Resolución de problemas de licencia inteligente de ASA en dispositivos Firepower FXOS

Contenido

Introducción

Este documento describe la función de licencia inteligente de Adaptive Security Appliance (ASA) en Firepower eXtensible Operating System (FXOS).

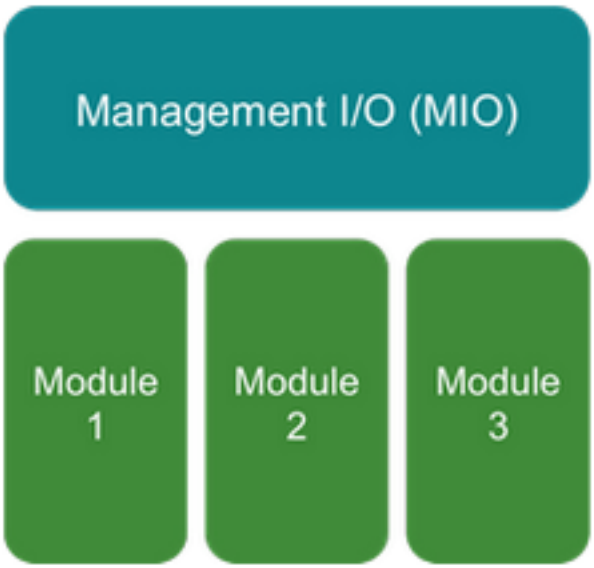
Antecedentes

Las licencias inteligentes en FXOS se utilizan cuando hay un ASA instalado en el chasis. Para Firepower Threat Defense (FTD) y Firepower Management Center (FMC), la licencia inteligente comprueba el registro y la resolución de problemas de la licencia inteligente de FMC y FTD.

Este documento cubre principalmente los escenarios donde el chasis FXOS tiene acceso directo a Internet. Si su chasis FXOS no puede acceder a Internet, debe considerar un servidor satélite o una reserva de licencia permanente (PLR). Consulte la guía de configuración de FXOS para obtener más detalles sobre la administración sin conexión.

Arquitectura de Smart Licensing

Una descripción general de alto nivel de los componentes del chasis:

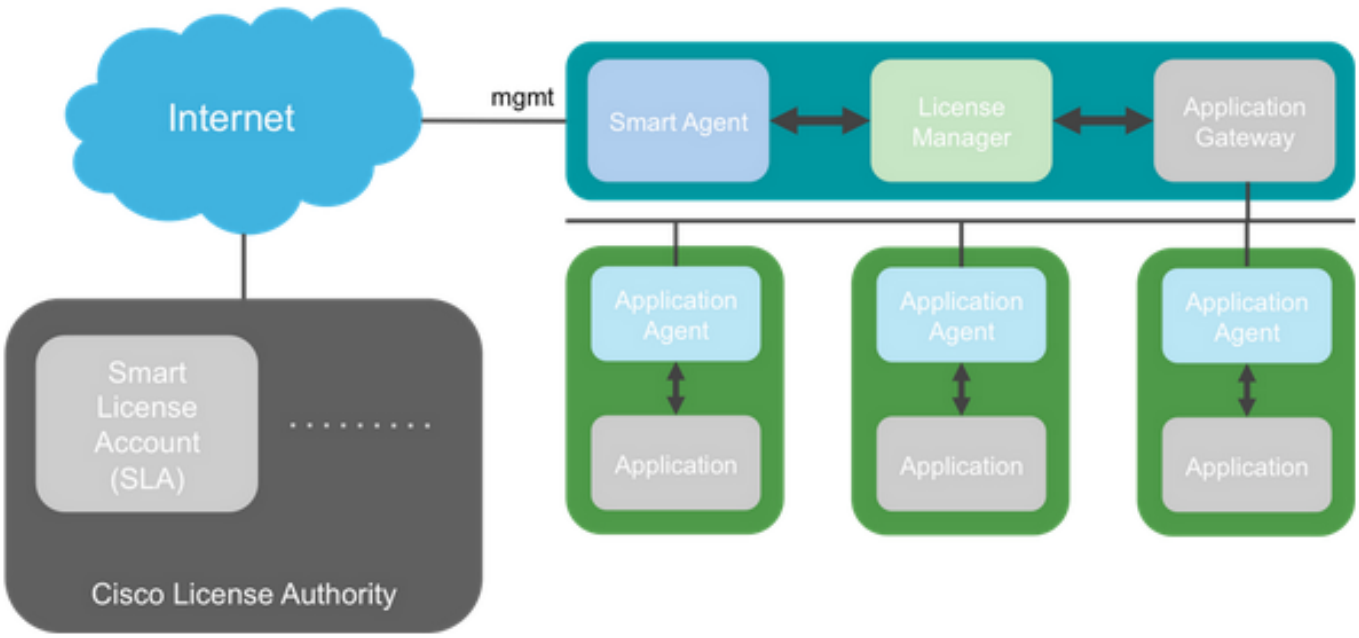


- Tanto Management Input/Output (MIO) como los módulos individuales desempeñan un papel en Smart Licensing
- MIO en sí no requiere ninguna licencia para su funcionamiento
- Las aplicaciones SA de cada módulo necesitan una licencia

El supervisor FXOS es el MIO. La MIO consta de tres componentes principales:

- Agente inteligente
- License Manager
- AppAG

Arquitectura general



Nomenclatura

Término	Descripción

Cisco License Authority	Motor de licencias de Cisco para Smart Licensing. Mantiene toda la información relacionada con las licencias de productos. Esto incluye los derechos y la información del dispositivo.
Cuenta de Smart License	Una cuenta que tiene todos los derechos para el dispositivo.
ID de token	Se utiliza un identificador para distinguir la cuenta de Smart License cuando se registra el dispositivo.
Derecho	Equivalente a una licencia. Corresponde a una función individual o a todo un nivel de funciones.
Clave de activación de producto (PAK)	El antiguo mecanismo de licencias. Vinculado a un único dispositivo.

Estados de Smart Agent

Estado	Descripción
No Configurado	Las licencias inteligentes no están habilitadas.
No Identificado	Se han habilitado las licencias inteligentes, pero Smart Agent aún no se ha puesto en contacto con Cisco para registrarse.
Registrado	El agente se ha puesto en contacto con la autoridad de licencias de Cisco y se ha registrado.
Autorizado	Cuando un agente recibe un estado de no conformidad en respuesta a una solicitud de autorización de derechos.
Incumplimiento (OOC)	Cuando un agente recibe un estado de OC en respuesta a una solicitud de autorización de derechos.
Autorización caducada	Si el agente no se ha comunicado con Cisco durante 90 días.

Derechos de ASA

Estos son los derechos de ASA admitidos:

- Nivel estándar
- Contexto múltiple
- Encriptación segura (3DES)
- Proveedor de servicios/móvil (GTP)

Configuración

Siga las instrucciones de estos documentos:

- Licencia de software inteligente (ASAv, ASA en Firepower)
- Gestión de licencias para ASA

Antes de cualquier configuración de nivel de característica:

```
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    *
*                                                                        *
**************************************************************************
```

Configurar nivel estándar:

```
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
```

Conmutación por fallo (alta disponibilidad)

Como se documenta en la Guía de configuración de ASA, cada unidad Firepower debe estar registrada con la Autoridad de licencia o el servidor satélite. Verificación desde ASA CLI:

```
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
```

La unidad en espera:

```
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
```

Caso práctico: Licencia de ASA HA en FP2100

- En 2100, ASA se comunica con el portal Cisco Smart Licensing (nube) a través de las interfaces ASA, no de la gestión de FXOS
- Debe registrar ambos ASA en el portal Cisco Smart Licensing (nube)

En este caso, la autenticación HTTP local se utiliza en una interfaz externa:

```
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
```

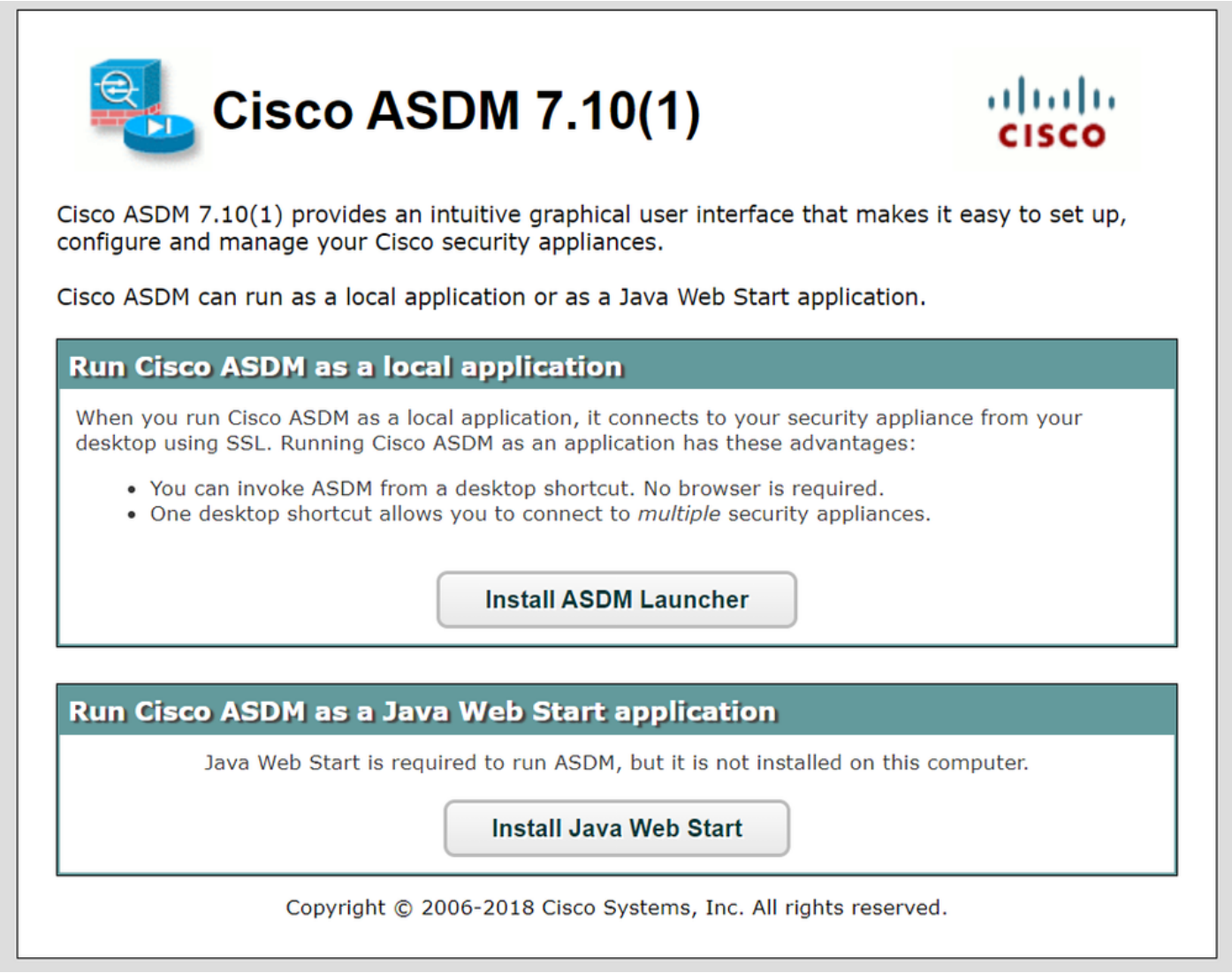
Solo puede conectarse al ASA a través de ASDM si hay una licencia 3DES/AES habilitada. Para un ASA que aún no está registrado esto es posible solamente en una interfaz que está management-only. Según la guía de configuración: "El cifrado avanzado (3DES/AES) está disponible para las conexiones de gestión antes de conectarse a la autoridad de licencias o al servidor satélite para

poder iniciar ASDM. Tenga en cuenta que el acceso ASDM sólo está disponible en las interfaces de administración con el cifrado predeterminado. No se permite el tráfico "mediante el dispositivo" hasta que no se conecte y obtenga la licencia de cifrado avanzado. En otro caso, obtendrá:

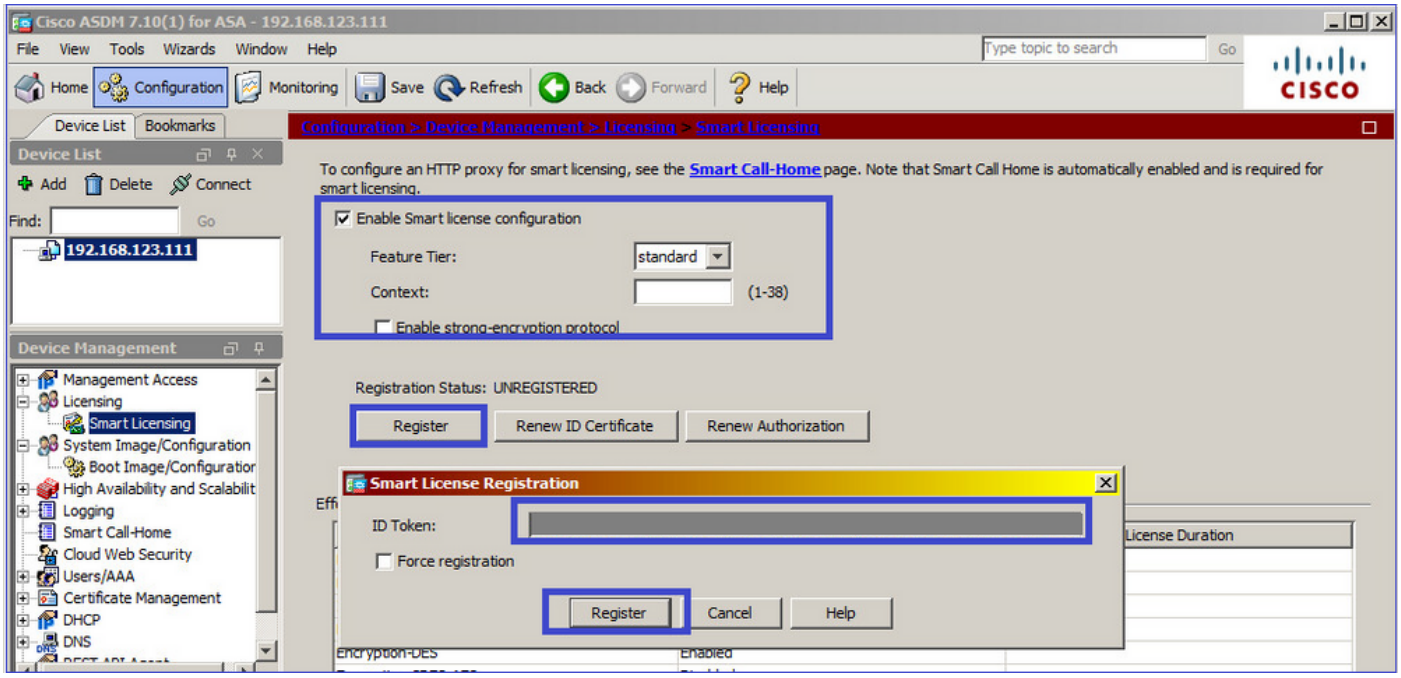
```
ciscoasa(config)# debug ssl 255
debug ssl enabled at level 255.
error:1408A0C1:SSL routines:ssl3_get_client_hello:no shared cipher
```

Para solucionar el problema, ASA solo tiene la administración configurada en la interfaz de cara a Internet y, por lo tanto, es posible la conexión ASDM:

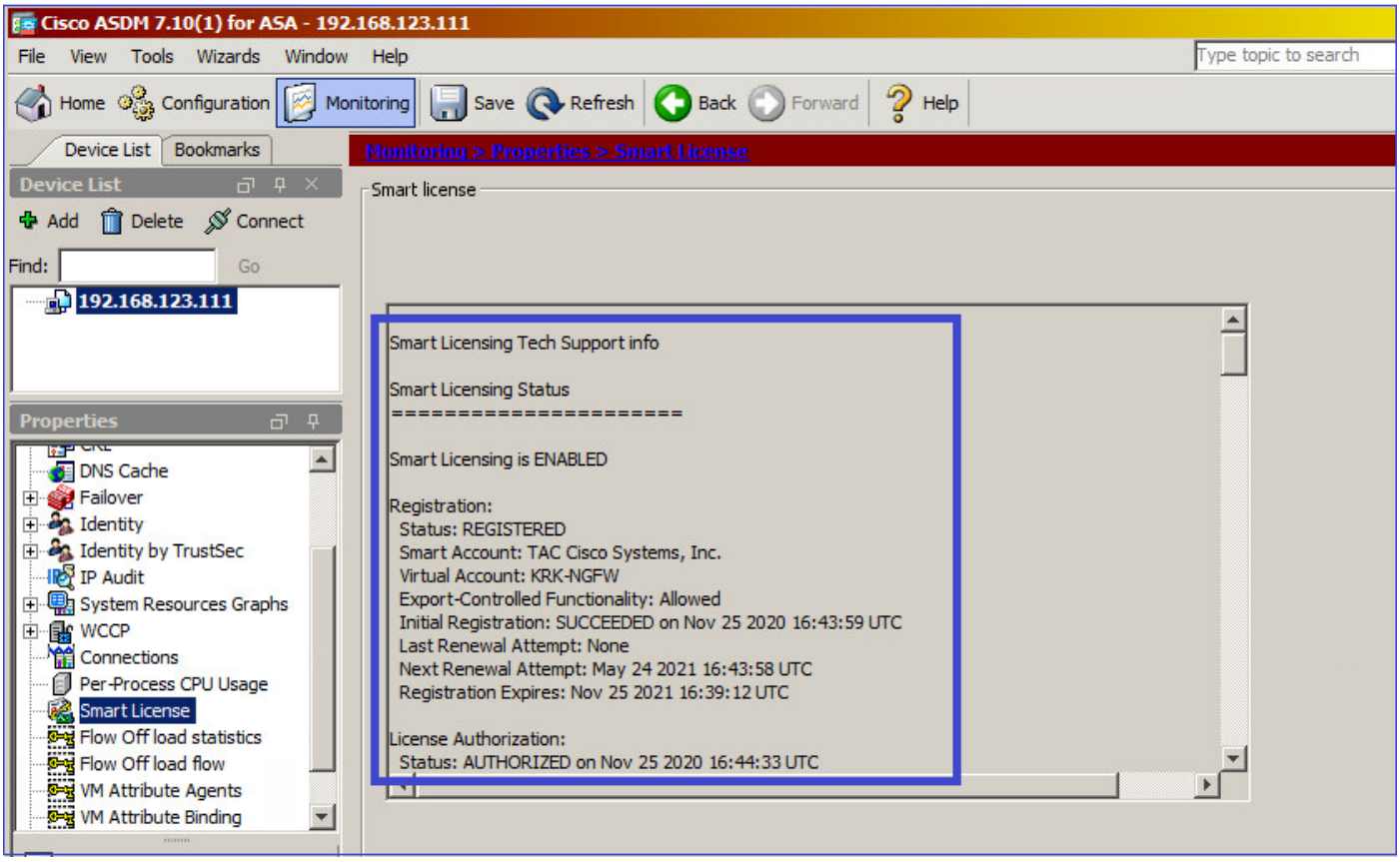
```
interface Ethernet1/2
management-only
nameif outside
security-level 100
ip address 192.168.123.111 255.255.255.0 standby 192.168.123.112
```



Configuración de Smart Licensing en ASA principal:



Desplácese hasta **Monitoring > Properties > Smart License** para comprobar el estado del registro:



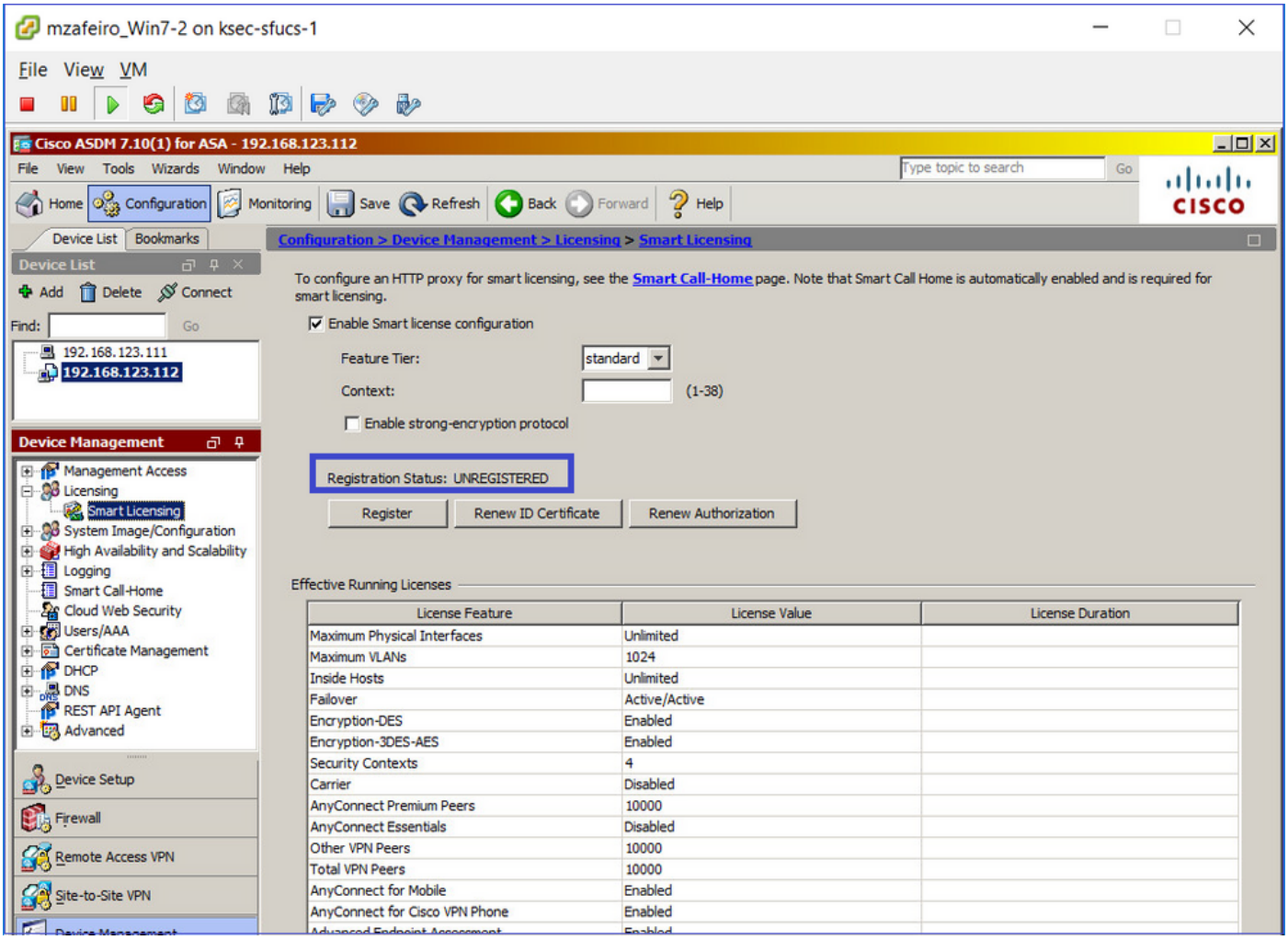
Verificación CLI de ASA principal:

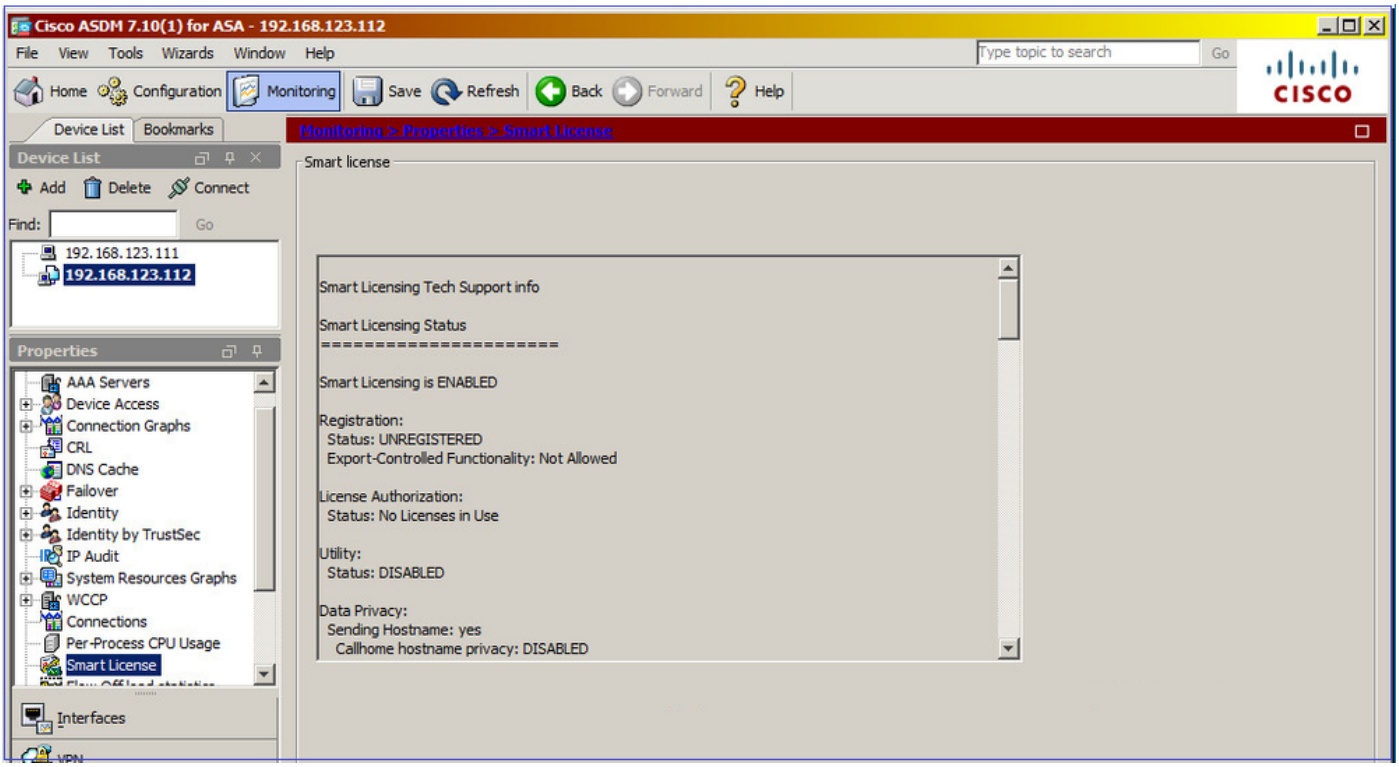
```
ciscoasa/pri/act# show license all

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
```

Conectar a través de ASDM al ASA en espera (esto solo es posible si el ASA se ha configurado con una IP en espera). El ASA en espera se muestra como UNREGISTERED y esto es lo que se espera, ya que aún no se ha registrado en el portal de Smart Licensing:





La CLI de ASA en espera muestra:

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

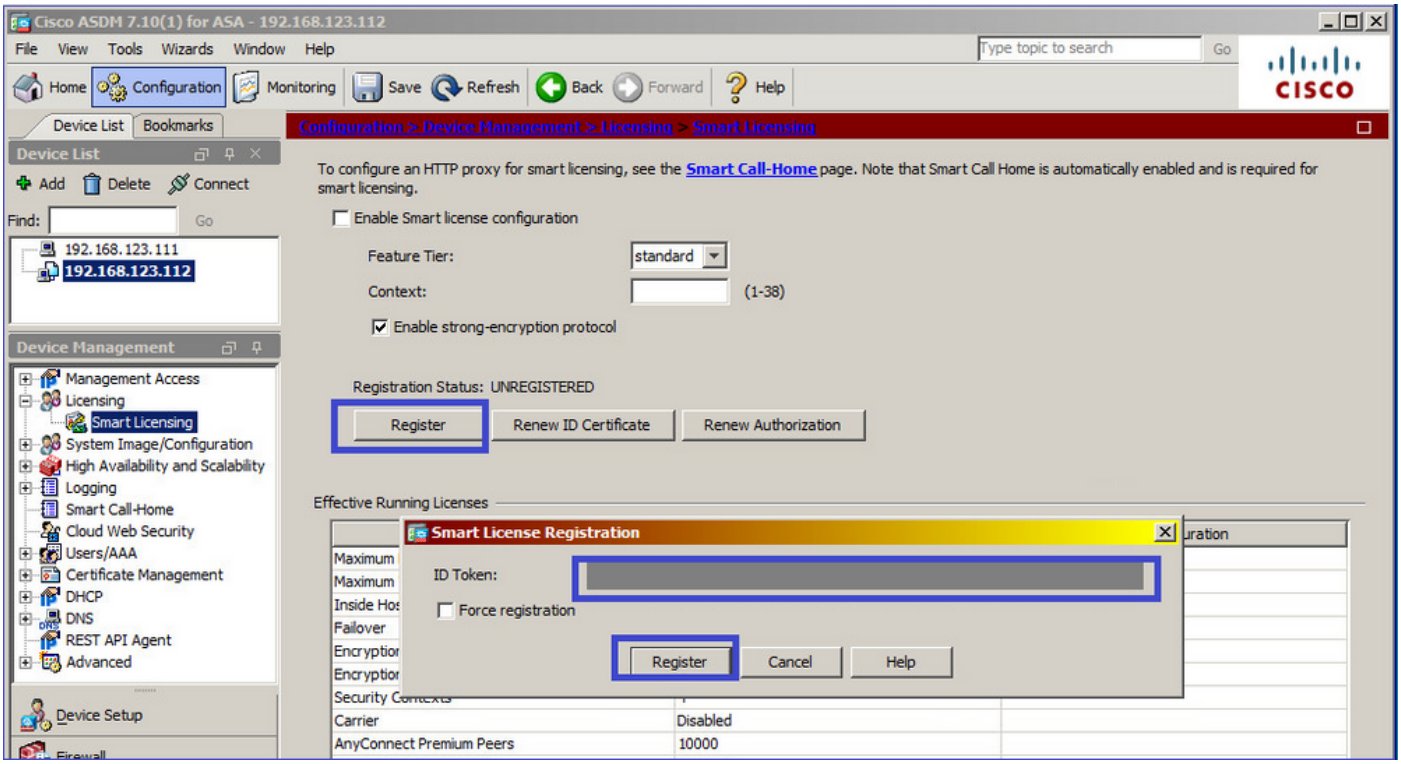
```
Smart Licensing Status
======================

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
```

Las funciones de licencia habilitadas en el ASA en espera:

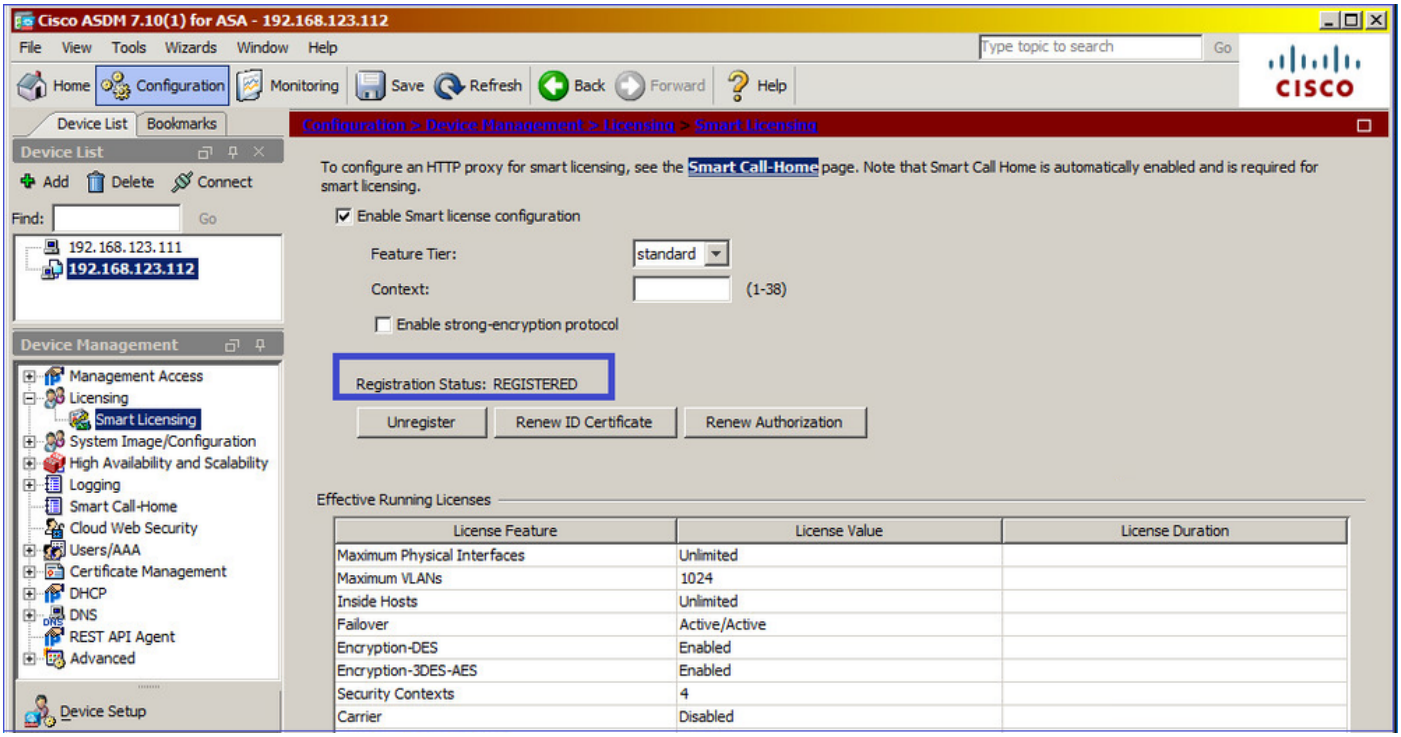
```
ciscoasa/sec/stby# show license features
Serial Number: JAD123456A
Export Compliant: NO

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
```

Registre el ASA en espera:



El resultado en el ASA en espera es que es REGISTERED:



Verificación de CLI en ASA en espera:

```
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
```

Clúster ASA

Si los dispositivos tienen una discordancia de licencia, el clúster no se forma:

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

Una configuración de clúster correcta:

```
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.
```

Nodo de control de clúster:

```
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
```

Unidad de datos del clúster:

```
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
```

Verificación y depuración

Resumen de comandos de verificación del chasis (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
```

Verificación de configuración:

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

Resumen de comandos de verificación de 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
```

Salidas de muestra de chasis (MIO) de comandos de verificación

```
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
```

Resultados de muestra de ASA de comandos de verificación

```
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
```

Registro correcto

El resultado proviene de la interfaz de usuario (IU) del administrador del chasis:

```
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
```

Autorización caducada

El resultado proviene de la interfaz de usuario del administrador de chasis:

```
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
```

Salidas de muestra de la CLI del chasis

NO REGISTRADO

```
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
```

Registro en curso

```
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
```

Error de registro

```
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
```

Período de evaluación

```
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
```

Problemas comunes de licencia en el chasis FXOS (MIO)

Error de registro: token no válido

```
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."]}
```

Pasos recomendados

1. Compruebe si la URL de inicio de llamada apunta a CSSM.
2. Inicie sesión en el CSSM y compruebe si el token se genera desde allí o si ha caducado.

Error de registro: el producto ya está registrado

```
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."]}
```

Pasos recomendados

1. Inicie sesión en el CSSM.
2. Compruebe el Product Instances en TODAS las cuentas virtuales.
3. Localice la instancia de registro anterior por SN y elimínela.
4. Este problema podría deberse a estos dos motivos: Error al renovar automáticamente cuando la fecha/hora no está configurada correctamente; por ejemplo, no se ha configurado ningún servidor NTP.Orden incorrecto de las operaciones cuando cambia entre un satélite y un servidor de producción, por ejemplo, cambie primero la URL y luego ejecute 'anular registro'

Error de registro: desplazamiento de fecha más allá del límite

```
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."]}
```

Paso recomendado

Compruebe la configuración de fecha y hora para asegurarse de que se ha configurado un servidor NTP.

Error de registro: no se pudo resolver el host

```
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
```

Pasos recomendados

1. Compruebe si la URL de callhome SLDest es correcta (scope monitoring > scope callhome > show expand)
2. Verifique si la configuración del servidor DNS MIO es correcta, por ejemplo, desde CLI:

```
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. Intente hacer ping desde la CLI del chasis al **tools.cisco.com** y ver si resuelve:

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

4. Intente hacer ping desde la CLI del chasis al servidor 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. Habilite la captura en la interfaz de administración del chasis (MIO) (esto solo se aplica en FP41xx/FP93xx) y compruebe la comunicación DNS mientras ejecuta una prueba de ping a la **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
```

Error de registro: no se pudo autenticar el servidor

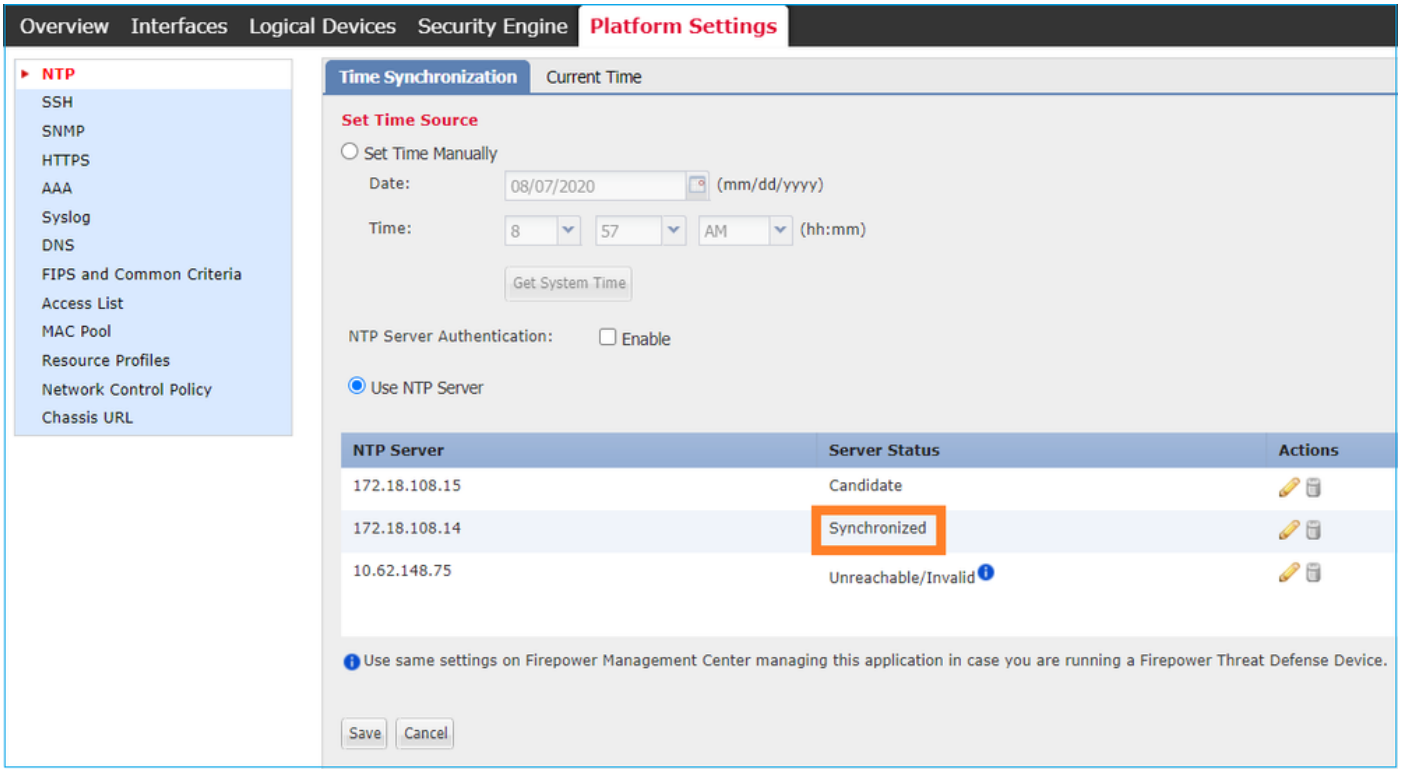
```
FPR4125-1# show license all

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
```

Pasos recomendados

1. Compruebe si el punto de confianza MIO CHdefault tiene el certificado correcto, por ejemplo:

```
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. Compruebe si el servidor NTP y la zona horaria están configurados correctamente. La verificación de certificados necesita el mismo tiempo entre el servidor y el cliente. Para lograr esto, utilice NTP para sincronizar la hora. Por ejemplo, la verificación de la IU de FXOS:



Verificación de 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
```

Active una captura y compruebe la comunicación TCP (HTTPS) entre la MIO y la **tools.cisco.com**. Aquí tiene algunas opciones:

- Puede cerrar la sesión HTTPS con la interfaz de usuario de FXOS y, a continuación, establecer un filtro de captura en CLI para HTTPS, por ejemplo:

```
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
```

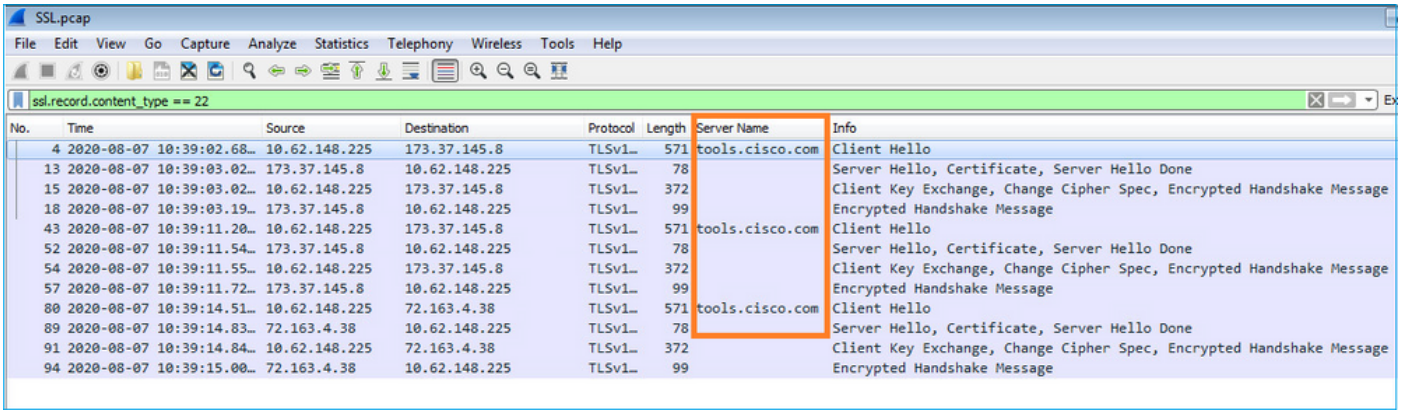
- Además, si desea mantener la interfaz de usuario de FXOS abierta, puede especificar en la captura las IP de destino (72.163.4.38 y 173.37.145.8 son el **tools.cisco.com** servidores en el momento de escribir este documento). También se recomienda guardar la captura en formato pcap y comprobarla en Wireshark. Este es un ejemplo de un registro exitoso:

```
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
```

- Para exportar el archivo pcap a un servidor FTP remoto:

```
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)#
```



Error de registro: error en el transporte 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
```

Pasos recomendados

1. Compruebe si la URL de inicio de llamada es correcta. Puede comprobarlo desde la interfaz de usuario de FXOS o desde la CLI (**scope monitoring > show callhome detail expand**).
2. Active una captura y compruebe la comunicación TCP (HTTPS) entre la MIO y la **tools.cisco.com** como se muestra en la sección "Error al autenticar el servidor" de este documento.

Error de registro: no se pudo conectar al host

```
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
```

Pasos recomendados

1. Si se habilita una configuración de proxy, verifique que la URL y el puerto del proxy estén configurados correctamente.
2. Active una captura y compruebe la comunicación TCP (HTTPS) entre la MIO y la **tools.cisco.com** como se muestra en la sección "Error al autenticar el servidor" de este documento.

Error de registro: el servidor HTTP devuelve un código de error >= 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
```

Pasos recomendados

1. Si hay una configuración de proxy habilitada, póngase en contacto con el administrador del

servidor proxy para obtener información acerca de la configuración de proxy.

2. Active una captura y compruebe la comunicación TCP (HTTPS) entre la MIO y la **tools.cisco.com** como se muestra en la sección "Error al autenticar el servidor" de este documento. Intente registrarse de nuevo (opción "force") desde la CLI de FXOS:

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

Error de registro: error en el mensaje de respuesta del motor de análisis

```
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
```

Pasos recomendados

1. Intentos de reintento automático más tarde. Use 'renovar' para volver a intentarlo inmediatamente.

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

2. Compruebe si la URL de inicio de llamada es correcta.

Problemas de licencia en ASA - 1xxx/21xx Series

Error de registro: error de envío de mensaje de comunicación

```
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
```

Pasos recomendados

1. Compruebe la configuración de DNS

```
ciscoasa# show run dns
```

2. Intente hacer ping **tools.cisco.com**. En este caso, se utiliza la interfaz de administración:

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

3. Compruebe la tabla de enrutamiento:

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

Asegúrese de que tiene una licencia habilitada, por ejemplo:

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

4. Habilite la captura en la interfaz que enruta hacia el **tools.cisco.com** (si realiza la captura sin ningún filtro IP, asegúrese de que no tenga abierto ASDM cuando realice la captura para evitar ruidos de captura innecesarios).

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

> **Advertencia**: la captura de paquetes puede tener un impacto negativo en el rendimiento.

5. Habilite temporalmente el nivel 7 de Syslog (debug) y verifique los mensajes de Syslog de ASA durante el proceso de registro:

```
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
```

Intente registrarse de nuevo:

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

Requisitos especiales para los derechos complementarios

- Es necesario adquirir un derecho de nivel de característica válido antes de configurar cualquier derecho de complemento
- Todos los derechos de complementos deben liberarse antes de liberar el derecho de nivel de característica

Estado de autorización durante la operación de reinicio

- Los estados de derecho se guardan en la memoria flash
- Durante el arranque, esta información se lee de la memoria flash y las licencias se establecen en función del modo de aplicación guardado
- La configuración de inicio se aplica en función de esta información de derechos almacenada en caché
- Los derechos se solicitan de nuevo después de cada reinicio

Compromiso con el soporte del Cisco TAC

FP41xx/FP9300

Si todos los elementos mencionados en este documento fallan, recopile estos resultados de la CLI del chasis y comuníquese con el TAC de Cisco:

Resultado 1:

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

Resultado 2:

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

Resultado 3:

Paquete de soporte de chasis FXOS

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

Resultado 4 (muy recomendado):

Captura de Ethanalyzer desde la CLI del chasis

FP1xxx/FP21xx

Resultado 1:

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

Resultado 2:

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

Preguntas más frecuentes (FAQ)

En FP21xx, ¿dónde está la ficha Licencias en la interfaz gráfica de usuario del chasis (FCM)?

A partir de la versión 9.13.x, FP21xx admite 2 modos ASA:

- Dispositivo
- Platform

En el modo de dispositivo, no hay ninguna interfaz de usuario de chasis. En el modo de plataforma, hay una interfaz de usuario del chasis, pero la licencia se configura desde la CLI de ASA o ASDM.
Por otro lado, en las plataformas FPR4100/9300, la licencia debe configurarse en FCM mediante GUI o FXOS CLI y los derechos de ASA deben solicitarse a ASA CLI o ASDM.
Referencias:

- Gestión de licencias para ASA
- Dispositivos lógicos para Firepower 4100/9300
- Licencias: licencia de software inteligente (ASAv, ASA en Firepower)
- Implementación del modo de plataforma ASA con ASDM y Firepower Chassis Manager

¿Cómo puede habilitar una licencia de cifrado segura?
Esta funcionalidad se habilita automáticamente si el token utilizado en el registro de FCM tenía la opción de permitir la funcionalidad de control de exportación en los productos registrados con este token habilitado.

¿Cómo puede habilitar una licencia de cifrado fuerte si las funciones controladas por exportación en el nivel de FCM y el cifrado 3DES-AES relacionado en el nivel de ASA están inhabilitadas?
Si el token no tiene esta opción habilitada, anule el registro de FCM y regístrelo de nuevo con un token que tenga esta opción habilitada.

¿Qué puede hacer si la opción Permitir la funcionalidad de exportación controlada en los productos registrados con este token no está disponible al generar el token?
Póngase en contacto con su equipo de cuentas de Cisco.

¿Es obligatorio configurar la función Strong Encryption en el nivel ASA?
La opción de encriptación segura de la función es obligatoria solo si FCM está integrado con un servidor satélite anterior a la versión 2.3.0. Este es solo un escenario en el que debe configurar esta función.

¿Qué IP se deben permitir en la ruta entre FCM y la nube de licencias inteligentes?
El FXOS utiliza la dirección https://tools.cisco.com/ (puerto 443) para comunicarse con la nube de licencias. La dirección https://tools.cisco.com/ se resuelve en estas direcciones IP:

- 72.163.4.38
- 173.37.145.8

¿Por qué aparece un error de incumplimiento?
El dispositivo puede quedar fuera de conformidad en las siguientes situaciones:

- Utilización excesiva (el dispositivo utiliza licencias no disponibles)
- Expiración de la licencia: una licencia basada en tiempo ha caducado
- Falta de comunicación: el dispositivo no puede ponerse en contacto con la autoridad responsable de las licencias para volver a autorizarlo

Para comprobar si su cuenta se encuentra en un estado de Incumplimiento o se acerca a él, debe comparar los derechos que actualmente utiliza su chasis Firepower con los de su cuenta Smart Account.
En un estado de incumplimiento, puede realizar cambios de configuración en funciones que requieren licencias especiales, pero la operación no se verá afectada. Por ejemplo, en los contextos de límite de licencia estándar que ya existen, se sigue ejecutando y se puede modificar su configuración, pero no se puede agregar un nuevo contexto.

¿Por qué sigue recibiendo un error de incumplimiento después de agregar las licencias?
De forma predeterminada, el dispositivo se comunica con la autoridad de licencias cada 30 días

para comprobar los derechos. Si desea activarlo manualmente, debe seguir estos pasos:

Para las plataformas FPR1000/2100, debe hacerse a través de ASDM o de CLI:

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

Para las plataformas FPR4100/9300, se debe realizar a través de la CLI de FXOS:

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

¿Por qué no hay ninguna licencia en uso en el nivel ASA?

Asegúrese de que el derecho de ASA se haya configurado en el nivel de ASA, por ejemplo:

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

¿Por qué las licencias siguen sin utilizarse incluso después de la configuración de un derecho de ASA?

Este estado se espera si ha implementado un par de failover activo/en espera de ASA y comprueba el uso de la licencia en el dispositivo en espera.
Según la Guía de configuración, la configuración se replica en la unidad standby, pero la unidad standby no utiliza la configuración; permanece en un estado en caché. Sólo la unidad activa solicita las licencias al servidor. Las licencias se agregan en una sola licencia de failover que es compartida por el par de failover, y esta licencia agregada también se almacena en caché en la unidad standby que se utilizará si se convierte en la unidad activa en el futuro. Para referencia: Licencias de clúster de conmutación por error o ASA.

¿Qué puede hacer si FCM no tiene acceso a Internet?

Como alternativa, puede implementar Cisco Smart Software Manager en las instalaciones (anteriormente conocido como satélite Cisco Smart Software Manager). Se trata de un componente de Cisco Smart Licensing que funciona junto con Cisco Smart Software Manager. Ofrece visibilidad casi en tiempo real y capacidades de generación de informes de las licencias de Cisco que compra y consume. También proporciona a las organizaciones sensibles a la seguridad una forma de acceder a un subconjunto de la funcionalidad de Cisco SSM sin el uso de una conexión directa a Internet para gestionar su base instalada.

¿Dónde puede encontrar más información sobre Cisco Smart Software Manager On-Prem?

Puede encontrar esta información en la Guía de configuración de FXOS:

- Configuración de un servidor satélite de licencia inteligente para el chasis Firepower 4100/9300
- Configuración del registro de Firepower Chassis Manager en un administrador de software inteligente in situ

Información Relacionada

- Guía de configuración CLI de operaciones generales de la serie Cisco ASA
- Gestión de licencias para ASA
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).