customer Id:
Site Id:
Switch Priority: Debugging
Enable/Disable HTTP/HTTPS Proxy: Off
HTTP/HTTPS Proxy Server Address:
HTTP/HTTPS Proxy Server Port: 80
SMTP Server Address:
SMTP Server Port: 25

Anonymous Reporting:
Admin State
-----------
Off

Callhome periodic system inventory:
Send periodically: Off
Interval days: 30
```

```
Hour of day to send: 0
Minute of hour: 0
Time last sent: Never
Next scheduled: Never

Destination Profile:
Name: full_txt
Level: Warning
Alert Groups: All,Cisco Tac,Diagnostic,Environmental
Max Size: 5000000
Format: Full Txt
Reporting: Smart Call Home Data

Name: short_txt
Level: Warning
Alert Groups: All,Cisco Tac,Diagnostic,Environmental
Max Size: 5000000
Format: Short Txt
Reporting: Smart Call Home Data

Name: SLProfile
Level: Normal
Alert Groups: Smart License
Max Size: 5000000
Format: Xml
Reporting: Smart License Data

Destination:
Name Transport Protocol Email or HTTP/HTTPS URL Address
---------- ----------------- ------------------------------
SLDest Https https://tools.cisco.com/its/service/oddce/services/DDCEService

FPR4125-1# scope system
FPR4125-1 /system # scope services
FPR4125-1 /system/services # show dns
Domain Name Servers:
   IP Address: 172.16.200.100
FPR4125-1 /system/services # show ntp-server

NTP server hostname:
   Name                                                                  Time Sync Status
   ----------------------------------------------------------------- ----------------
   10.62.148.75                                                          Unreachable Or Invalid Ntp
Server
   172.18.108.14                                                         Time Synchronized
   172.18.108.15                                                         Candidate

FPR4125-1# scope security
FPR4125-1 /security # show trustpoint
Trustpoint Name: CHdefault
Trustpoint certificate chain: -----BEGIN CERTIFICATE-----
MIIFtzCCA5+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwRTELMAkGA1UEBhMCQk0x
…
8eOx79+Rj1QqCyXBJhnEUhAFZdWCEOrCMc0u
-----END CERTIFICATE-----
Cert Status: Valid
Trustpoint Name: CiscoLicRoot
Trustpoint certificate chain: -----BEGIN CERTIFICATE-----
MIIDITCCAgmgAwIBAgIBATANBgkqhkiG9w0BAQsFADAyMQ4wDAYDVQQKEwVDaXNj
…
QYYWqUCT4ElNEKt1J+hvc5MuNbWIYv2uAnUVb3GbsvDWl99/KA==
-----END CERTIFICATE-----
Cert Status: Valid
```

```
Trustpoint Name: CSCO2099SUDI
Trustpoint certificate chain: -----BEGIN CERTIFICATE-----
MIIDITCCAgmgAwIBAgIJAZozWHjOFsHBMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV
…
PKkmBlNQ9hQcNM3CSzVvEAK0CCEo/NJ/xzZ6WX1/f8Df1eXbFg==
-----END CERTIFICATE-----
Cert Status: Valid
Trustpoint Name: CSCOBA2099SUDI
Trustpoint certificate chain: -----BEGIN CERTIFICATE-----
MIIDQTCCAimgAwIBAgIJAaZa8V7plOvhMA0GCSqGSIb3DQEBCwUAMD0xDjAMBgNV
…
b/JPEAZkbji0RQTWLyfR82LWFLo0
-----END CERTIFICATE-----
Cert Status: Valid

FPR4125-1# show clock
Tue Aug  4 09:55:50 UTC 2020
FPR4125-1# show timezone
Timezone:

FPR4125-1# scope system
FPR4125-1 /system # scope services
FPR4125-1 /system/services # show configuration
 scope services
    create ssh-server host-key rsa
    delete ssh-server host-key ecdsa
    disable ntp-authentication
    disable telnet-server
    enable https
    enable ssh-server
     enter dns 192.0.2.100
    enter ip-block 0.0.0.0 0 https
    exit
    enter ip-block 0.0.0.0 0 ssh
    exit
     enter ntp-server 10.62.148.75
        set ntp-sha1-key-id 0
 !       set ntp-sha1-key-string
    exit
     enter ntp-server 172.18.108.14
        set ntp-sha1-key-id 0
 !       set ntp-sha1-key-string
    exit
     enter ntp-server 172.18.108.15
        set ntp-sha1-key-id 0
 !       set ntp-sha1-key-string
    exit
    scope shell-session-limits
        set per-user 32
        set total 32
    exit
    scope telemetry
        disable
    exit
    scope web-session-limits
        set per-user 32
        set total 256
    exit
    set domain-name ""
    set https auth-type cred-auth
    set https cipher-suite "ALL:!DHE-PSK-AES256-CBC-SHA:!EDH-RSA-DES-CBC3-SHA:!
EDH-DSS-DES-CBC3-SHA:!DES-CBC3-
SHA:!ADH:!3DES:!EXPORT40:!EXPORT56:!LOW:!MEDIUM:!NULL:!RC4:!MD5:!IDEA:+HIGH:+EXP"
```

```
    set https cipher-suite-mode high-strength
    set https crl-mode strict
    set https keyring default
    set https port 443
    set ssh-server host-key ecdsa secp256r1
    set ssh-server host-key rsa 2048
    set ssh-server kex-algorithm diffie-hellman-group14-sha1
    set ssh-server mac-algorithm hmac-sha1 hmac-sha2-256 hmac-sha2-512
    set ssh-server encrypt-algorithm aes128-cbc aes128-ctr aes192-cbc aes192-ctr aes256-cbc
aes256-ctr chacha20-poly1305_openssh_com
    set ssh-server rekey-limit volume none time none
    set ssh-client kex-algorithm diffie-hellman-group14-sha1
    set ssh-client mac-algorithm hmac-sha1 hmac-sha2-256 hmac-sha2-512
    set ssh-client encrypt-algorithm aes128-ctr aes192-ctr aes256-ctr
    set ssh-client rekey-limit volume none time none
    set ssh-client stricthostkeycheck disable
     set timezone ""
 exit

FPR4125-1# show license usage

License Authorization:
 Status: AUTHORIZED on Aug 04 2020 07:58:46 UTC

Firepower 4100 ASA Standard (FIREPOWER_4100_ASA_STANDARD):
 Description: Firepower 4100 ASA Standard
 Count: 1
 Version: 1.0
 Status: AUTHORIZED
 Export status: NOT RESTRICTED
```

Exemples de résultats des commandes de vérification ASA

```
asa# show run license
license smart
 feature tier standard

asa# show license all

Smart licensing enabled: Yes

Compliance status: In compliance

Overall licensed status: Authorized (3)

Entitlement(s):

Feature tier:
       Tag: regid.2015-10.com.cisco.FIREPOWER_4100_ASA_STANDARD,1.0_7d7f5ee2-1398-4b0e-aced-
b3f7fb1cacfc
       Version: 1.0
       Enforcement mode: Authorized
       Handle: 1
       Requested time: Tue, 04 Aug 2020 07:58:13 UTC
       Requested count: 1
       Request status: Complete

Serial Number:  FCH12345ABC
```

```
License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 1024
Inside Hosts                      : Unlimited
Failover                          : Active/Active
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Enabled
Security Contexts                 : 10
Carrier                           : Disabled
AnyConnect Premium Peers          : 20000
AnyConnect Essentials             : Disabled
Other VPN Peers                   : 20000
Total VPN Peers                   : 20000
AnyConnect for Mobile             : Enabled
AnyConnect for Cisco VPN Phone    : Enabled
Advanced Endpoint Assessment      : Enabled
Shared License                    : Disabled
Total TLS Proxy Sessions          : 15000
Cluster                           : Enabled

asa# show license entitlement

Entitlement(s):

Feature tier:
       Tag: regid.2015-10.com.cisco.FIREPOWER_4100_ASA_STANDARD,1.0_7d7f5ee2-1398-4b0e-aced-
b3f7fb1cacfc
       Version: 1.0
       Enforcement mode: Authorized
       Handle: 1
       Requested time: Tue, 04 Aug 2020 07:58:13 UTC
       Requested count: 1
       Request status: Complete

asa# show license features
Serial Number:  FCH12345ABC

License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 1024
Inside Hosts                      : Unlimited
Failover                          : Active/Active
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Enabled
Security Contexts                 : 10
Carrier                           : Disabled
AnyConnect Premium Peers          : 20000
AnyConnect Essentials             : Disabled
Other VPN Peers                   : 20000
Total VPN Peers                   : 20000
AnyConnect for Mobile             : Enabled
AnyConnect for Cisco VPN Phone    : Enabled
Advanced Endpoint Assessment      : Enabled
Shared License                    : Disabled
Total TLS Proxy Sessions          : 15000
Cluster                           : Enabled

asa#  show tech-support license
```

```
Smart licensing enabled: Yes

Compliance status: In compliance

Overall licensed status: Authorized (3)

Entitlement(s):

Feature tier:
       Tag: regid.2015-10.com.cisco.FIREPOWER_4100_ASA_STANDARD,1.0_7d7f5ee2-1398-4b0e-aced-
b3f7fb1cacfc
       Version: 1.0
       Enforcement mode: Authorized
       Handle: 1
       Requested time: Tue, 04 Aug 2020 07:58:13 UTC
       Requested count: 1
       Request status: Complete
```

Inscription réussie

Le résultat provient de l'interface utilisateur du gestionnaire de châssis :

```
Smart Licensing is ENABLED

Utility:
Status: DISABLED

Data Privacy:
Sending Hostname: yes
Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
Type: Callhome

Registration:
Status: REGISTERED
Smart Account: TAC Cisco Systems, Inc.
Virtual Account: EU TAC
Export-Controlled Functionality: ALLOWED
Initial Registration: SUCCEEDED on Dec 10 2018 23:30:02 UTC
Last Renewal Attempt: SUCCEEDED on Mar 12 2020 23:16:11 UTC
Next Renewal Attempt: Sep 08 2020 23:16:10 UTC
Registration Expires: Mar 12 2021 23:11:09 UTC

License Authorization:
Status: AUTHORIZED on Jul 05 2020 17:49:15 UTC
Last Communication Attempt: SUCCEEDED on Jul 05 2020 17:49:15 UTC
Next Communication Attempt: Aug 04 2020 17:49:14 UTC
Communication Deadline: Oct 03 2020 17:44:13 UTC

License Conversion:
Automatic Conversion Enabled: True
Status: Not started

Export Authorization Key:
Features Authorized:
<none>

Cisco Success Network: DISABLED
```

Autorisation expirée

Le résultat provient de l'interface utilisateur du gestionnaire de châssis :

```
Smart Licensing is ENABLED

Utility:
Status: DISABLED

Data Privacy:
Sending Hostname: yes
Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
Type: Callhome

Registration:
Status: REGISTERED
Smart Account: Cisco SVS temp - request access through licensing@cisco.com
Virtual Account: Sample Account
Export-Controlled Functionality: ALLOWED
Initial Registration: SUCCEEDED on Nov 22 2019 08:17:30 UTC
Last Renewal Attempt: FAILED on Aug 04 2020 07:32:08 UTC
Failure reason: Agent received a failure status in a response message. Please check the Agent
log file for the detailed message.
Next Renewal Attempt: Aug 04 2020 08:33:48 UTC
Registration Expires: Nov 21 2020 08:12:20 UTC

License Authorization:
Status: AUTH EXPIRED on Aug 04 2020 07:10:16 UTC
Last Communication Attempt: FAILED on Aug 04 2020 07:10:16 UTC
Failure reason: Data and signature do not match
Next Communication Attempt: Aug 04 2020 08:10:14 UTC
Communication Deadline: DEADLINE EXCEEDED

License Conversion:
Automatic Conversion Enabled: True
Status: Not started

Export Authorization Key:
Features Authorized:
<none>

Last Configuration Error
========================
Command : register idtoken
ZDA2MjFlODktYjllMS00NjQwLTk0MmUtYmVkYWU2NzIyZjYwLTE1ODIxODY2%0AMzEwODV8K2RWVTNURGFIK0tDYUhOSjg3b
jFsdytwbU1SUi81N20rQTVPN2lT%0AdEtvYz0%3D%0A
Error : Smart Agent already registered

Cisco Success Network: DISABLED
```

Exemples de résultats de la CLI du châssis

Non Enregistré

```
firepower# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED

License Authorization:
  Status: No Licenses in Use

License Usage
==============

No licenses in use

Product Information
===================
UDI: PID:F9K-C9300-SUP-K9,SN:JAD12345678

Agent Version
=============
Smart Agent for Licensing: 1.2.2_throttle/6
```

Inscription en cours

```
firepower# scope license
firepower /license # register idtoken
```

```
firepower /license # show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED - REGISTRATION PENDING
  Initial Registration: First Attempt Pending

License Authorization:
 Status: No Licenses in Use

License Usage
==============

No licenses in use

Product Information
===================
```

```
UDI: PID:F9K-C9300-SUP-K9,SN:JAD12345678

Agent Version
=============
Smart Agent for Licensing: 1.2.2_throttle/6
```

Erreur d'enregistrement

```
firepower /license # show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED - REGISTRATION FAILED
  Initial Registration: FAILED on Aug 04 04:46:47 2020 UTC
    Failure reason: HTTP transport failed

License Authorization:
 Status: No Licenses in Use

License Usage
==============

No licenses in use

Product Information
===================
UDI: PID:F9K-C9300-SUP-K9,SN:JAD12345678

Agent Version
=============
Smart Agent for Licensing: 1.2.2_throttle/6
```

Période d'évaluation

```
firepower# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
 Status: REGISTERING - REGISTRATION IN PROGRESS
 Initial Registration: FAILED on Aug 04 04:46:47 2020 UTC
 Next Registration Attempt: Aug 04 05:06:16 2020 UTC

License Authorization:
 Status: EVALUATION MODE
 Evaluation Period Remaining: 89 days, 14 hours, 26 minutes, 20 seconds

License Usage
==============
```

```
(ASA-SSP-STD):
 Description:
 Count: 1
 Version: 1.0
 Status: EVALUATION MODE


Product Information
==================
UDI: PID:F9K-C9300-SUP-K9,SN:JAD12345678

Agent Version
=============
Smart Agent for Licensing: 1.2.2_throttle/6
```

Problèmes de licence courants sur les châssis FXOS (MIO)

Erreur d'enregistrement : jeton non valide

```
FPR4125-1# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
 Status: UNREGISTERED - REGISTRATION FAILED
 Export-Controlled Functionality: NOT ALLOWED
 Initial Registration: FAILED on Aug 07 2020 06:39:24 UTC
    Failure reason: {"token":["The token 'ODNmNTExMTAtY2YzOS00Mzc1LWEzNWMtYmNiMm
UyNzM4ZmFjLTE1OTkxMTkz%0ANDk0NjR8NkJJdWZpQzRDbmtPR0xBWlVpUzZqMjlySnl5QUczT2M0YVI
vcmxm%0ATGczND0%3D%0B' is not valid."]}
```

Étapes recommandées

1. Vérifiez si l'URL de renvoi d'appel pointe vers CSSM.
2. Connectez-vous au CSSM et vérifiez si le jeton est généré à partir de là ou s'il a expiré.

Erreur d'enregistrement : produit déjà enregistré

```
FPR4125-1# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
Status: UNREGISTERED - REGISTRATION FAILED
 Export-Controlled Functionality: Not Allowed
 Initial Registration: FAILED on Aug 07 01:30:00 2020 UTC
 Failure reason: {"sudi":["The product 'firepower.com.cisco.
```

```
FPR9300,1.0_ed6dadbe-c965-4aeb-ab58-62e34033b453' and sudi {\"suvi\"=>nil,
\"uuid\"=>nil, \"host_identifier\"=>nil, \"udi_pid\"=>\"FPR9K-SUP\",
\"udi_serial_number\"=>\"JAD1234567S\", \"udi_vid\"=>nil, \"mac_address\"=>nil}
have already been registered."]}
```

Étapes recommandées

1. Connectez-vous au CSSM.
2. Vérifiez la Product Instances dans TOUS les comptes virtuels.
3. Recherchez l'ancienne instance d'enregistrement par numéro de série et supprimez-la.
4. Ce problème peut être dû aux deux causes suivantes : Échec du renouvellement automatique lorsque l'heure/la date n'est pas configurée correctement, par exemple, aucun serveur NTP n'est configuré.Mauvais ordre des opérations lorsque vous passez d'un satellite à un serveur de production, par exemple, modifiez d'abord l'URL, puis émettez « désenregistrer »

Erreur d'inscription : date de décalage au-delà de la limite

```
FPR4125-1# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
 Status: UNREGISTERED - REGISTRATION FAILED
 Export-Controlled Functionality: Not Allowed
 Initial Registration: FAILED on Aug 07 01:30:00 2020 UTC
Failure reason: {"timestamp":["The device date '1453329321505' is offset beyond the allowed
tolerance limit."]}
```

Étape recommandée

Vérifiez la configuration heure/date pour vous assurer qu'un serveur NTP est configuré.

Erreur d'inscription : échec de la résolution de l'hôte

```
FPR4125-1# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
 Status: REGISTERING - REGISTRATION IN PROGRESS
 Export-Controlled Functionality: NOT ALLOWED
 Initial Registration: FAILED on Aug 07 2020 06:58:46 UTC
   Failure reason: Failed to resolve host
 Next Registration Attempt: Aug 07 2020 07:16:42 UTC
```

Registration Error: Failed to resolve host

Étapes recommandées

1. Vérifiez si l'URL de callhome SLDest est correcte (scope monitoring > scope callhome > show expand)
2. Vérifiez si la configuration du serveur DNS MIO est correcte, par exemple, à partir de l'interface de ligne de commande :

```
FPR4125-1# scope system
FPR4125-1 /system # scope services
FPR4125-1 /system/services # show dns
Domain Name Servers:
   IP Address: 172.31.200.100
```

3. Essayez d'envoyer une requête ping à partir de l'interface CLI du châssis **tools.cisco.com** et voir s'il résout :

```
FPR4125-1# connect local-mgmt
FPR4125-1(local-mgmt)# ping tools.cisco.com
```

4. Essayez d'envoyer une requête ping à partir de l'interface de ligne de commande du châssis vers le serveur DNS :

```
FPR4125-1# connect local-mgmt
FPR4125-1(local-mgmt)# ping 172.31.200.100
PING 172.31.200.100 (172.31.200.100) from 10.62.148.225 eth0: 56(84) bytes of data.
^C
--- 172.31.200.100 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3001ms
```

5. Activez l'interface de gestion de capture sur châssis (MIO) (applicable uniquement sur FP41xx/FP93xx) et vérifiez la communication DNS lors de l'exécution d'un test ping vers le **tools.cisco.com**:

```
FPR4125-1# connect fxos
FPR4125-1(fxos)# ethanalyzer local interface mgmt capture-filter "udp port 53" limit-captured-
frames 0 limit-frame-size 10000
Capturing on 'eth0'
   1 2020-08-07 08:10:45.252955552 10.62.148.225  172.31.200.100 DNS 75 Standard query 0x26b4 A
tools.cisco.com
   2 2020-08-07 08:10:47.255015331 10.62.148.225  172.31.200.100 DNS 75 Standard query 0x26b4 A
tools.cisco.com
   3 2020-08-07 08:10:49.257160749 10.62.148.225  172.31.200.100 DNS 75 Standard query 0x5019 A
tools.cisco.com
   4 2020-08-07 08:10:51.259222753 10.62.148.225  172.31.200.100 DNS 75 Standard query 0x5019 A
tools.cisco.com
```

Erreur d'enregistrement : échec de l'authentification du serveur

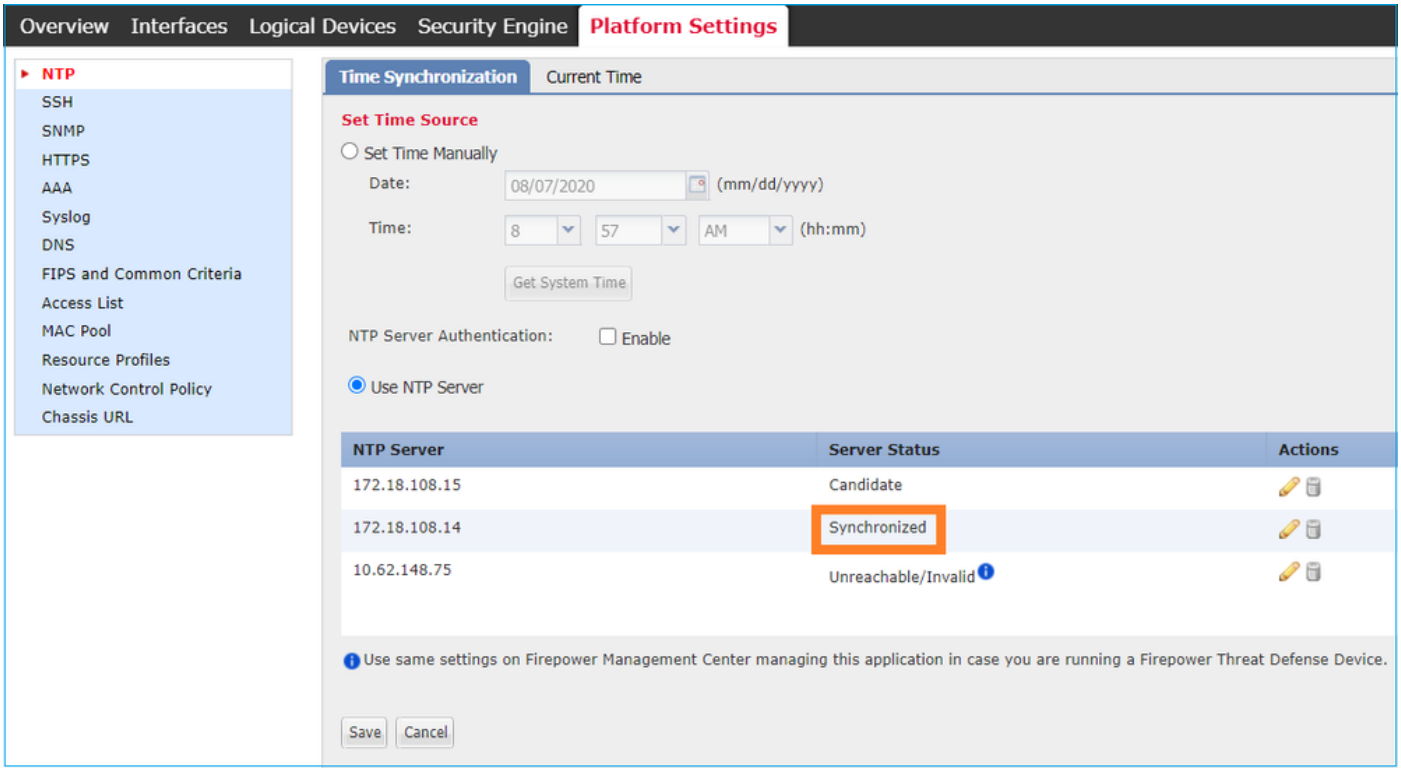
```
FPR4125-1# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
 Status: UNREGISTERED - REGISTRATION FAILED
 Export-Controlled Functionality: Not Allowed
 Initial Registration: FAILED on Aug 07 2020 06:58:46 UTC
  Failure reason: Failed to authenticate server
```

Étapes recommandées

1. Vérifiez si le point de confiance MIO CHdefault possède le certificat correct, par exemple :

```
FPR4125-1# scope security
FPR4125-1 /security # show trustpoint
Trustpoint Name: CHdefault
Trustpoint certificate chain: -----BEGIN CERTIFICATE-----
MIIFtzCCA5+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwRTELMAkGA1UEBhMCQk0x
...
8eOx79+Rj1QqCyXBJhnEUhAFZdWCEOrCMc0u
-----END CERTIFICATE-----
Cert Status: Valid
```

2. Vérifiez si le serveur NTP et le fuseau horaire sont définis correctement. La vérification du certificat nécessite le même temps entre le serveur et le client. Pour ce faire, utilisez NTP pour synchroniser l'heure. Par exemple, vérification de l'interface utilisateur FXOS :



Vérification CLI

```
FPR4125-1# scope system
FPR4125-1 /system # scope services
FPR4125-1 /system/services # show ntp-server

NTP server hostname:
   Name                                                Time Sync Status
   ---------------------------------------------------- ---------------
   10.62.148.75                                       Unreachable Or Invalid Ntp Server
    172.18.108.14                                       Time Synchronized
   172.18.108.15                                      Candidate
```

Activez une capture et vérifiez la communication TCP (HTTPS) entre le MIO et le **tools.cisco.com**. Voici quelques options qui s'offrent à vous :

- Vous pouvez fermer votre session HTTPS sur l'interface utilisateur FXOS, puis définir un filtre de capture sur l'interface de ligne de commande pour HTTPS, par exemple :

```
FPR4100(fxos)# ethanalyzer local interface mgmt capture-filter "tcp port 443" limit-captured-
frames 50
Capturing on eth0
2017-01-12 13:09:44.296256 10.62.148.37 -> 72.163.4.38  TCP 43278 > https [SYN] Seq=0 Len=0
MSS=1460 TSV=206433871 TSER=0 WS=9
2017-01-12 13:09:44.452405  72.163.4.38 -> 10.62.148.37 TCP https > 43278 [SYN,ACK] Seq=0 Ack=1
Win=32768 Len=0 MSS=1380 TSV=2933962056 TSER=206433871
2017-01-12 13:09:44.452451 10.62.148.37 -> 72.163.4.38  TCP 43278 > https [ACK] Seq=1 Ack=1
Win=5840 Len=0 TSV=206433887 TSER=2933962056
2017-01-12 13:09:44.453219 10.62.148.37 -> 72.163.4.38  SSL Client Hello
2017-01-12 13:09:44.609171  72.163.4.38 -> 10.62.148.37 TCP https > 43278 [ACK] Seq=1 Ack=518
Win=32251 Len=0 TSV=2933962263 TSER=206433887
```

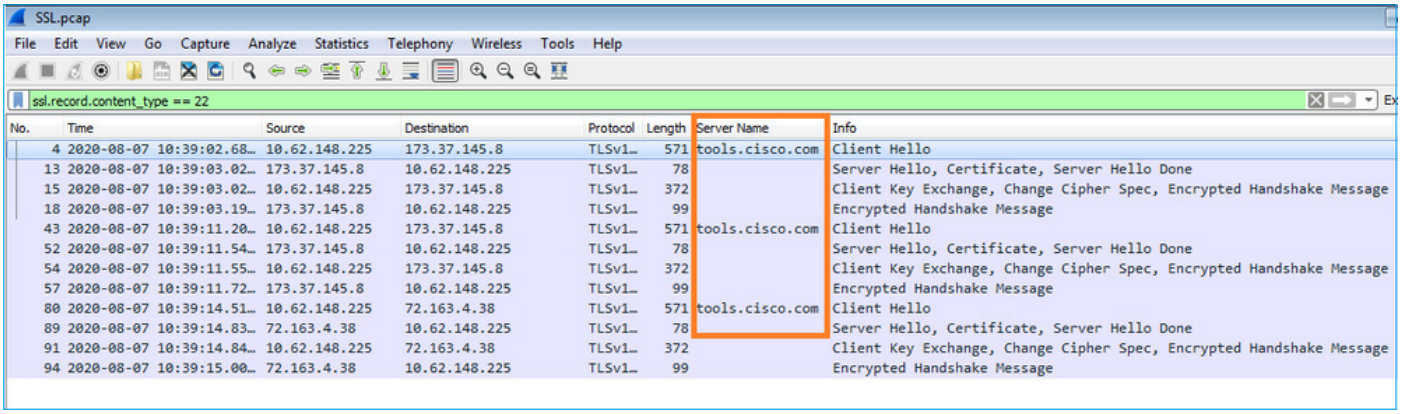
```
2017-01-12 13:09:44.609573  72.163.4.38 -> 10.62.148.37 SSL Continuation Data
2017-01-12 13:09:44.609595 10.62.148.37 -> 72.163.4.38  TCP 43278 > https [ACK] Seq=518 Ack=1369
Win=8208 Len=0 TSV=206433902 TSER=2933962264
2017-01-12 13:09:44.609599  72.163.4.38 -> 10.62.148.37 SSL Continuation Data
2017-01-12 13:09:44.609610 10.62.148.37 -> 72.163.4.38  TCP 43278 > https [ACK] Seq=518 Ack=2737
Win=10944 Len=0 TSV=206433902 TSER=2933962264
```

- En outre, si vous souhaitez garder l'interface utilisateur FXOS ouverte, vous pouvez spécifier dans la capture les adresses IP de destination (72.163.4.38 et 173.37.145.8) **tools.cisco.com** serveurs au moment de la rédaction de ce document). Il est également fortement recommandé d'enregistrer la capture au format pcap et de la vérifier dans Wireshark. Voici un exemple d'inscription réussie :

```
FPR4125-1(fxos)# ethanalyzer local interface mgmt capture-filter "tcp port 443 and (host
72.163.4.38 or host 173.37.145.8)" limit-captured-frames 0 limit-frame-size 10000 write
workspace:///SSL.pcap
Capturing on 'eth0'
   1 2020-08-07 08:39:02.515693672 10.62.148.225  173.37.145.8 TCP 74 59818  443 [SYN] Seq=0
Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=800212367 TSecr=0 WS=512
   2 2020-08-07 08:39:02.684723361 173.37.145.8  10.62.148.225 TCP 60 443  59818 [SYN, ACK]
Seq=0 Ack=1 Win=8190 Len=0 MSS=1330
   3 2020-08-07 08:39:02.684825625 10.62.148.225  173.37.145.8 TCP 54 59818  443 [ACK] Seq=1
Ack=1 Win=29200 Len=0
   4 2020-08-07 08:39:02.685182942 10.62.148.225  173.37.145.8 TLSv1 571 Client Hello
…
  11 2020-08-07 08:39:02.854525349 10.62.148.225  173.37.145.8 TCP 54 59818  443 [ACK] Seq=518
Ack=3991 Win=37240 Len=0
```

- Pour exporter le fichier pcap vers un serveur FTP distant :

```
FPR4125-1# connect local-mgmt
FPR4125-1(local-mgmt)# dir

1 56936 Aug 07 08:39:35 2020 SSL.pcap
1    29 May 06 17:48:02 2020 blade_debug_plugin
1    19 May 06 17:48:02 2020 bladelog
1    16 Dec 07 17:24:43 2018 cores
2  4096 Dec 07 17:28:46 2018 debug_plugin/
1    31 Dec 07 17:24:43 2018 diagnostics
2  4096 Dec 07 17:22:28 2018 lost+found/
1    25 Dec 07 17:24:31 2018 packet-capture
2  4096 Sep 24 07:05:40 2019 techsupport/

Usage for workspace://
3999125504 bytes total
284364800 bytes used
3509907456 bytes free
FPR4125-1(local-mgmt)# copy workspace:///SSL.pcap ftp://ftp_user@10.62.148.41/SSL.pcap
Password:
FPR4125-1(local-mgmt)#
```



Erreur d'inscription : échec du transport HTTP

```
FPR4125-1# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
 Status: UNREGISTERED - REGISTRATION FAILED
 Export-Controlled Functionality: Not Allowed
 Initial Registration: FAILED on Aug 07 2020 06:58:46 UTC
Failure reason: HTTP transport failed
```

Étapes recommandées

1. Vérifiez si l'URL de call-home est correcte. Vous pouvez le vérifier à partir de l'interface utilisateur de FXOS ou de l'interface de ligne de commande (**scope monitoring > show callhome detail expand**.
2. Activez une capture et vérifiez la communication TCP (HTTPS) entre le MIO et le **tools.cisco.com** comme le montre la section « Échec de l'authentification du serveur » de ce document.

Erreur d'inscription : impossible de se connecter à l'hôte

```
FPR4125-1# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
Status: UNREGISTERED - REGISTRATION FAILED
 Export-Controlled Functionality: Not Allowed
 Initial Registration: FAILED on Aug 07 2020 06:58:46 UTC
 Failure reason: Couldn't connect to host
```

Étapes recommandées

1. Si une configuration de proxy est activée, vérifiez que l'URL et le port du proxy sont correctement configurés.
2. Activez une capture et vérifiez la communication TCP (HTTPS) entre le MIO et le **tools.cisco.com** comme le montre la section « Échec de l'authentification du serveur » de ce document.

Erreur d'enregistrement : le serveur HTTP renvoie un code d'erreur >= 400

```
FPR4125-1# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
Status: UNREGISTERED - REGISTRATION FAILED
 Export-Controlled Functionality: Not Allowed
 Initial Registration: FAILED on Aug 07 2020 06:58:46 UTC
 Failure reason: HTTP server returns error code >= 400. Contact proxy server admin if proxy
configuration is enabled
```

Étapes recommandées

1. Si une configuration de proxy est activée, contactez l'administrateur du serveur proxy à propos des paramètres de proxy.
2. Activez une capture et vérifiez la communication TCP (HTTPS) entre le MIO et le **tools.cisco.com** comme le montre la section « Échec de l'authentification du serveur » de ce document. Essayez de vous enregistrer à nouveau (option « force ») à partir de l'interface de ligne de commande FXOS :

```
FPR4125-1 /license # register idtoken
ODNmNTExMTAtY2YzOS00Mzc1LWEzNWMtYmNiMmUyNzM4ZmFjLTE1OTkxMTkz%0ANDk0NjR8NkJJdWZpQzRDbmtPR0xBWlVpU
zZqMjlySnl5QUczT2M0YVIvcmxm%0ATGczND0%3D%0A force
```

Erreur d'inscription : échec du message de réponse du serveur principal d'analyse

```
FPR4125-1# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
 Status: UNREGISTERED - REGISTRATION FAILED
```

```
 Export-Controlled Functionality: Not Allowed
 Initial Registration: FAILED on Aug 07 2020 06:58:46 UTC
 Failure reason: Parsing backend response message failed
```

Étapes recommandées

1. Réessayez automatiquement ultérieurement. Utilisez « renouveler » pour réessayer immédiatement.

```
FPR4125-1# scope license
FPR4125-1 /license # scope licdebug
FPR4125-1 /license/licdebug # renew
```

2. Vérifiez si l'URL de renvoi d'appel est correcte.

Problèmes de licence sur ASA - Gamme 1xxx/21xx

Erreur d'enregistrement : erreur d'envoi du message de communication

```
ciscoasa# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
 Status: REGISTERING - REGISTRATION IN PROGRESS
 Export-Controlled Functionality: NOT ALLOWED
 Initial Registration: FAILED on Aug 07 2020 11:29:42 UTC
    Failure reason: Communication message send error
 Next Registration Attempt: Aug 07 2020 11:46:13 UTC
```

Étapes recommandées

1. Vérifiez les paramètres DNS

```
ciscoasa# show run dns
```

2. Essayez d'envoyer une requête ping **tools.cisco.com**. Dans ce cas, l'interface de gestion est utilisée :

```
ciscoasa# ping management tools.cisco.com
                ^
ERROR: % Invalid Hostname
```

3. Vérifiez la table de routage :

```
ciscoasa# show route management-only
```

Assurez-vous qu'une licence est activée, par exemple :

```
ciscoasa# show run license
license smart
 feature tier standard
 feature strong-encryption
```

4. Activez la capture sur l'interface qui achemine vers le **tools.cisco.com** (si vous effectuez la capture sans filtre IP, assurez-vous que l'application ASDM n'est pas ouverte lorsque vous effectuez la capture pour éviter tout bruit de capture inutile).

```
ciscoasa# capture CAP interface management match tcp any any eq 443
```

Avertissement : la capture de paquets peut avoir un impact négatif sur les performances.

5. Activez temporairement Syslog niveau 7 (debug) et vérifiez les messages Syslog ASA pendant le processus d'enregistrement :

```
ciscoasa(config)# logging buffer-size 10000000
ciscoasa(config)# logging buffered  7
ciscoasa(config)# logging enable
ciscoasa# show logging
%ASA-7-717025: Validating certificate chain containing 3 certificate(s).
%ASA-7-717029: Identified client certificate within certificate chain. serial number:
3000683B0F7504F7B244B3EA7FC00927E960D735, subject name: CN=tools.cisco.com,O=Cisco Systems\,
Inc.,L=San Jose,ST=CA,C=US.
%ASA-7-717030: Found a suitable trustpoint _SmartCallHome_ServerCA to validate certificate.
%ASA-6-717028: Certificate chain was successfully validated with warning, revocation status was
not checked.
%ASA-6-717022: Certificate was successfully validated. serial number:
3000683B0F7504F7B244B3EA7FC00927E960D735, subject name:  CN=tools.cisco.com,O=Cisco Systems\,
Inc.,L=San Jose,ST=CA,C=US.
%ASA-6-725002: Device completed SSL handshake with server management:10.62.148.184/22258 to
173.37.145.8/443 for TLSv1.2 session
```

Réessayez de vous inscrire :

```
ciscoasa # license smart register idtoken
```

Conditions particulières pour les droits d'extension

- Vous devez acquérir une autorisation de niveau de fonctionnalité valide avant de configurer des autorisations de module complémentaire
- Toutes les habilitations de module complémentaire doivent être libérées avant que vous ne libériez l'habilitation de niveau de fonctionnalité

État des droits pendant le redémarrage

- Les états d'autorisation sont enregistrés dans la mémoire Flash
- Au démarrage, ces informations sont lues à partir de la mémoire flash et les licences sont définies en fonction du mode d'application enregistré
- La configuration initiale est appliquée en fonction de ces informations d'autorisation mises en cache
- Les droits sont demandés à nouveau après chaque redémarrage

Engager l'assistance TAC Cisco

FP41xx/FP9300

Si tous les éléments mentionnés dans ce document échouent, collectez ces résultats à partir de l'interface de ligne de commande du châssis et contactez le centre d'assistance technique Cisco :

Résultat 1 :

```
FPR4125-1# show license techsupport
```

Résultat 2 :

```
FPR4125-1# scope monitoring
FPR4125-1 /monitoring # scope callhome
FPR4125-1 /monitoring/callhome # show detail expand
```

Résultat 3 :

Offre groupée de support châssis FXOS

```
FPR4125-1# connect local-mgmt
FPR4125-1(local-mgmt)# show tech-support chassis 1 detail
```

Résultat 4 (fortement recommandé) :

Capture d'analyseur à partir de la CLI du châssis

FP1xxx/FP21xx

Résultat 1 :

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

Résultat 2 :

```
ciscoasa# connect fxos admin
firepower-2140# connect local-mgmt
firepower-2140(local-mgmt)# show tech-support fprm detail
```

Foire aux questions (FAQ)

Sur FP21xx, où se trouve l'onglet Licensing sur l'interface graphique du châssis (FCM) ?
Depuis la version 9.13.x, FP21xx prend en charge 2 modes ASA :

- Appareil
- Plateforme

En mode Appliance, il n'y a pas d'interface utilisateur de châssis. En mode Plate-forme, il existe une interface utilisateur de châssis, mais la licence est configurée à partir de l'interface de ligne de commande ASA ou de l'ASDM.
D'autre part, sur les plates-formes FPR4100/9300, la licence doit être configurée dans FCM via l'interface utilisateur graphique ou l'interface de ligne de commande FXOS et les droits ASA doivent être demandés à l'interface de ligne de commande ASA ou à l'ASDM.
Références:

- Gestion des licences pour l'ASA
- Périphériques logiques pour Firepower 4100/9300
- Licences : licences logicielles Smart (ASAv, ASA sur Firepower)
- Déploiement en mode plate-forme ASA avec ASDM et Firepower Chassis Manager

Comment pouvez-vous activer une licence de cryptage fort ?
Cette fonctionnalité est activée automatiquement si le jeton utilisé dans l'enregistrement FCM avait l'option Autoriser la fonctionnalité de contrôle des exportations sur les produits enregistrés avec ce jeton activé.

Comment pouvez-vous activer une licence de cryptage fort si les fonctionnalités d'exportation contrôlée au niveau FCM et le cryptage 3DES-AES associé au niveau ASA sont désactivés ?
Si cette option n'est pas activée pour le jeton, annulez l'enregistrement du FCM et réenregistrez-le avec un jeton pour lequel cette option est activée.

Que pouvez-vous faire si l'option Autoriser la fonctionnalité de contrôle des exportations sur les produits enregistrés avec ce jeton n'est pas disponible lorsque vous générez le jeton ?
Contactez votre équipe de compte Cisco.

Est-il obligatoire de configurer la fonctionnalité Strong Encryption au niveau ASA ?

L'option de cryptage fort de la fonctionnalité est obligatoire uniquement si FCM est intégré à un serveur satellite antérieur à la version 2.3.0. Il ne s'agit que d'un scénario dans lequel vous devez configurer cette fonctionnalité.

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

Le FXOS utilise l'adresse https://tools.cisco.com/ (port 443) pour communiquer avec le cloud de licence. L'adresse https://tools.cisco.com/ est résolue en ces adresses IP :

- 72.163.4.38
- 173.37.145.8

Pourquoi obtenez-vous une erreur de non-conformité ?

Le périphérique peut devenir non conforme dans les situations suivantes :

- Surutilisation (le périphérique utilise des licences non disponibles)
- Expiration de la licence - Une licence basée sur le temps a expiré
- Manque de communication - Le périphérique ne peut pas joindre l'autorité de délivrance des licences pour une nouvelle autorisation

Pour vérifier si votre compte est dans un état de non-conformité ou s'il approche de cet état, vous devez comparer les droits actuellement utilisés par votre châssis Firepower avec ceux de votre compte Smart.
Dans un état de non-conformité, vous pouvez apporter des modifications à la configuration des fonctionnalités qui nécessitent des licences spéciales, mais le fonctionnement n'est pas affecté. Par exemple, les contextes de limite de licence standard qui existent déjà continuent à s'exécuter et vous pouvez modifier leur configuration, mais vous ne pouvez pas ajouter un nouveau contexte.

Pourquoi obtenez-vous toujours une erreur de non-conformité après l'ajout de licences ?

Par défaut, le périphérique communique avec l'autorité de licence tous les 30 jours pour vérifier les droits. Si vous souhaitez le déclencher manuellement, vous devez suivre les étapes suivantes :

Pour les plates-formes FPR1000/2100, cette opération doit être effectuée via ASDM ou CLI :

```
ASA# license smart renew auth
```

Pour les plates-formes FPR4100/9300, cette opération doit être effectuée via l'interface de ligne de commande FXOS :

```
FP4100# scope system
FP4100 /system # scope license
FP4100 /license # scope licdebug
FP4100 /license/licdebug # renew
```

Pourquoi aucune licence n'est utilisée au niveau ASA ?

Assurez-vous que l'autorisation ASA a été configurée au niveau ASA, par exemple :

```
ASA(config)# license smart
ASA(config-smart-lic)# feature tier standard
```

Pourquoi les licences ne sont-elles toujours pas utilisées même après la configuration d'un droit ASA ?
Cet état est attendu si vous avez déployé une paire de basculement actif/veille ASA et que vous vérifiez l'utilisation de la licence sur le périphérique en veille.
Selon le Guide de configuration, la configuration est répliquée sur l'unité en veille, mais celle-ci n'utilise pas la configuration ; elle reste dans un état mis en cache. Seule l'unité active demande les licences au serveur. Les licences sont agrégées en une seule licence de basculement partagée par la paire de basculement, et cette licence agrégée est également mise en cache sur l'unité de secours à utiliser si elle devient l'unité active à l'avenir. Pour référence : Licences de basculement ou de cluster ASA.

Que pouvez-vous faire si la FCM n'a pas accès à Internet ?
Vous pouvez également déployer Cisco Smart Software Manager On-Prem (anciennement appelé Cisco Smart Software Manager Satellite). Il s'agit d'un composant de Cisco Smart Licensing qui fonctionne avec Cisco Smart Software Manager. Il offre une visibilité et des rapports quasiment en temps réel sur les licences Cisco que vous achetez et consommez. Elle permet également aux entreprises sensibles à la sécurité d'accéder à un sous-ensemble de fonctionnalités Cisco SSM sans utiliser de connexion Internet directe pour gérer leur base installée.

Où pouvez-vous trouver plus d'informations sur Cisco Smart Software Manager On-Prem ?
Vous trouverez ces informations dans le Guide de configuration de FXOS :

- Configuration d'un serveur de licences Smart Satellite pour le châssis Firepower 4100/9300
- Configuration de l'enregistrement du gestionnaire de châssis Firepower sur Smart Software Manager On-Prem

Informations connexes

- Guide de configuration CLI des opérations générales de la gamme Cisco ASA
- Gestion des licences pour l'ASA
- Assistance et documentation techniques - Cisco Systems

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

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