Solução de problemas do ASA Smart License em dispositivos FXOS Firepower

Contents

Introduction

Este documento descreve o recurso Smart Licensing do Adaptive Security Appliance (ASA) no Firepower eXtensible Operating System (FXOS).

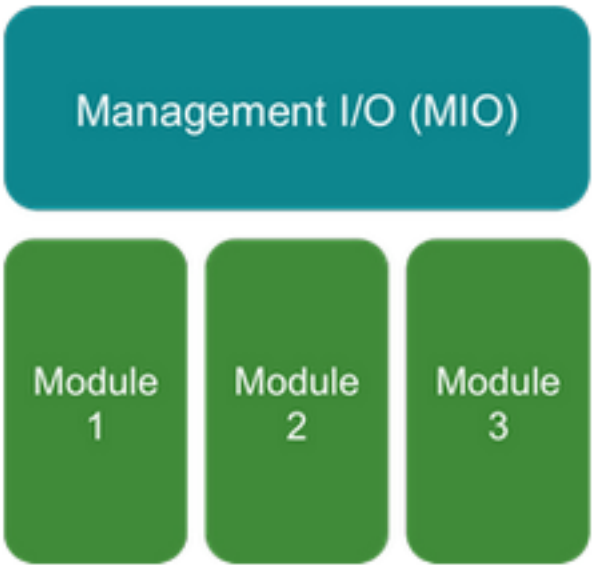
Informações de Apoio

O Smart Licensing no FXOS é usado quando há um ASA instalado no chassi. Para o Firepower Threat Defense (FTD) e o Firepower Management Center (FMC), o Smart Licensing verifica o registro e a solução de problemas do FMC e do FTD Smart License.

Este documento aborda principalmente os cenários em que o chassi FXOS tem acesso direto à Internet. Se o chassi FXOS não puder acessar a Internet, você precisará considerar um servidor satélite ou uma reserva de licença permanente (PLR). Consulte o guia de configuração do FXOS para obter mais detalhes sobre o Gerenciamento Offline.

Arquitetura do Smart Licensing

Uma visão geral de alto nível dos componentes do chassi:

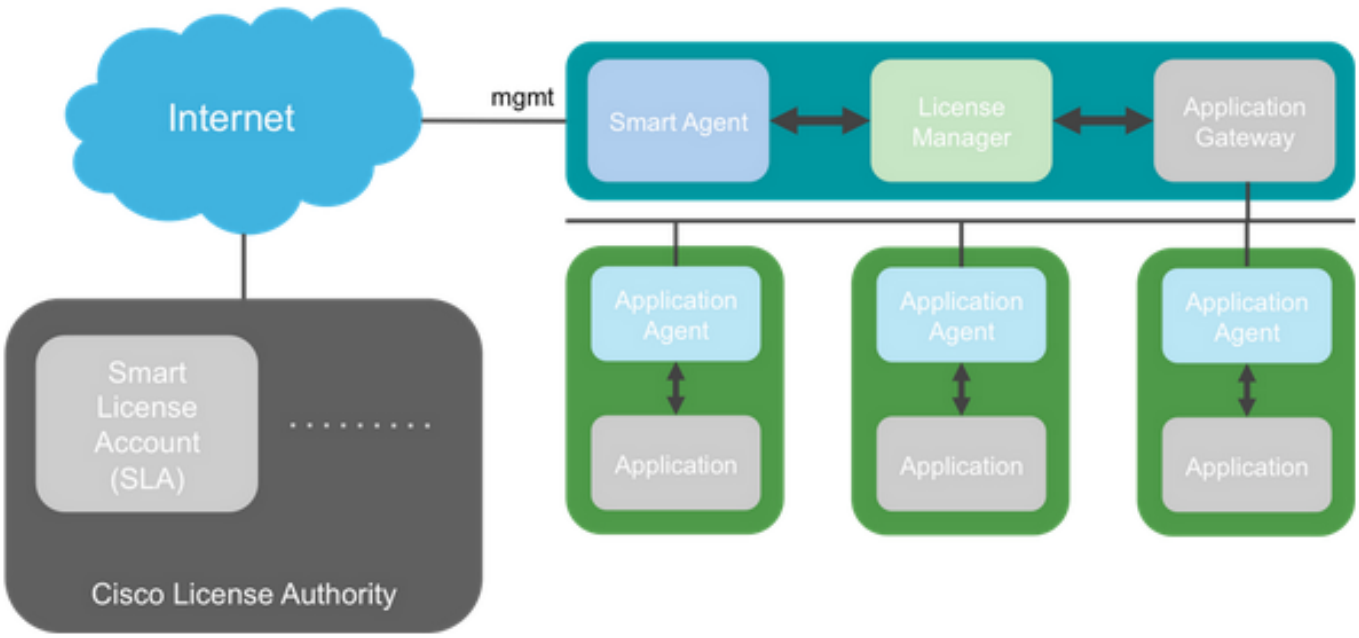


- Os módulos Management Input/Output (MIO) e individuais desempenham funções no Smart Licensing
- O próprio MIO não exige licenças para sua operação
- Os aplicativos SA em cada módulo precisam ser licenciados

O supervisor FXOS é o MIO. O MIO contém três componentes principais:

- Agente inteligente
- License Manager
- AppAG

Arquitetura geral



Nomenclatura

Termo	Descrição

Autoridade de licença da Cisco	O back-end de licenças da Cisco para Smart Licensing. Mantém todas as informações relacionadas ao licenciamento do produto. Isso inclui direitos e informações do dispositivo.
Conta de Licença inteligente	Uma conta que tem todos os direitos para o equipamento.
ID do token	Um identificador é usado para distinguir a Smart License Account quando o dispositivo é registrado.
Direito	Equivalente a uma licença. Corresponde a um recurso individual ou a uma camada de recursos inteira.
Chave de ativação do produto (PAK)	O antigo mecanismo de licenciamento. Vinculado a um único dispositivo.

Estados de agentes inteligentes

Estado	Descrição
Não configurado	Licenciamento inteligente não habilitado.
Não Identificado	O licenciamento inteligente foi ativado, mas o Agente Inteligente ainda não entrou em contato com a Cisco para se registrar.
Registrado	O agente entrou em contato com a autoridade de licenciamento da Cisco e registrou-se.
Autorizado	Quando um agente recebe um status em conformidade em resposta a uma solicitação de autorização de qualificação.
Fora de conformidade (OOC)	Quando um agente recebe um status OOC em resposta a uma solicitação de Autorização de Direitos.
Autorização expirada	Se o agente não se comunicar com a Cisco por 90 dias.

Direitos do ASA

Estas são as qualificações suportadas do ASA:

- Camada padrão
- Contexto múltiplo
- Criptografia forte (3DES)
- Móvel/provedor de serviços (GTP)

Configuração

Siga as instruções destes documentos:

- Licenciamento de software inteligente (ASAv, ASA no Firepower)
- Gerenciamento de licenças para o ASA

Antes de qualquer configuração de camada de recursos:

```
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 camada padrão:

```
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
```

Failover (alta disponibilidade)

Conforme documentado no Guia de configuração do ASA, cada unidade Firepower deve ser registrada na autoridade de licença ou no servidor satélite. Verificação da CLI do 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
```

A unidade de standby:

```
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
```

Estudo de caso: Licença ASA HA no FP2100

- Em 2010, o ASA se comunica com o portal Cisco Smart Licensing (nuvem) através das interfaces do ASA, não do gerenciamento FXOS
- Você precisa registrar os dois ASAs no portal Cisco Smart Licensing (nuvem)

Nesse caso, a autenticação local HTTP é usada em uma interface 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
```

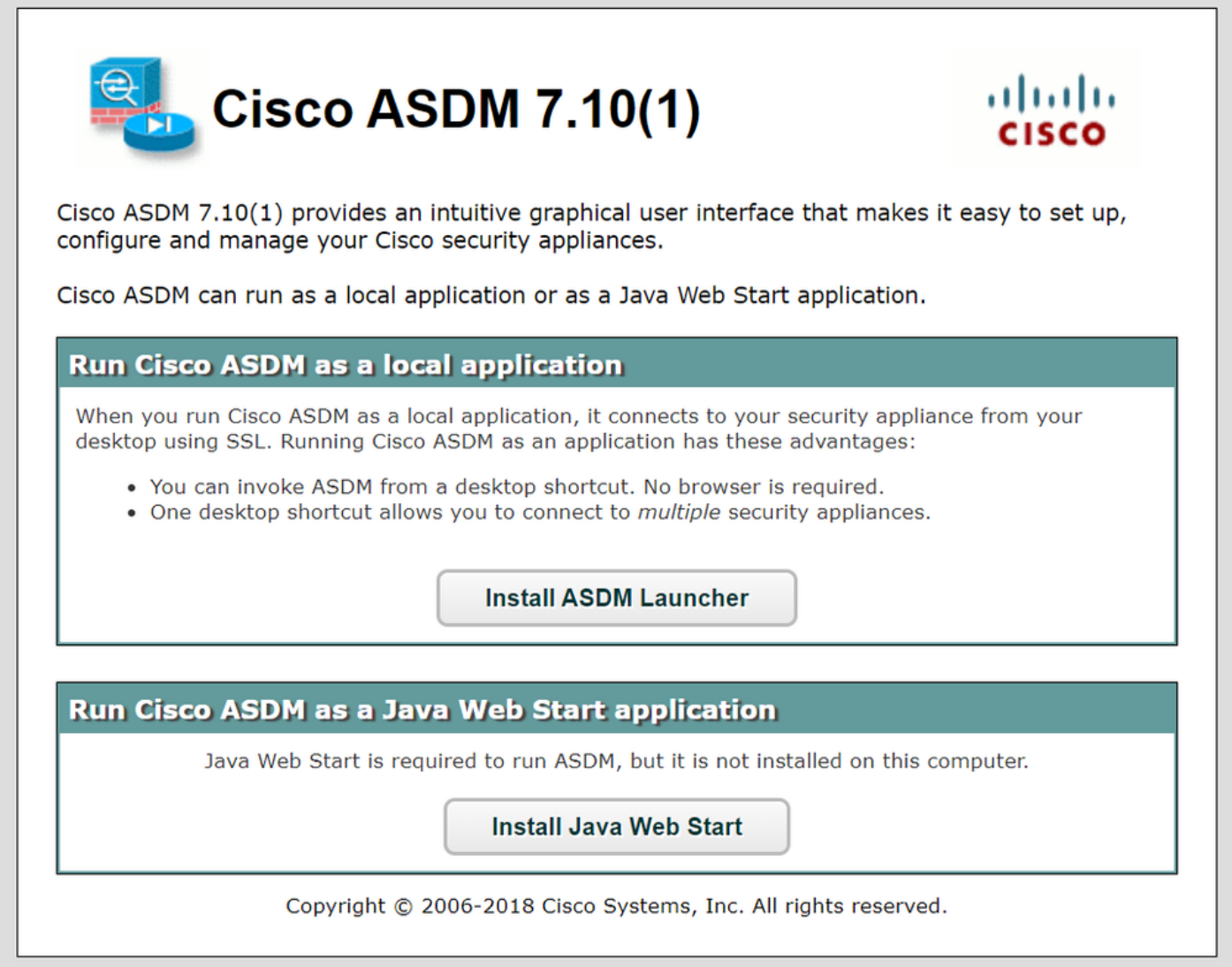
Você só poderá se conectar ao ASA via ASDM se houver uma licença 3DES/AES habilitada. Para um ASA que ainda não esteja registrado, isso só é possível em uma interface que esteja management-only. De acordo com o guia de configuração: "Strong Encryption (3DES/AES) está disponível para conexões de gerenciamento antes de você se conectar à autoridade de licença ou

ao servidor satélite para que você possa iniciar o ASDM. Observe que o acesso ao ASDM só está disponível em interfaces somente de gerenciamento com a criptografia padrão. O tráfego não incluído não é permitido até que você se conecte e obtenha a licença "Strong Encryption". Em um caso diferente, você obtém:

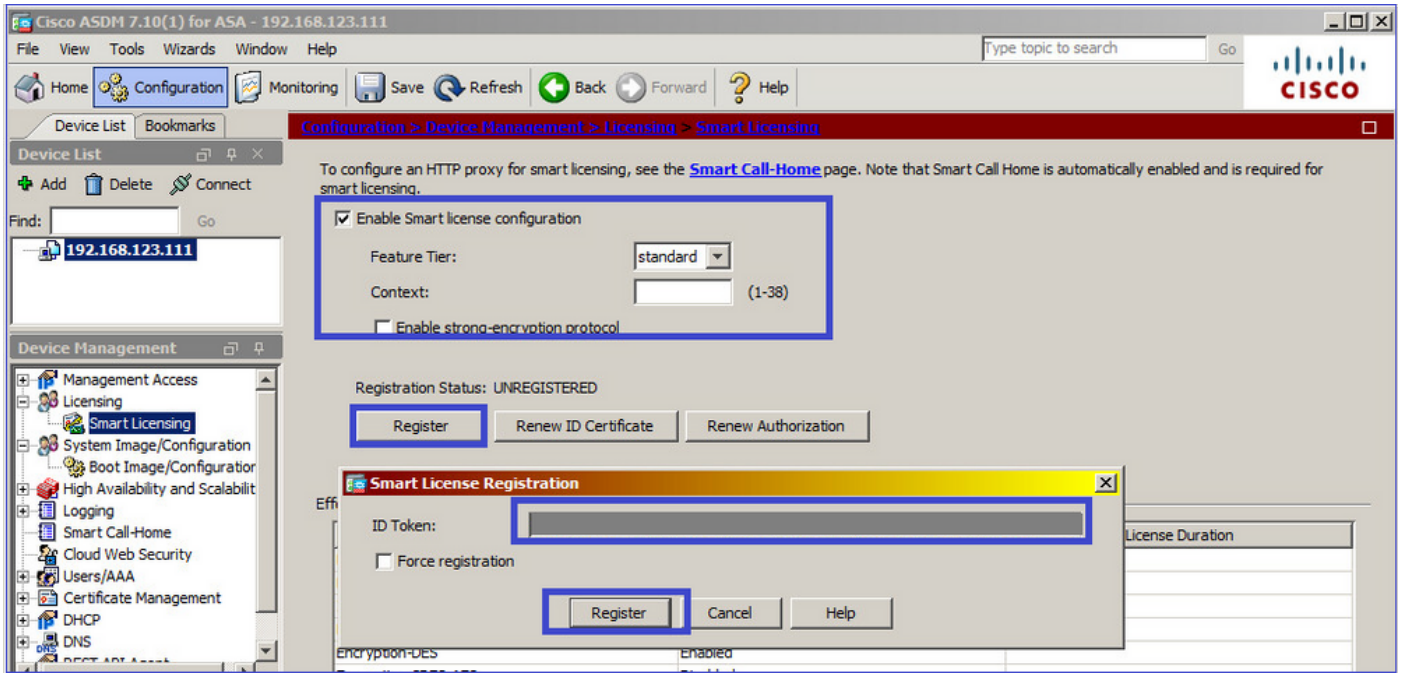
```
ciscoasa(config)# debug ssl 255
debug ssl enabled at level 255.
error:1408A0C1:SSL routines:ssl3_get_client_hello:no shared cipher
```

Para superar o ASA tem gerenciamento apenas configurado na interface de Internet e, assim, a conexão ASDM é possível:

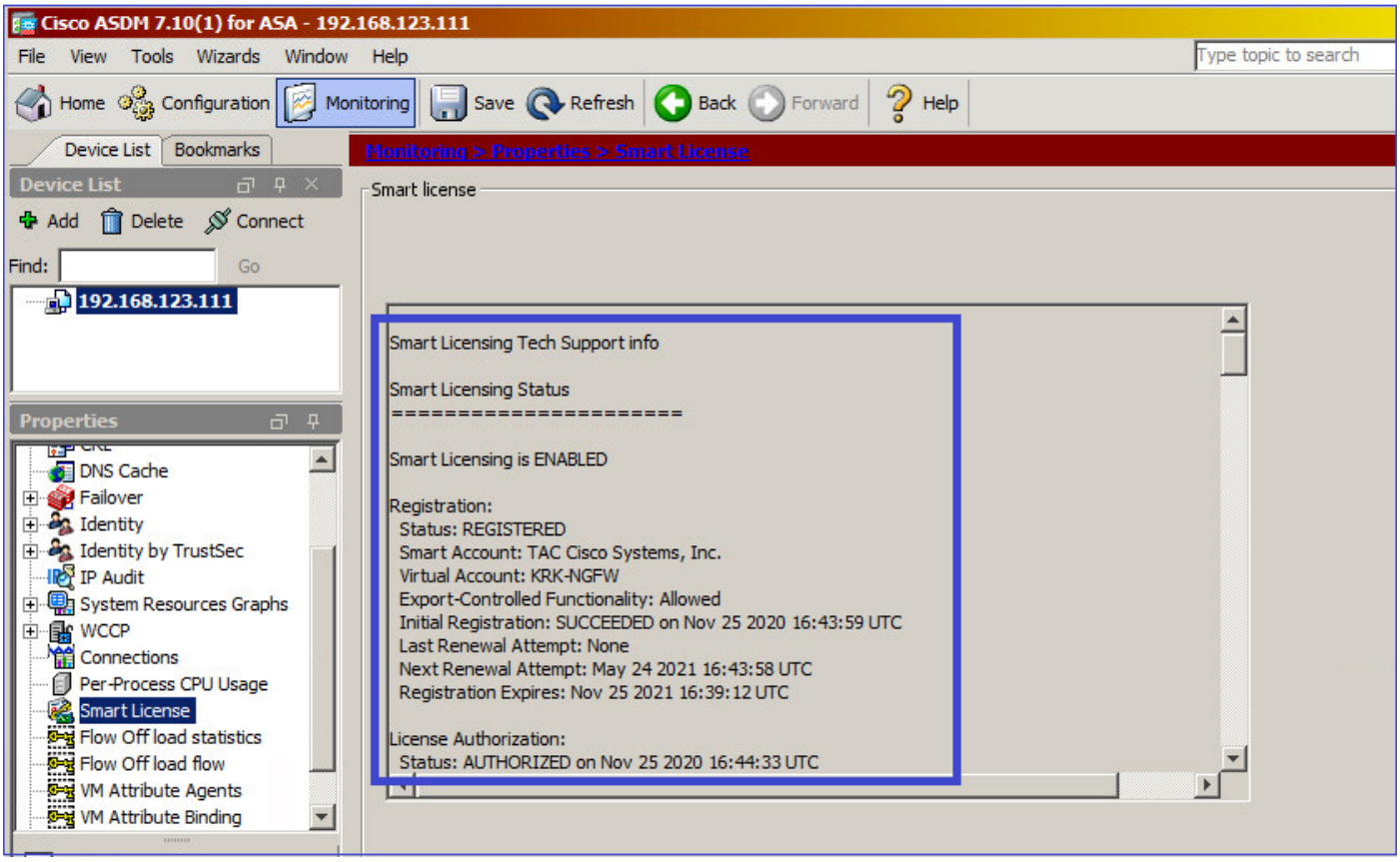
```
interface Ethernet1/2
management-only
nameif outside
security-level 100
ip address 192.168.123.111 255.255.255.0 standby 192.168.123.112
```



Configure o Smart Licensing no ASA principal:



Navegue até **Monitoring > Properties > Smart License** para verificar o status do registro:



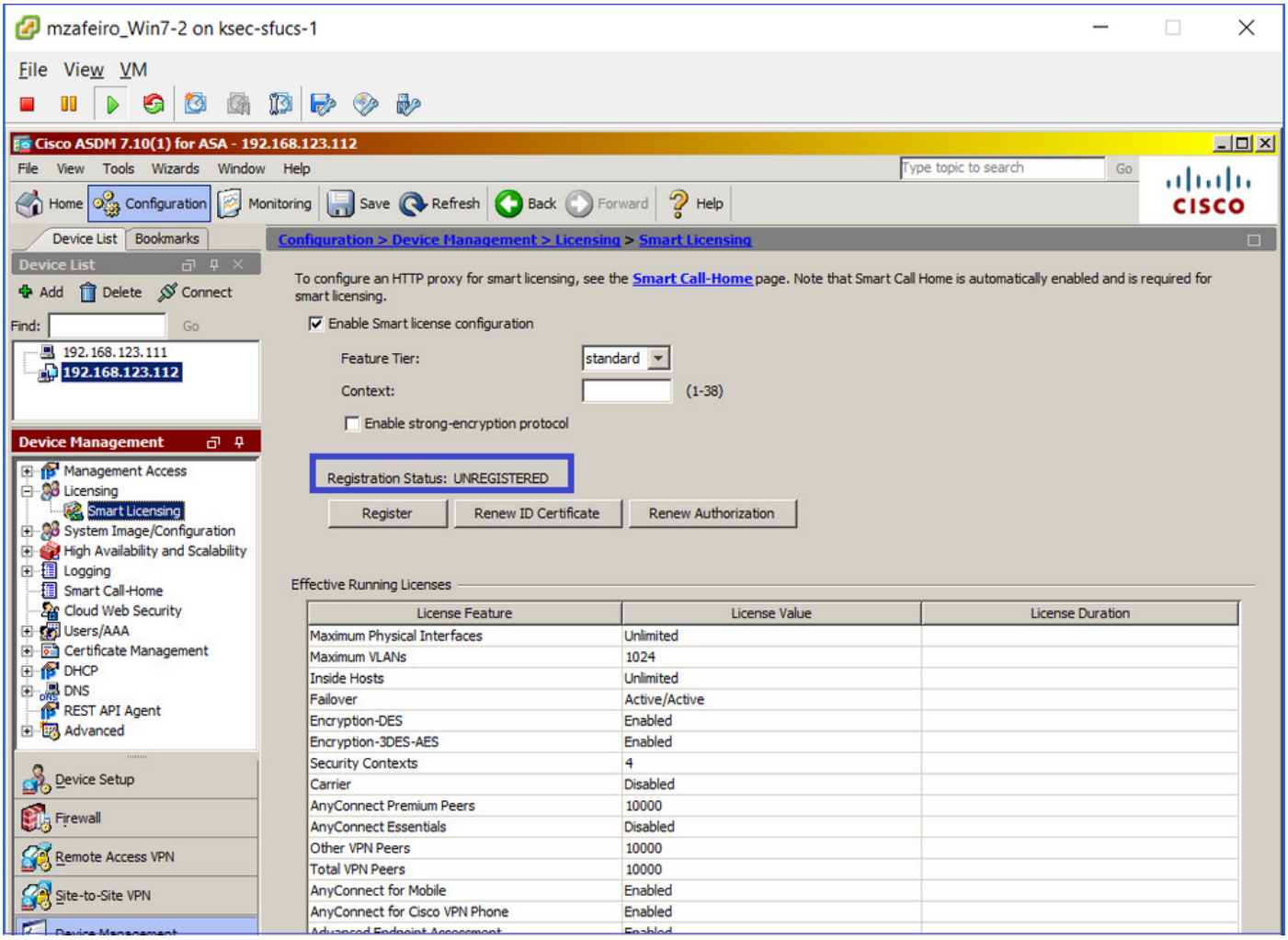
Verificação CLI do ASA primário:

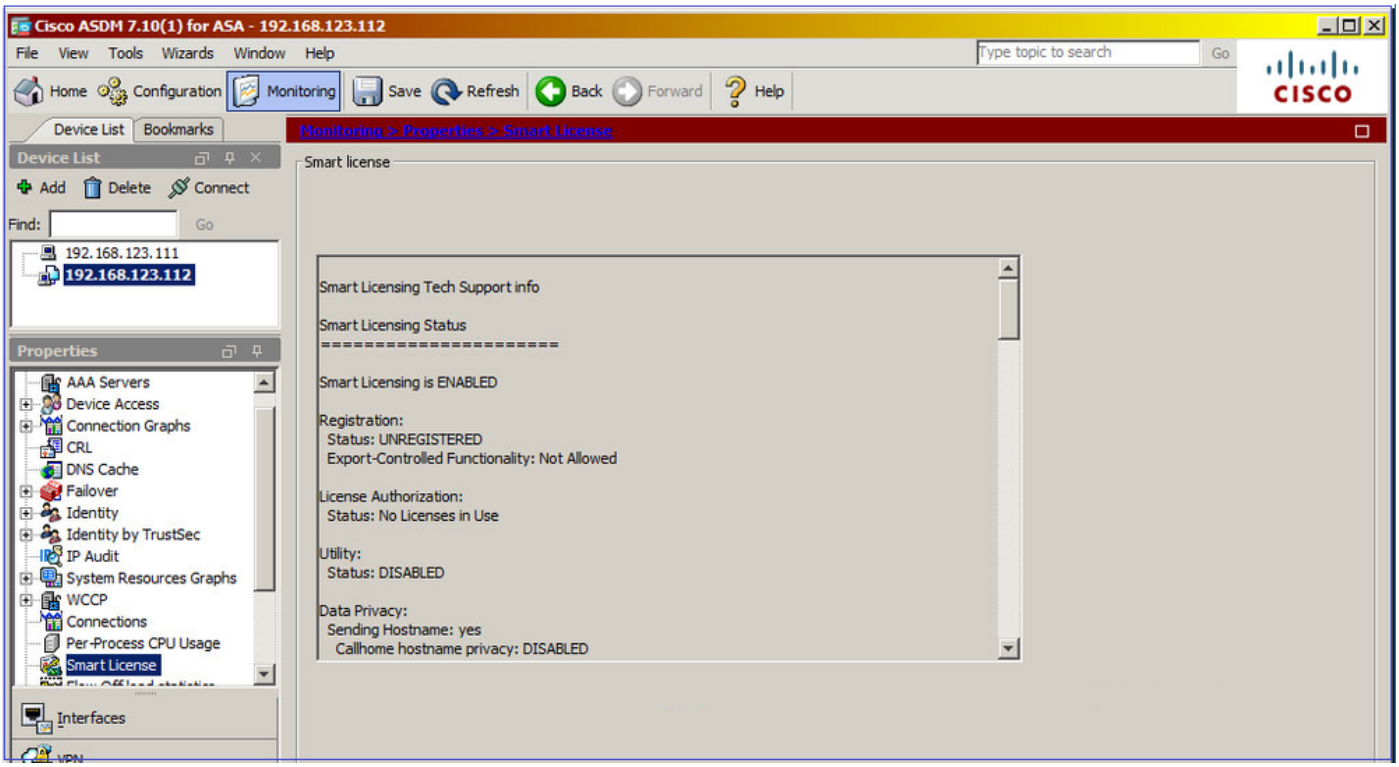
```
ciscoasa/pri/act# show license all

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-se via ASDM ao ASA em standby (isso só será possível se o ASA tiver sido configurado com um IP em standby). O ASA em standby é mostrado como UNREGISTERED e isso é esperado, já que ele ainda não foi registrado no portal Smart Licensing:





A CLI do ASA em standby mostra:

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

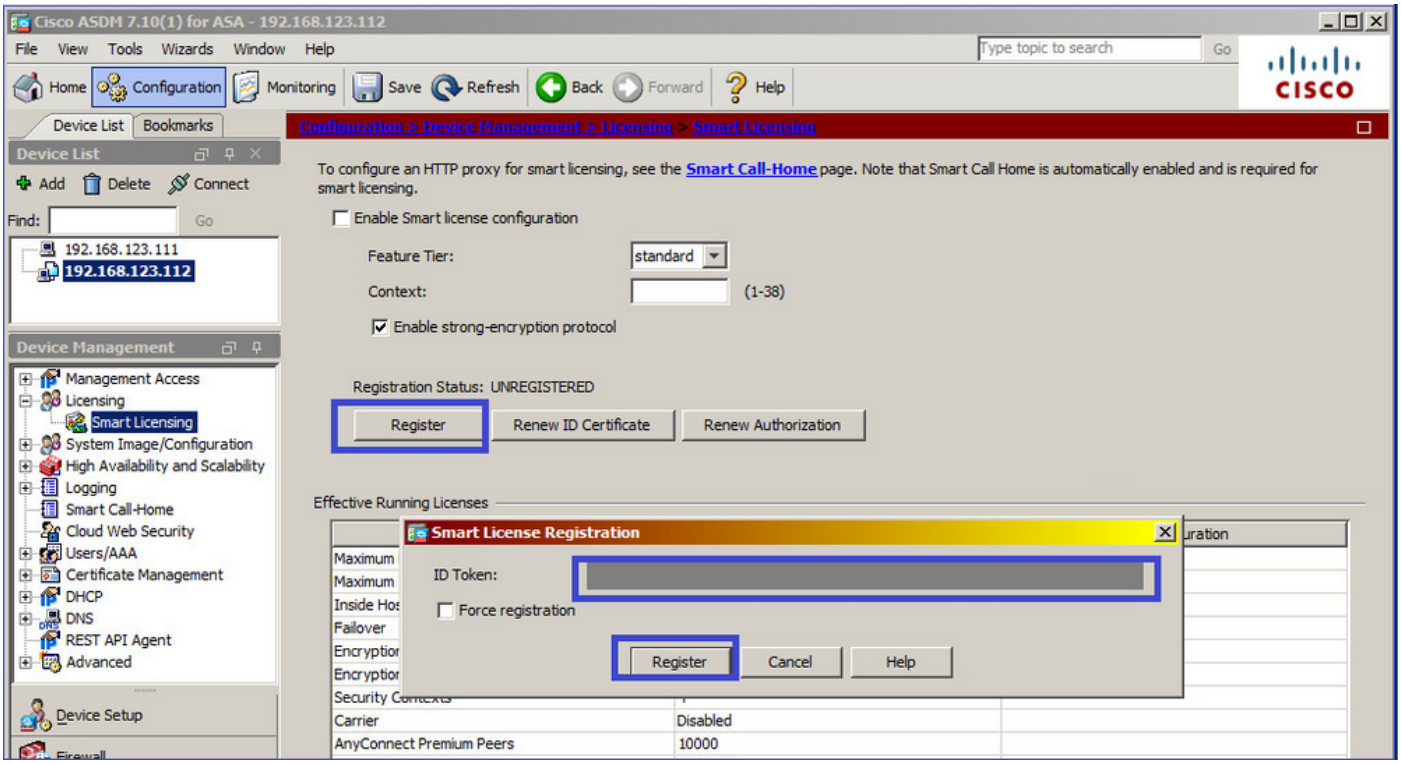
```
Smart Licensing Status
======================

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
```

Os recursos de licença ativados no ASA em standby:

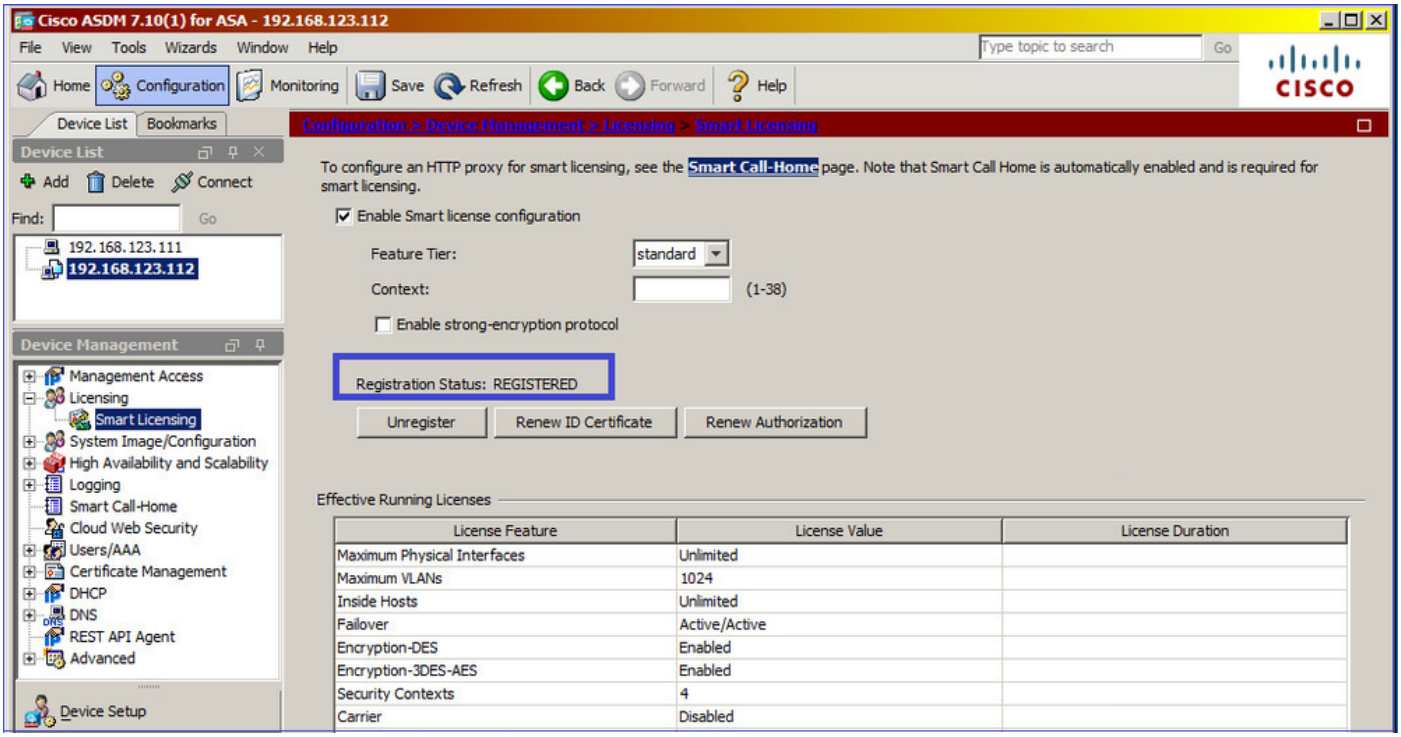
```
ciscoasa/sec/stby# show license features
Serial Number: JAD123456A
Export Compliant: NO

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 o ASA em espera:



O resultado no ASA em espera é que ele é REGISTERED:



Verificação de CLI no ASA em standby:

```
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

Se os dispositivos tiverem uma incompatibilidade de licença, o cluster não será formado:

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

Uma configuração de cluster bem-sucedida:

```
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.
```

Nó de Controle 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
```

Unidade de dados 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
```

Verificação e depuração

Resumo dos comandos de verificação do MIO (Chassis):

```
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
```

Verificação de configuração:

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

Resumo dos comandos de verificação do 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
```

Exemplos de saída de comandos de verificação do MIO (Chassis)

```
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
```

Exemplos de saída de comandos de verificação do 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
```

Registro bem-sucedido

A saída é da Interface do Usuário (UI) do gerenciador de chassis:

```
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
```

Autorização expirada

A saída é da interface do usuário do gerenciador de chassis:

```
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
```

Exemplos de saída do CLI do chassi

Não 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 em andamento

```
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
```

Erro 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 avaliação

```
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 Comuns de Licença no Chassi FXOS (MIO)

Erro de registro: token inválido

```
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."]}
```

Etapas recomendadas

1. Verifique se o URL do call-home aponta para o CSSM.
2. Faça login no CSSM e verifique se o token foi gerado a partir dele ou se expirou.

Erro de registro: produto já 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."]}
```

Etapas recomendadas

1. Faça login no CSSM.
2. Marque a caixa Product Instances em TODAS as Virtual Accounts.
3. Localize a instância de registro antiga por SN e remova-a.
4. Esse problema pode ser causado por estes dois: Falha ao renovar automaticamente quando a hora/data não está configurada corretamente; por exemplo, nenhum servidor NTP está configurado.Ordem errada de operações quando você alterna entre um satélite e um servidor de produção, por exemplo, altere a URL primeiro e, em seguida, emita 'deregister'

Erro de registro: deslocamento de data além do 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."]}
```

Etapa recomendada

Verifique a configuração de data/hora para garantir que um servidor NTP esteja configurado.

Erro de registro: falha ao resolver o 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
```

Etapas recomendadas

1. Verifique se a URL do SLDest do callhome está correta (scope monitoring > scope callhome > show expand)
2. Verifique se a configuração do servidor DNS MIO está correta, por exemplo, a partir da 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. Tente fazer ping a partir do CLI do chassi no **tools.cisco.com** e veja se ele resolve:

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

4. Tente fazer ping a partir do CLI do chassi para o 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 a interface de gerenciamento MIO (capture on chassis, captura no chassi) (aplicável somente em FP41xx/FP93xx) e verifique a comunicação DNS enquanto executa um teste de ping para o **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
```

Erro de registro: falha ao autenticar servidor

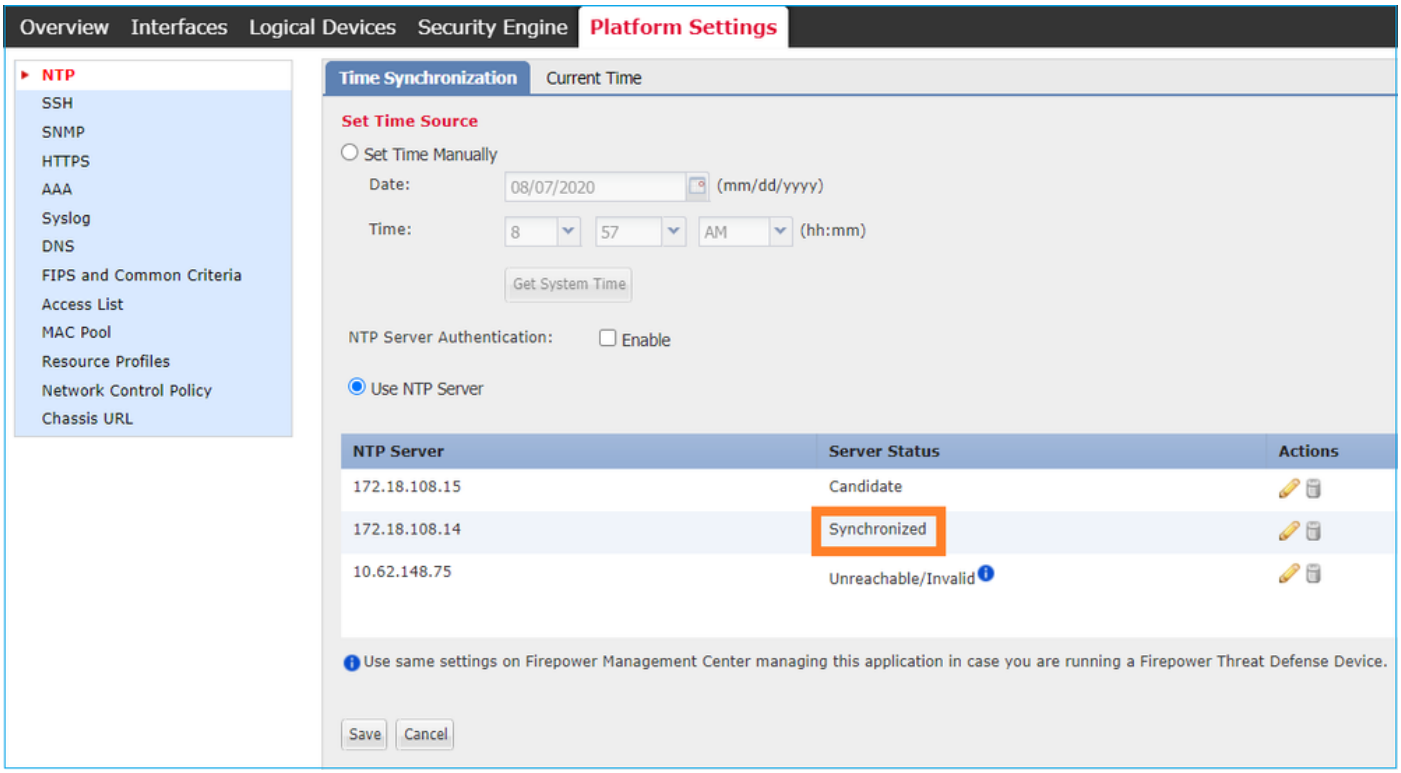
```
FPR4125-1# show license all

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
```

Etapas recomendadas

1. Verifique se o ponto de confiança MIO CHdefault tem o certificado correto, por exemplo:

```
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. Verifique se o servidor NTP e o fuso horário estão definidos corretamente. A verificação de certificado precisa do mesmo tempo entre o servidor e o cliente. Para fazer isso, use o NTP para sincronizar a hora. Por exemplo, verificação de interface de usuário FXOS:



Verificação da 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
```

Habilite uma captura e verifique a comunicação TCP (HTTPS) entre o MIO e o **tools.cisco.com**. Aqui você tem algumas opções:

- Você pode fechar sua sessão HTTPS para a interface do usuário FXOS e definir um filtro de captura na CLI para HTTPS, por exemplo:

```
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
```

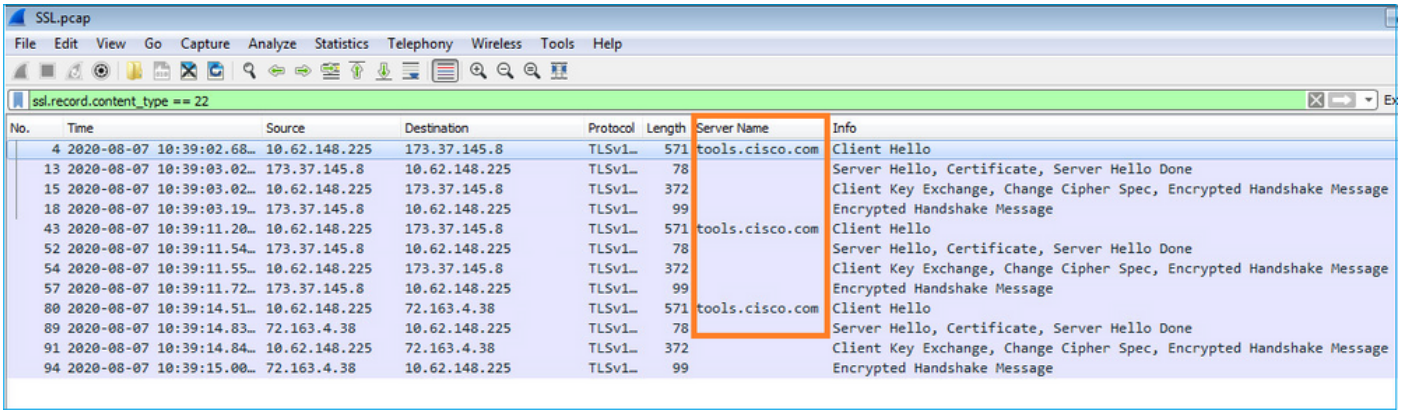
- Além disso, se desejar manter a interface do usuário FXOS aberta, você poderá especificar na captura que os IPs de destino (72.163.4.38 e 173.37.145.8) são os **tools.cisco.com** servidores no momento desta gravação). Também é altamente recomendável salvar a captura no formato pcap e verificá-la no Wireshark. Este é um exemplo de um registro bem-sucedido:

```
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 o arquivo pcap para um 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)#
```



Erro de Registro: Falha no 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
```

Etapas recomendadas

1. Verifique se a URL do call-home está correta. Você pode verificar isso na interface do usuário FXOS ou na CLI (**scope monitoring > show callhome detail expand**).
2. Habilite uma captura e verifique a comunicação TCP (HTTPS) entre o MIO e o **tools.cisco.com** conforme demonstrado na seção "Falha ao autenticar o servidor" deste documento.

Erro de registro: não foi possível conectar ao 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
```

Etapas recomendadas

1. Se uma configuração de proxy estiver habilitada, verifique se a URL e a porta do proxy estão configuradas corretamente.
2. Habilite uma captura e verifique a comunicação TCP (HTTPS) entre o MIO e o **tools.cisco.com** conforme demonstrado na seção "Falha ao autenticar o servidor" deste documento.

Erro de registro: o servidor HTTP retorna o código de erro >= 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
```

Etapas recomendadas

1. Se uma configuração de proxy estiver habilitada, entre em contato com o administrador do servidor proxy sobre as configurações de proxy.
2. Habilite uma captura e verifique a comunicação TCP (HTTPS) entre o MIO e o **tools.cisco.com**

conforme demonstrado na seção "Falha ao autenticar o servidor" deste documento. Tente se registrar novamente (opção "forçar") a partir da CLI do FXOS:

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

Erro de Registro: Falha ao Analisar Mensagem de Resposta de Back-end

```
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
```

Etapas recomendadas

1. Tentativas de repetição automática posteriormente. Use 'renew' para tentar novamente imediatamente.

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

2. Verifique se o URL do call-home está correto.

Problemas de licença no ASA - Série 1xxx/21xx

Erro de registro: Erro de envio de mensagem de comunicação

```
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
```

Etapas recomendadas

1. Verifique as configurações DNS

```
ciscoasa# show run dns
```

2. Tente fazer ping **tools.cisco.com**. Nesse caso, a interface de gerenciamento é usada:

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

3. Verifique a tabela de roteamento:

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

Certifique-se de que você tenha uma licença habilitada, por exemplo:

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

4. Habilite a captura na interface que roteia em direção ao **tools.cisco.com** (se você fizer a captura sem nenhum filtro IP, certifique-se de que o ASDM não esteja aberto quando você fizer a captura para evitar ruído de captura desnecessário).

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

> **Aviso**: a captura de pacotes pode ter um impacto adverso no desempenho.

5. Ative temporariamente o Syslog nível 7 (debug) e verifique as mensagens de Syslog do ASA durante o processo 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
```

Tente se registrar novamente:

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

Requisitos especiais para direitos adicionais

- Énecessário adquirir um direito de nível de recurso válido antes de configurar qualquer direito complementar
- Todos os direitos do complemento precisam ser liberados antes que você libere o direito da camada de recursos

Estado da Qualificação Durante a Operação de Reinicialização

- Os estados de qualificação são salvos na memória flash
- Durante o tempo de inicialização, essas informações são lidas da memória flash e as licenças são definidas com base no modo de imposição salvo
- A configuração de inicialização é aplicada com base nessas informações de qualificação em cache
- As qualificações são solicitadas novamente após cada reinicialização

Envolva o suporte do Cisco TAC

FP41xx/FP9300

Se todos os itens mencionados neste documento falharem, colete essas saídas da CLI do chassi e entre em contato com o TAC da Cisco:

Saída 1:

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

Saída 2:

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

Saída 3:

Pacote de suporte de chassi FXOS

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

Saída 4 (altamente recomendável):

Captura do Ethanalyzer a partir da CLI do chassi

FP1xxx/FP21xx

Saída 1:

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

Saída 2:

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

Perguntas frequentes (FAQs)

No FP21xx, onde está a guia Licensing (Licenciamento) na GUI do chassi (FCM)?
A partir da versão 9.13.x, o FP21xx oferece suporte a dois modos ASA:

- Dispositivo
- Platform

No modo Appliance, não há interface do usuário do chassi. No modo de plataforma, há uma interface do usuário do chassi, mas a licença é configurada a partir da CLI do ASA ou do ASDM. Por outro lado, nas plataformas FPR4100/9300, a licença deve ser configurada no FCM via GUI ou FXOS CLI e as qualificações do ASA devem ser solicitadas ao ASA CLI ou ASDM.
Referências:

- Gerenciamento de licenças para o ASA
- Dispositivos lógicos para o Firepower 4100/9300

- Licenças: Smart Software Licensing (ASAv, ASA no Firepower)
- Implantação do modo de plataforma ASA com ASDM e Firepower Chassis Manager

Como você pode habilitar uma Licença de Criptografia Forte?
Essa funcionalidade será habilitada automaticamente se o token usado no registro do FCM tiver a opção de permitir a funcionalidade de exportação controlada nos produtos registrados com esse token habilitado.

Como você pode habilitar uma Licença de Criptografia Forte se os Recursos Controlados por Exportação no nível do FCM e o Encryption-3DES-AES relacionado no nível do ASA estiverem desabilitados?
Se o token não tiver essa opção habilitada, cancele o registro do FCM e registre-o novamente com um token que tenha essa opção habilitada.

O que você pode fazer se a opção Permitir a funcionalidade de exportação controlada nos produtos registrados com este token não estiver disponível quando você gerar o token?
Entre em contato com sua equipe de contas da Cisco.

É obrigatório configurar o recurso Strong Encryption no nível do ASA?
A opção de criptografia forte de recurso é obrigatória apenas se o FCM estiver integrado a um servidor satélite anterior à versão 2.3.0. Esse é apenas um cenário em que você deve configurar esse recurso.

Quais IPs devem ser permitidos no caminho entre o FCM e a nuvem de Smart Licensing?
O FXOS usa o endereço https://tools.cisco.com/ (porta 443) para se comunicar com a nuvem de licenciamento. O endereço https://tools.cisco.com/ é resolvido para estes endereços IP:

- 72.163.4.38
- 173.37.145.8

Por que você recebe um erro de fora de conformidade?
O dispositivo pode ficar fora de conformidade nestas situações:

- Superutilização (o dispositivo usa licenças indisponíveis)
- Expiração da licença - Uma licença baseada em tempo expirou
- Falta de comunicação - O dispositivo não pode entrar em contato com a Autoridade de Licenciamento para obter uma nova autorização

Para verificar se sua conta está ou se aproxima de um estado de não conformidade, você deve comparar os direitos atualmente em uso pelo chassi do Firepower com os de sua Conta inteligente.
Em um estado fora de conformidade, você pode fazer alterações de configuração em recursos que exigem licenças especiais, mas a operação não será afetada. Por exemplo, acima do limite de licença Padrão, os contextos que já existem continuam a ser executados e você pode modificar a configuração deles, mas não é possível adicionar um novo contexto.

Por que você ainda recebe um erro de fora de conformidade após a adição de licenças?
Por padrão, o dispositivo se comunica com a autoridade de licença a cada 30 dias para verificar os direitos. Se quiser acioná-lo manualmente, siga estas etapas:

Para as plataformas FPR1000/2100, isso deve ser feito via ASDM ou via CLI:

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

Para plataformas FPR4100/9300, isso deve ser feito via CLI FXOS:

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

Por que não há Licença em Uso no nível ASA?

Verifique se a qualificação do ASA foi configurada no nível do ASA, por exemplo:

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

Por que as licenças ainda não estão em uso, mesmo após a configuração de uma qualificação para o ASA?

Esse status é esperado se você implantou um par de failover ativo/em espera do ASA e verificou o uso da licença no dispositivo em espera.
De acordo com o Guia de configuração, a configuração é replicada para a unidade de standby, mas a unidade de standby não usa a configuração; ela permanece em um estado de cache. Somente a unidade ativa solicita as licenças do servidor. As licenças são agregadas em uma única licença de failover que é compartilhada pelo par de failover, e essa licença agregada também é armazenada em cache na unidade de standby a ser usada se ela se tornar a unidade ativa no futuro. Para referência: Licenças de cluster de failover ou ASA.

O que você pode fazer se o FCM não tiver acesso à Internet?

Como alternativa, você pode implantar o Cisco Smart Software Manager On-Prem (anteriormente conhecido como Cisco Smart Software Manager Satellite). Este é um componente do Cisco Smart Licensing que funciona em conjunto com o Cisco Smart Software Manager. Ele oferece visibilidade e relatórios quase em tempo real das licenças da Cisco que você compra e consome. Ele também oferece às organizações sensíveis à segurança uma maneira de acessar um subconjunto da funcionalidade do Cisco SSM sem o uso de uma conexão direta com a Internet para gerenciar sua base de instalação.

Onde você pode encontrar mais informações sobre o Cisco Smart Software Manager On-Prem?

Essas informações podem ser encontradas no Guia de configuração do FXOS:

- Configurar um servidor satélite de licença inteligente para o chassi Firepower 4100/9300
- Configurar o registro do Firepower Chassis Manager em um Smart Software Manager no local

Informações Relacionadas

- Guia de configuração da CLI de operações gerais do Cisco ASA Series
- Gerenciamento de licenças para o ASA
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.