FXOS Firepower 设备上的 ASA 智能许可证故障排除

目录

简介

背景信息

- 智能许可架构
- 整体架构
  - 命名法
  - 智能代理状态
  - ASA授权

配置

- 故障转移（高可用性）
  - 案例分析：ASA HA许可证，适用于FP2100
  - ASA集群

验证与调试

- 机箱(MIO)验证命令的输出示例
- 验证命令的ASA示例输出
  - 成功注册
  - 过期的授权
- 机箱CLI的输出示例
  - 未注册
  - 注册正在进行中
  - 注册错误
  - 评估期

FXOS机箱(MIO)上的常见许可证问题

- 注册错误：无效令牌
  - 建议步骤
  - 注册错误：产品已注册
  - 建议步骤
  - 注册错误：超出限制的日期偏移
  - 建议步骤
  - 注册错误：无法解析主机
  - 建议步骤
  - 注册错误：无法验证服务器
  - 建议步骤
- CLI验证
  - 注册错误：HTTP传输失败
  - 建议步骤
  - 注册错误：无法连接到主机
  - 建议步骤
  - 注册错误：HTTP服务器返回错误代码>= 400
  - 建议步骤
  - 注册错误：分析后端响应消息失败
  - 建议步骤

- ASA - 1xxx/21xx系列的许可证问题
  - 注册错误：通信消息发送错误
  - 建议步骤
  - 附加权利的特殊要求
  - 重新启动操作期间的授权状态
- 联系Cisco TAC支持
  - FP41xx/FP9300
  - FP1xxx/FP21xx

常见问题(FAQ)

相关信息

简介

本文档介绍 Firepower 可扩展操作系统 (FXOS) 上的自适应安全设备 (ASA) 智能许可功能。

背景信息

当机箱上安装了ASA时，会使用Firepower可扩展操作系统(FXOS)上的智能许可。对于Firepower威胁防御(FTD)和Firepower管理中心(FMC)智能许可，请参阅如何使用FMC和FTD智能许可证注册和常见问题故障排除指南。

本文档主要介绍FXOS机箱能够直接访问互联网的场景。如果您的FXOS机箱无法访问互联网，则必须考虑卫星服务器或永久许可证预留(PLR)。 有关离线管理的详细信息，请查看FXOS配置指南。

智能许可架构

机箱组件的高级概述：

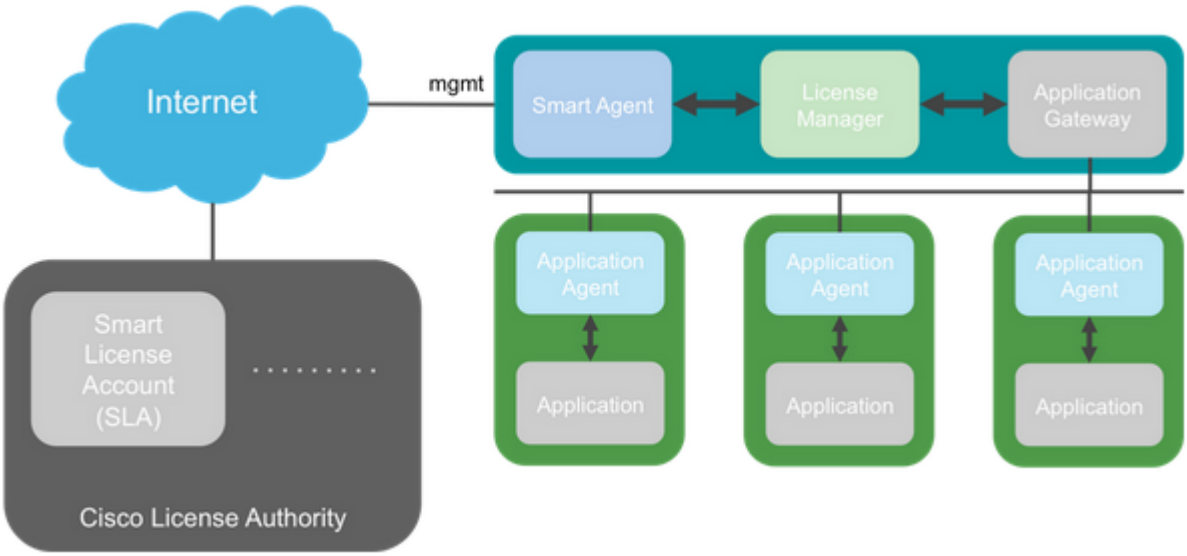


- 管理输入/输出(MIO)和单个模块都在智能许可中扮演角色。
- MIO不需要任何许可证即可运行。
- 每个模块上的SA应用必须获得许可

FXOS管理引擎是MIO。MIO包含三个主要组件：

- 智能代理
- 许可证管理器
- AppAG

整体架构



命名法

期限	描述
思科许可证颁发机构	用于智能许可的后端思科许可证。维护所有产品许可相关信息。这包括授权和设备信息。
智能许可证帐户	具有设备的所有授权的帐户。
令牌ID	用于在设备注册时区分智能许可证帐户的标识符。
授权	相当于许可证。对应于单个功能或整个功能层。
产品激活密钥(PAK)	与单个设备绑定的旧许可机制。

智能代理状态

状态	描述
未配置	未启用智能许可。
未识别	智能许可已启用，但智能代理尚未联系思科进行注册。
Registered	代理已联系思科许可机构并已注册。
已授权	当座席收到不合规状态以响应授权授权授权请求时。
不合规(OOC)	当代理收到OOC状态以响应授权授权请求时。
授权已过期	如果座席在90天内未与思科通信。

ASA授权

以下是受支持的ASA授权：

- 标准层
- 多情景
- 强加密(3DES)
- 移动/服务提供商(GTP)

配置

请使用以下文档中的说明：

- 智能软件许可（ASAv、Firepower上的ASA）
- ASA许可证管理

在任何功能层配置之前：

<#root>

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    *



*                                                                        *



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

配置标准层：

<#root>

```
asa(config)#
```

license smart

INFO: License(s) corresponding to an entitlement will be activated only after an entitlement request ha
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

故障转移（高可用性）

如《ASA配置指南》所述，每个Firepower设备都必须向许可证颁发机构或卫星服务器注册。

从ASA CLI验证：

```
<#root>
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-b3f7fb1cac
        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
```

备用设备：

<#root>

```
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

案例分析：ASA HA许可证，适用于FP2100

- 在2100上，ASA通过ASA接口（而不是FXOS管理）与思科智能许可门户（云）通信。
- 您必须将两个ASA注册到思科智能许可门户（云）。

在这种情况下，HTTP本地身份验证用于外部接口：

<#root>

```
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
```

如果启用3DES/AES许可证，则只能通过ASDM连接到ASA。对于尚未注册的ASA，这只能在已注册的接口上实management-only现。根据配置指南，“在连接到许可证颁发机构或卫星服务器之前，管理连接可以使用强加密(3DES/AES)，因此您可以启动ASDM。请注意，ASDM访问仅在使用默认加密的仅管理接口上可用。在连接并获取强加密许可证之前，不允许直通流量。”

在其他情况下，您会收到：

<#root>

```
ciscoasa(config)#

 debug ssl 255


debug ssl enabled at level 255.
```

error:1408A0C1:SSL routines:ssl3_get_client_hello:

no shared cipher

为了克服ASA的压力，在面向互联网的接口上配置了仅管理功能，因此可以进行ASDM连接：

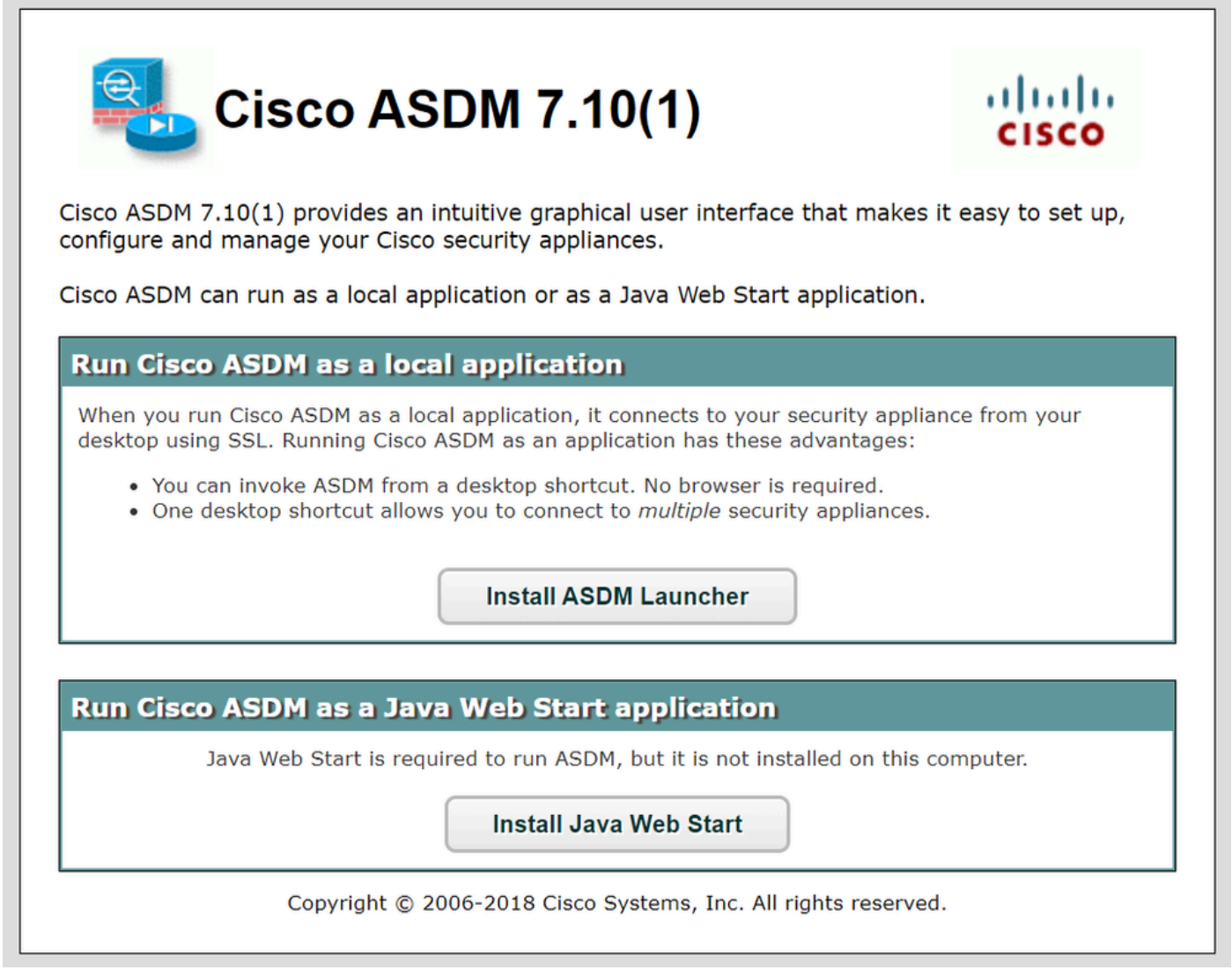
<#root>

interface Ethernet1/2

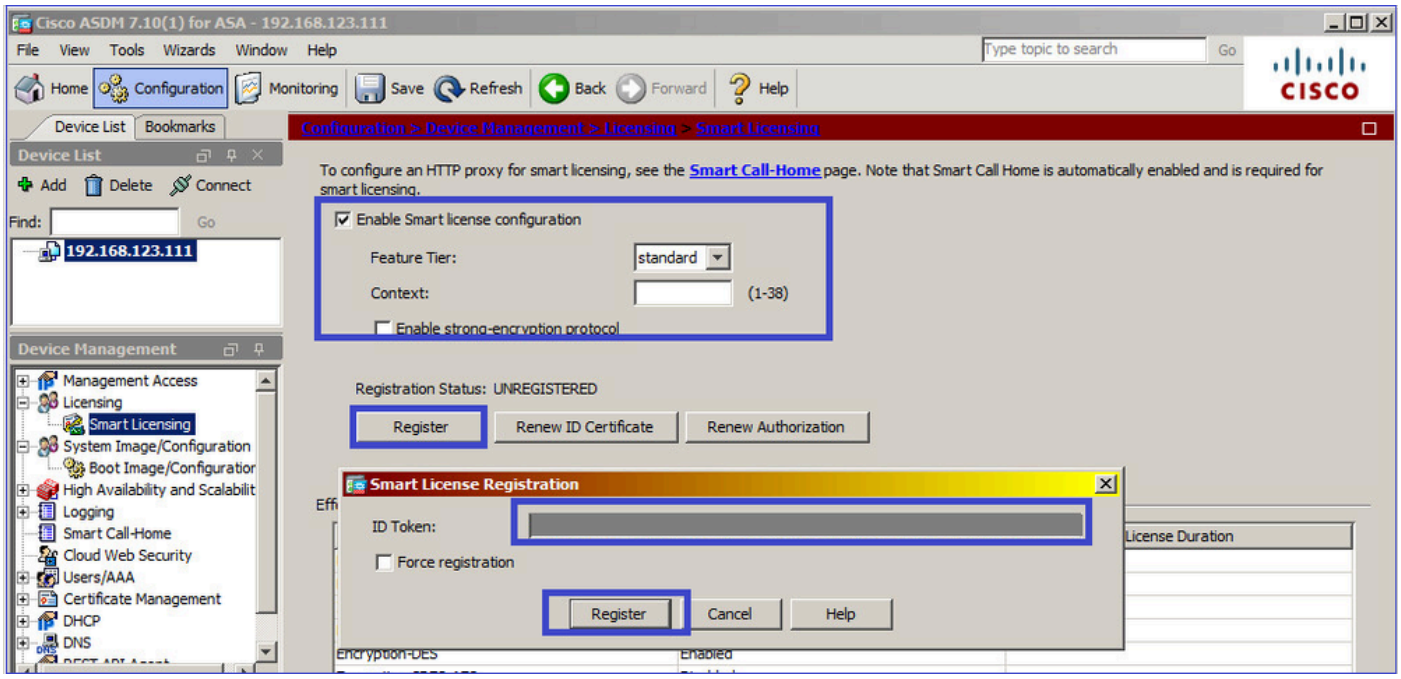
management-only

nameif outside
security-level 100

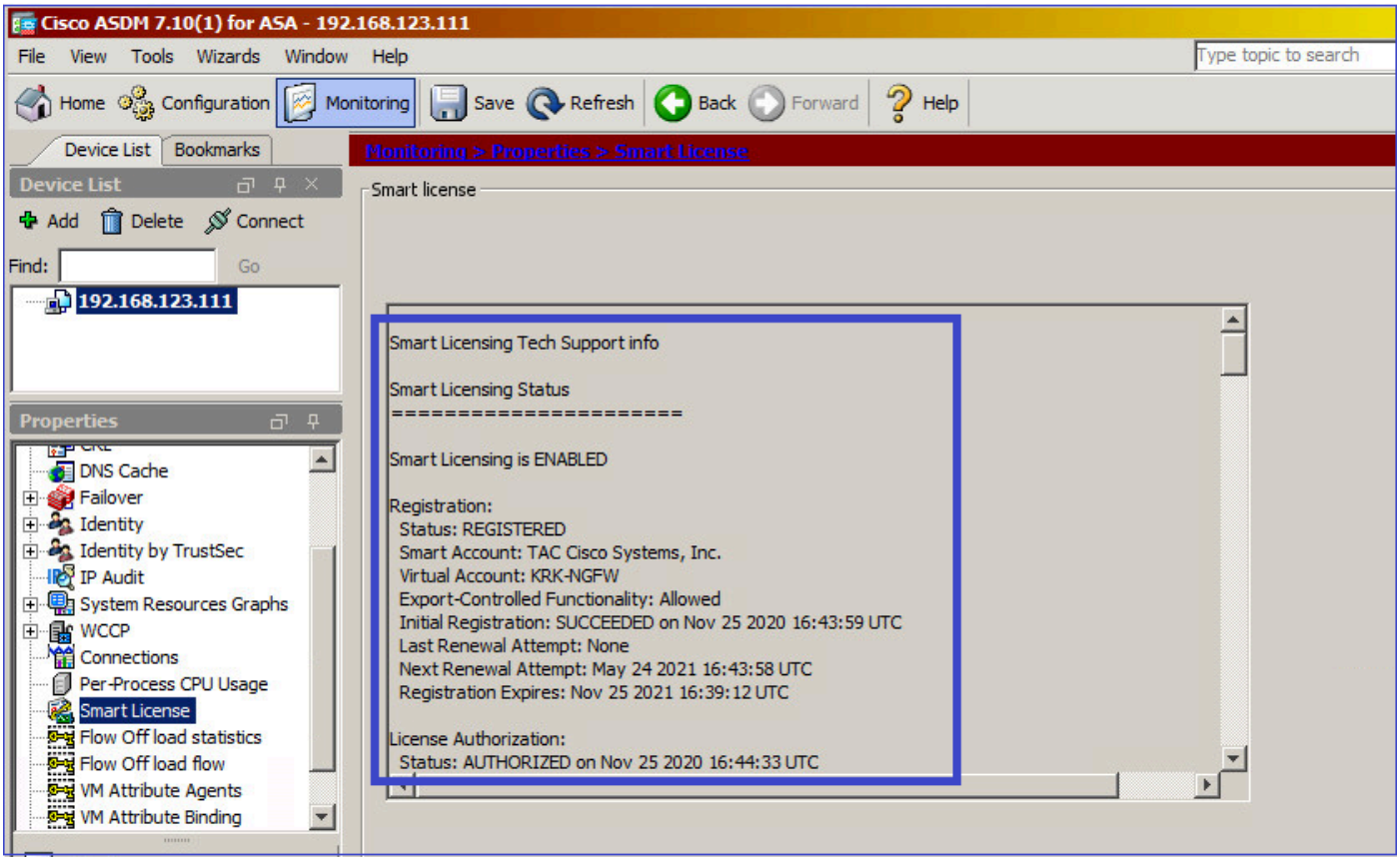
ip address 192.168.123.111 255.255.255.0 standby 192.168.123.112



在主ASA上配置智能许可：



导航到监控>属性>智能许可证以检查注册状态：



主ASA CLI验证：

<#root>

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
```

<#root>

ciscoasa/pri/act#

show license features

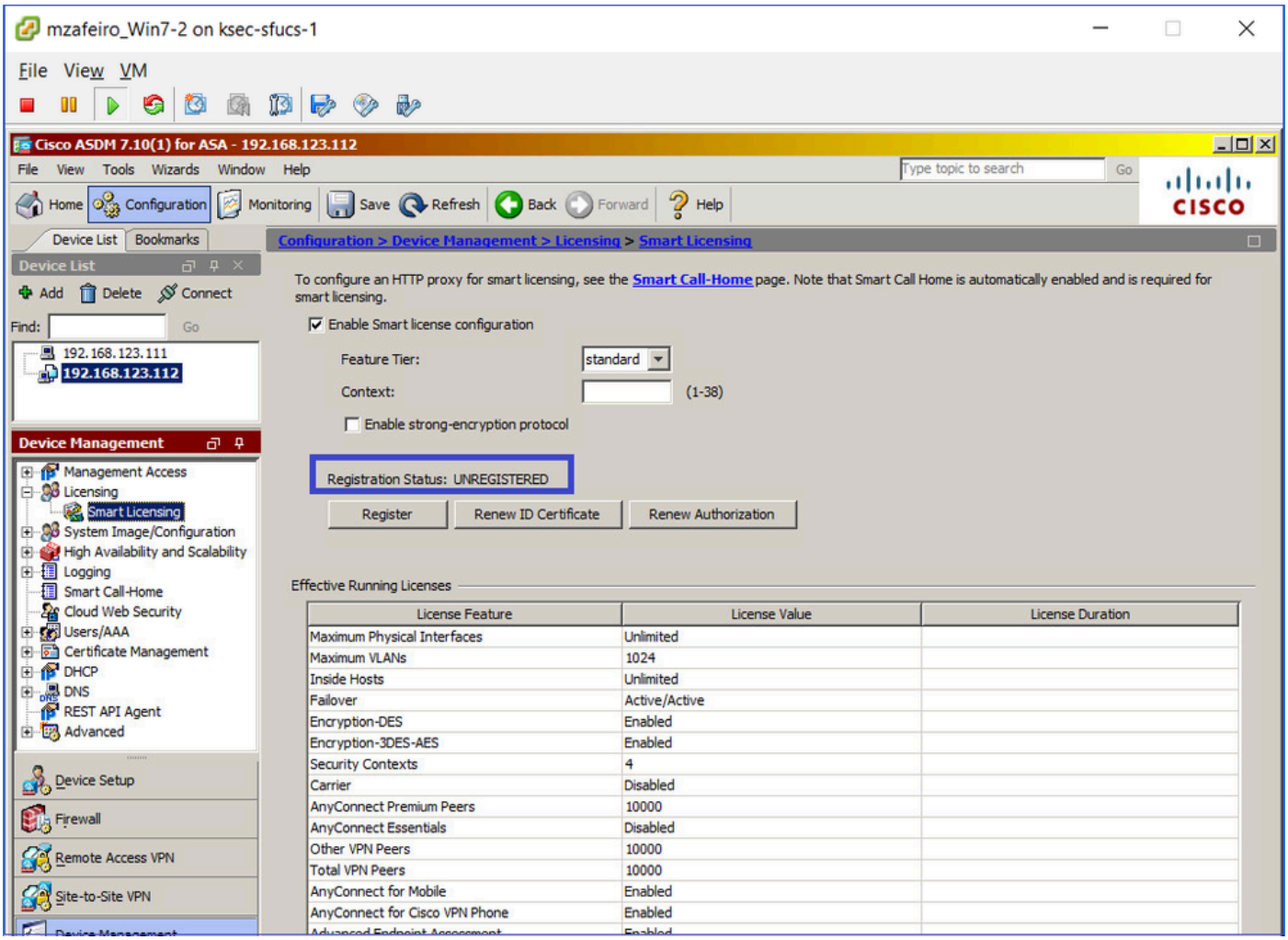
```
Serial Number: JAD12345ABC
Export Compliant: YES

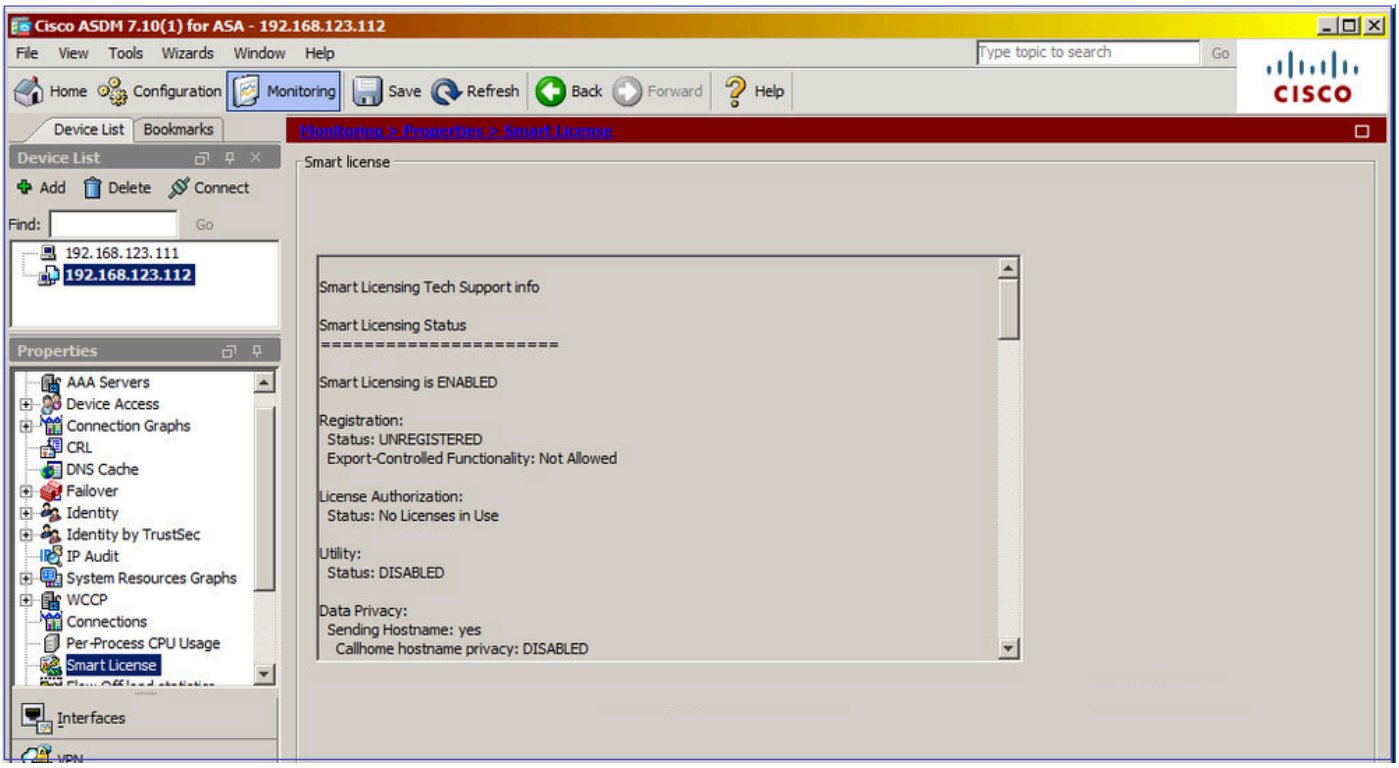
License mode: Smart Licensing

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
```

通过ASDM连接到备用ASA（仅当已为ASA配置了备用IP时才可能如此）。 备用ASA显示为 ，UNREGISTERED 这是预期情况，因为它尚未注册到智能许可门户：





备用ASA CLI显示：

<#root>

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
```

在备用ASA上启用的许可证功能：

<#root>

```
ciscoasa/sec/stby#
```

show license features

```
Serial Number: JAD123456A
Export Compliant: NO

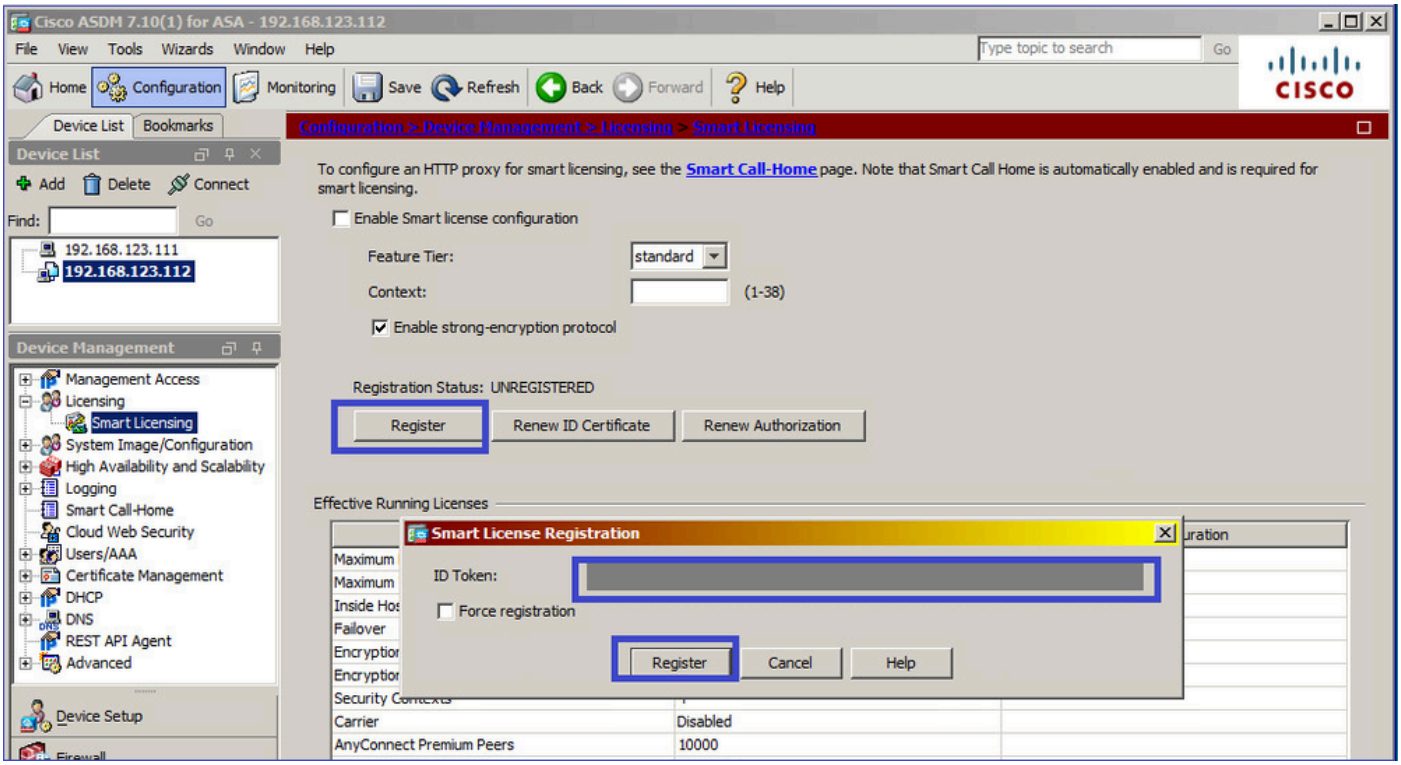
License mode: Smart Licensing

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
```

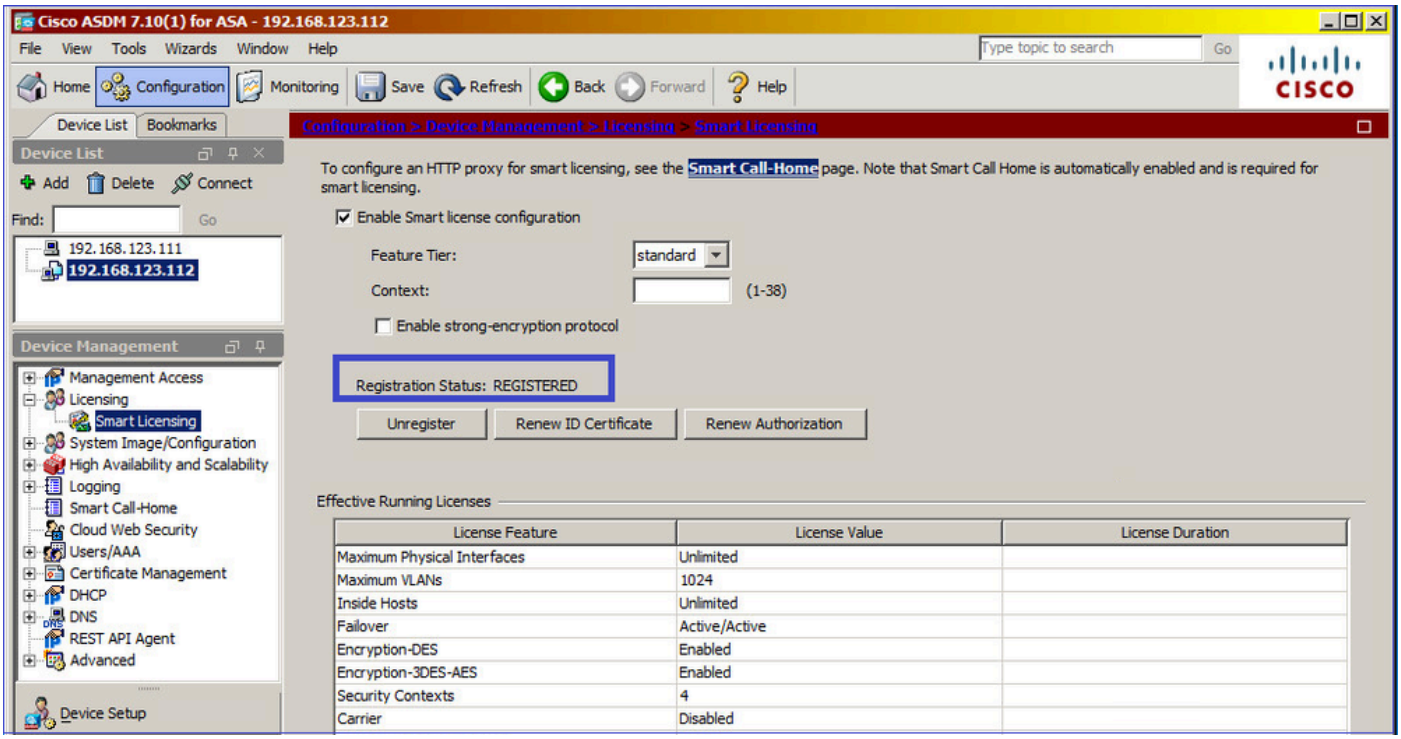
```
Total TLS Proxy Sessions : 10000
Cluster : Disabled


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
```

注册备用ASA:



备用ASA的结果是REGISTERED:



备用ASA上的CLI验证：

<#root>

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
```

ASA集群

如果设备许可证不匹配，则不会形成集群：

<#root>

```
Cluster unit unit-1-1 transitioned from DISABLED to CONTROL
New cluster member unit-2-1

rejected due to encryption license mismatch
```

成功的集群设置：

<#root>

```
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.
```

群集控制节点：

<#root>

```
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-b3f7fb1cac
        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
```

群集数据单元：

<#root>

```
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-ee0438d3
        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
```

验证与调试

机箱(MIO)验证命令摘要：

<#root>

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
```

配置验证：

<#root>

```
FPR4125-1#
scope system

FPR4125-1 /system #
scope services

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

ASA验证命令摘要：

<#root>

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

机箱(MIO)验证命令的输出示例

<#root>

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
```

<#root>

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

<#root>

```
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
```

<#root>

```
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
```

<#root>

```
FPR4125-1#
```

show clock

```
Tue Aug  4 09:55:50 UTC 2020
FPR4125-1#
```

```
show timezone

Timezone:

<#root>
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:+H
    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
    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
```

<#root>

```
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
```

验证命令的ASA示例输出

<#root>

```
asa#

show run license


license smart
 feature tier standard
```

<#root>

```
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-b3f7fb1cac
        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
```

<#root>

```
asa#
```

show license entitlement

```
Entitlement(s):

Feature tier:
        Tag: regid.2015-10.com.cisco.FIREPOWER_4100_ASA_STANDARD,1.0_7d7f5ee2-1398-4b0e-aced-b3f7fb1cac
        Version: 1.0
        Enforcement mode: Authorized
        Handle: 1
        Requested time: Tue, 04 Aug 2020 07:58:13 UTC
        Requested count: 1
        Request status: Complete
```

<#root>

```
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
```

<#root>

```
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-b3f7fb1cac
        Version: 1.0
        Enforcement mode: Authorized
        Handle: 1
        Requested time: Tue, 04 Aug 2020 07:58:13 UTC
        Requested count: 1
        Request status: Complete
```

成功注册

输出来自机箱管理器用户界面(UI):

<#root>

```
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
```

过期的授权

输出来自机箱管理器UI:

<#root>

```
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
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 ZDA2MjFlODktYjllMSOONjQwLTkOMmUtYmVkYWU2NzIyZjYwLTE1ODIxODY2%OAMzEwODV8K2RWV
Error : Smart Agent already registered

Cisco Success Network: DISABLED
```

机箱CLI的输出示例

未注册

<#root>

```
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-C93OO-SUP-K9,SN:JAD12345678

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

注册正在进行中

<#root>

```
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-C93OO-SUP-K9,SN:JAD12345678

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

注册错误

<#root>

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-C93OO-SUP-K9,SN:JAD12345678

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

评估期

<#root>

```
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-C93OO-SUP-K9,SN:JAD12345678

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

FXOS机箱(MIO)上的常见许可证问题

注册错误：无效令牌

<#root>

```
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

."]}

建议步骤

1. 检查call-home URL是否指向思科许可证中心。
2. 登录到思科许可证中心，并检查令牌是否是从那里生成的，或令牌是否已过期。

注册错误：产品已注册

<#root>

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

."]}

建议步骤

1. 登录思科许可证中心。
2. 检查所有虚拟帐户中的产品实例选项卡。
3. 通过SN找到旧的注册实例并将其删除。
4. 此问题可能是由以下原因引起的：
    a. 在时间/日期设置不正确时（例如，未配置NTP服务器）无法自动更新。
    b. 在卫星和生产服务器之间切换时的操作顺序错误。例如，先更改URL，然后发出deregister命令。

注册错误：超出限制的日期偏移

<#root>

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

."]}

建议步骤

检查时间/日期配置，确保配置了NTP服务器。

注册错误：无法解析主机

<#root>

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

建议步骤

1. 检查callhome SLDest URL是否正确(scope monitoring > scope callhome > show expand)。
2. 例如，从CLI检查MIO DNS服务器配置是否正确：

<#root>

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.尝试从机箱CLI ping tools.cisco.com并查看其是否解决：

<#root>

```
FPR4125-1#

connect local-mgmt


FPR4125-1(local-mgmt)#

ping tools.cisco.com
```

4.尝试从机箱CLI ping DNS服务器：

<#root>

```
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.启用机箱(MIO)管理接口上的捕获（仅适用于FP41xx/FP93xx），并在对tools.cisco.com运行ping测试时检查DNS通信:

<#root>

```
FPR4125-1#

connect fxos


FPR4125-1(fxos)#

ethanalyzer local interface mgmt capture-filter "udp port 53" limit-captured-frames 0 limit-frame-size 1


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
    2 2020-08-07 08:10:47.255015331 10.62.148.225 → 172.31.200.100 DNS 75 Standard query 0x26b4 A tools.cisco
    3 2020-08-07 08:10:49.257160749 10.62.148.225 → 172.31.200.100 DNS 75 Standard query 0x5019 A tools.cisco
    4 2020-08-07 08:10:51.259222753 10.62.148.225 → 172.31.200.100 DNS 75 Standard query 0x5019 A tools.cisco
```

注册错误：无法验证服务器

<#root>

```
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
```

建议步骤

1.检查MIO信任点CHdefault是否具有正确的证书，例如：

<#root>

```
FPR4125-1#

scope security


FPR4125-1 /security #

show trustpoint

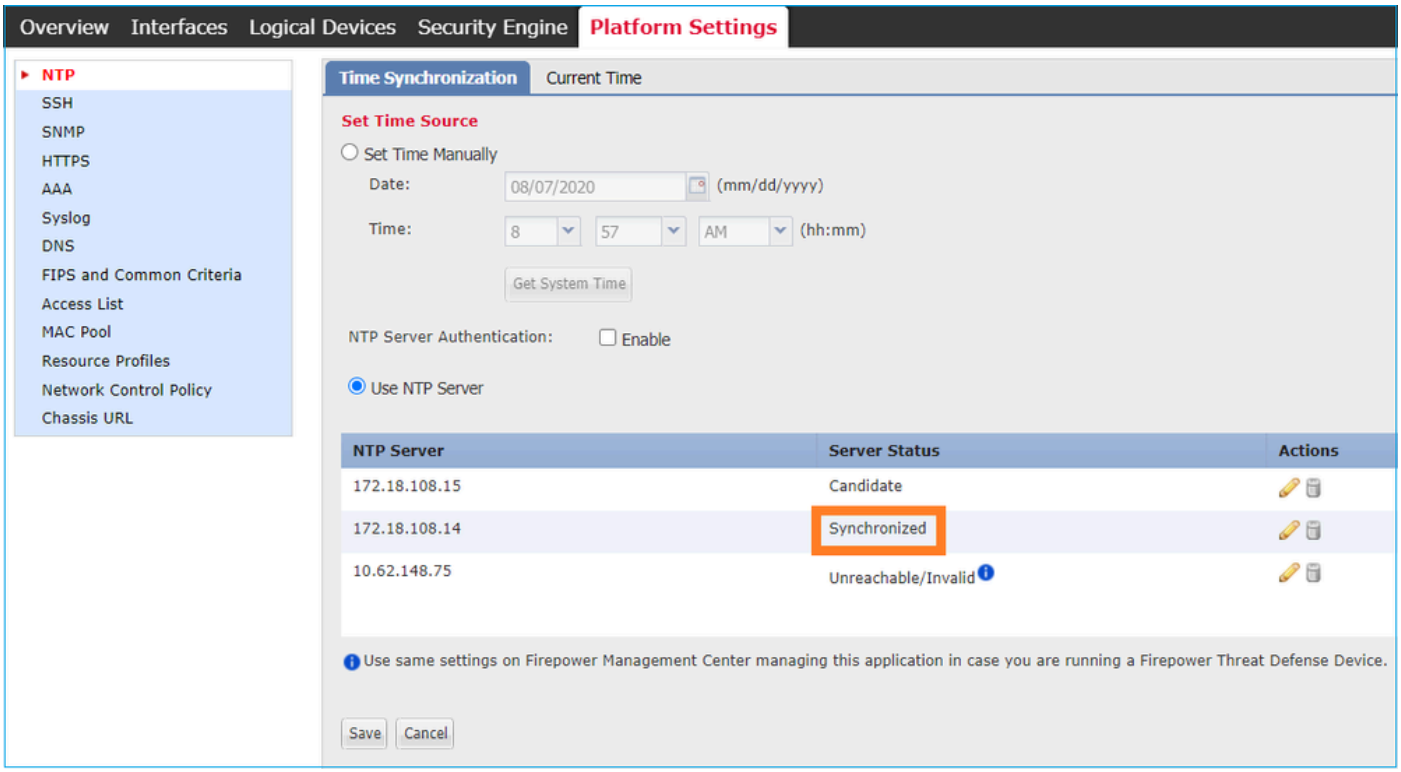


Trustpoint Name: CHdefault


Trustpoint certificate chain: -----BEGIN CERTIFICATE-----
MIIFtzCCA5+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwRTELMAkGA1UEBhMCQk0x
...
8eOx79+Rj1QqCyXBJhnEUhAFZdWCEOrCMc0u
-----END CERTIFICATE-----

Cert Status: Valid
```

2.检查NTP服务器和时区是否设置正确。服务器和客户端之间的证书验证时间必须相同。为此，请使用NTP同步时间。例如，FXOS UI验证：



CLI验证

<#root>

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
```

启用捕获并检查MIO和tools.cisco.com之间的TCP通信(HTTPS)。您有以下几种选择：

- 您可以关闭到FXOS UI的HTTPS会话，并在CLI上为HTTPS设置捕获过滤器，例如：

<#root>

```
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
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=82
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=10
```

- 此外，如果要保持FXOS UI打开，可以在捕获中指定目标IP（在撰写本文时，72.163.4.38和173.37.145.8是tools.cisco.com服务器）。 强烈建议以pcap格式保存捕获并在Wireshark中检查这些捕获。以下是成功注册的示例：

```
<#root>

FPR4125-1(fxos)#

ethanalyzer local interface mgmt capture-filter "tcp port 443 and (host 72.163.4.38 or host 173.37.145.8

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 W
```

- 将pcap文件导出到远程FTP服务器的步骤：

```
<#root>

FPR4125-1#

connect local-mgmt

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

dir

```
1 56936 Aug 07 08:39:35 2020

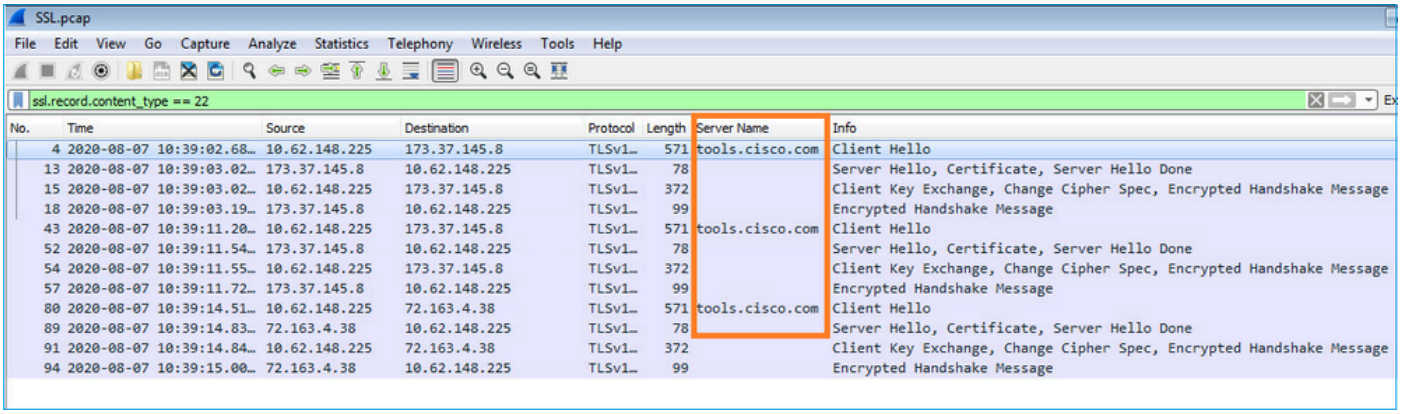
SSL.pcap

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)#
```



注册错误：HTTP传输失败

```
<#root>

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
```

建议步骤

1. 检查call-home URL是否正确。您可以从FXOS UI或CLI（范围监控>show callhome detail expand）检查此项。
2. 启用捕获并检查MIO和tools.cisco.com之间的TCP通信(HTTPS)，如本文档的“无法验证服务器”部分所示。

注册错误：无法连接到主机

<#root>

```
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: Could Not connect to host
```

建议步骤

1. 如果启用代理配置，请确保代理URL和端口配置正确。
2. 启用捕获并检查MIO和tools.cisco.com之间的TCP通信(HTTPS)，如本文档的“无法验证服务器”部分所示。

注册错误：HTTP服务器返回错误代码>= 400

<#root>

```
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 configuratio
```

建议步骤

1. 如果启用代理配置，请联系代理服务器管理员了解代理设置。
2. 启用捕获并检查MIO和tools.cisco.com之间的TCP通信(HTTPS)，如本文档的“无法验证服务器”部分所示。尝试从FXOS CLI重新注册（强制选项）：

```
<#root>

FPR4125-1 /license #

register idtoken ODNmNTExMTAtY2YzOS00Mzc1LWEzNWMtYmNiMmUyNzM4ZmFjLTE1OTkxMTkz%0ANDk0NjR8NkJJdWZpQzRDbmtF
```

注册错误：分析后端响应消息失败

```
<#root>

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
```

建议步骤

1.稍后自动重试尝试。使用续订立即重试。

<#root>

FPR4125-1#

scope license

FPR4125-1 /license #

scope licdebug

FPR4125-1 /license/licdebug #

renew

2.检查call-home URL是否正确。

ASA - 1xxx/21xx系列的许可证问题

注册错误：通信消息发送错误

<#root>

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
```

建议步骤

1.检查DNS设置：

<#root>

ciscoasa#

show run dns

2.尝试ping tools.cisco.com。在本例中，使用管理接口：

<#root>

ciscoasa#

ping management tools.cisco.com

```
                ^
ERROR: % Invalid Hostname
```

3.检查路由表：

<#root>

ciscoasa#

show route management-only

确保已启用许可证，例如：

<#root>

```
ciscoasa#

show run license


license smart
 feature tier standard
 feature strong-encryption
```

4.在路由到tools.cisco.com的接口上启用捕获（如果在不使用任何IP过滤器的情况下捕获数据，请确保在进行捕获时没有打开ASDM，以避免不必要的捕获噪音）。

<#root>

```
ciscoasa#

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



警告：数据包捕获可能会对性能产生负面影响。

5.在注册过程中临时启用系统日志级别7（调试）并检查ASA系统日志消息：

<#root>

```
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: 3000683B0F7504F7B

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.

尝试重新注册：

<#root>

ciscoasa #

license smart register idtoken

force

附加权利的特殊要求

- 在配置任何附加授权之前，必须获取有效的功能层授权。
- 在释放功能层授权之前，必须释放所有附加授权。

重新启动操作期间的授权状态

- 权限状态保存在闪存中。
- 在启动期间，将从闪存中读取此信息，并根据保存的实施模式设置许可证。
- 启动配置将基于此缓存的授权信息应用。
- 每次重新启动后都会再次请求授权。

联系Cisco TAC支持

FP41xx/FP9300

如果本文档中提到的所有项目均失败，请从机箱CLI收集这些输出并联系思科TAC:

输出1:

```
<#root>

FPR4125-1#

show license techsupport
```

输出2:

```
<#root>

FPR4125-1#
```

```
scope monitoring

FPR4125-1 /monitoring #

scope callhome

FPR4125-1 /monitoring/callhome #

show detail expand
```

输出3. FXOS机箱支持套件：

```
<#root>

FPR4125-1#

connect local-mgmt

FPR4125-1(local-mgmt)#

show tech-support chassis 1 detail
```

输出4（强烈建议）。 从机箱CLI捕获Ethanalyzer:

FP1xxx/FP21xx

输出1:

```
<#root>

ciscoasa#

 show tech-support license
```

输出2:

```
<#root>

ciscoasa#

connect fxos admin


firepower-2140#

connect local-mgmt


firepower-2140(local-mgmt)#

show tech-support fprm detail
```

常见问题(FAQ)

问:在FP21xx上，机箱(FCM)GUI上的Licensing选项卡位于何处？
答：从9.13.x开始，FP21xx支持2个ASA模式：

- 设备
- Platform

在设备模式下，没有机箱UI。

在平台模式下，有一个机箱UI，但从ASA CLI或ASDM配置许可证。
另一方面，在FPR4100/9300平台上，必须在FCM中通过GUI或FXOS CLI配置许可证，并且必须从ASA CLI或ASDM请求ASA授权。
参考资料:

- ASA许可证管理
- Firepower 4100/9300的逻辑设备
- 许可证：智能软件许可（ASAv、Firepower上的ASA）
- 使用ASDM和Firepower机箱管理器的ASA平台模式部署

问:如何启用强加密许可证？
答：如果在FCM注册中使用的令牌具有在启用该令牌的情况下注册的产品上允许导出控制功能的选

项，则此功能将自动启用。

问:如果在FCM级别上的导出控制功能和ASA级别上的相关Encryption-3DES-AES被禁用，如何启用强加密许可证？
A：如果令牌未启用此选项，请取消注册FCM并使用启用此选项的令牌再次注册它。

问:如果在生成令牌时，使用此令牌注册的产品上的允许导出控制功能的选项不可用，您会怎么做？
答：联系您的思科客户团队。

问:是否必须在ASA级别配置强加密功能？
答：仅当FCM与2.3.0之前的卫星服务器集成时，功能强加密选项才是必需的。这只是必须配置此功能的一个场景。

问:在FCM和智能许可云之间的路径中必须允许哪些IP?
答：FXOS使用地址https://tools.cisco.com/（端口443）与许可云通信。地址https://tools.cisco.com/被解析为以下IP地址：

- 72.163.4.38
- 173.37.145.8

问:为什么会出现“Out of Compliance”错误？
答：在以下情况下，设备可能会不合规：

- 过度使用（设备使用不可用的许可证）。
- 许可证到期：基于时间的许可证已过期。
- 缺乏沟通： 设备无法联系授权机构进行重新授权。

要验证您的帐户是否处于或接近不合规状态，必须将Firepower机箱当前使用的授权与智能帐户中的授权进行比较。在不合规状态下，可以对需要特殊许可证的功能进行配置更改，但操作不会受到影响。例如，超过标准许可证限制后，已经存在的情景会继续运行，您可以修改其配置，但不能添加新情景。

问:为什么添加许可证后仍然出现“Out of Compliance（合规性）”错误？
答：默认情况下，设备每30天与许可证颁发机构进行通信以检查授权。如果要手动触发它，必须使用以下步骤：

对于FPR1000/2100平台，必须通过ASDM或CLI完成：

```
<#root>

ASA#

license smart renew auth
```

对于FPR4100/9300平台，必须通过FXOS CLI完成：

```
<#root>

FP4100#

scope system


FP4100 /system #

scope license


FP4100 /license #

scope licdebug


FP4100 /license/licdebug #

renew
```

问:为什么没有在ASA级别使用许可证？
A：确保在ASA级别上配置了ASA授权，例如：

```
<#root>

ASA(config)#
```

```
license smart


ASA(config-smart-lic)#

feature tier standard
```

问:为什么即使在配置ASA授权之后，许可证仍然未使用？
答：如果部署了ASA主用/备用故障转移对并检查了备用设备上的许可证使用情况，则此状态为预期状态。根据配置指南，配置会复制到备用设备，但备用设备不使用配置；它保持缓存状态。只有主用设备会向服务器请求许可证。许可证会汇聚到由故障转移对共享的单个故障转移许可证中，并且此汇聚许可证也缓存在备用设备上，以便将来成为主用设备时使用。仅供参考：故障切换或ASA集群许可证。

问:如果FCM无法访问Internet，您可以做什么？
答：作为替代方案，您可以部署内部思科许可证中心（以前称为卫星）。 这是思科智能许可的一个组件，与思科许可证中心配合使用。它为您购买和使用的思科许可证提供接近实时的可视性和报告功能。它还为安全敏感型组织提供了一种访问思科许可证中心功能子集的方法，而无需使用直接互联网连接来管理其客户群。

问:在哪里可以找到有关思科内部许可证中心的更多信息？
答：您可以在《FXOS配置指南》中找到以下信息：

- 为Firepower 4100/9300机箱配置智能许可证卫星服务器
- 将Firepower机箱管理器注册配置为本地思科许可中心许可证

相关信息

- Cisco ASA系列常规操作CLI配置指南
- ASA许可证管理
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。