排除FXOS Firepower裝置上的ASA智慧許可證故障

目錄

簡介
背景資訊
智慧許可架構
整體架構
命名法
智慧代理狀態
ASA權利
組態
故障轉移（高可用性）
案例研究：FP2100上的ASA HA許可證
ASA集群
驗證與偵錯
機箱(MIO)驗證命令的輸出示例
驗證命令的ASA輸出示例
成功註冊
過期的授權
機箱CLI的輸出示例
未註冊
正在註冊
註冊錯誤
評估期
FXOS機箱(MIO)上的常見許可證問題
註冊錯誤：無效令牌
建議步驟
註冊錯誤：產品已註冊
建議步驟
註冊錯誤：日期偏移量超出限制
建議步驟
註冊錯誤：無法解析主機
建議步驟
註冊錯誤：無法驗證伺服器
建議步驟
CLI 驗證
註冊錯誤： HTTP傳輸失敗
建議步驟
註冊錯誤：無法連線到主機
建議步驟
註冊錯誤： HTTP伺服器返回錯誤代碼>= 400

[建議步驟](#)
[註冊錯誤：分析後端響應消息失敗](#)
[建議步驟](#)
[ASA上的許可證問題 — 1xxx/21xx系列](#)
[註冊錯誤：通訊消息傳送錯誤](#)
[建議步驟](#)
[附加權利的特殊要求](#)
[重新啟動操作期間的權利狀態](#)
[聯絡Cisco TAC支援](#)
[FP41xx/FP9300](#)
[FP1xxx/FP21xx](#)
[常見問題(FAQ)](#)
[相關資訊](#)

簡介

本檔案介紹Firepower可擴展作業系統(FXOS)上的自適應安全裝置(ASA)智慧許可功能。

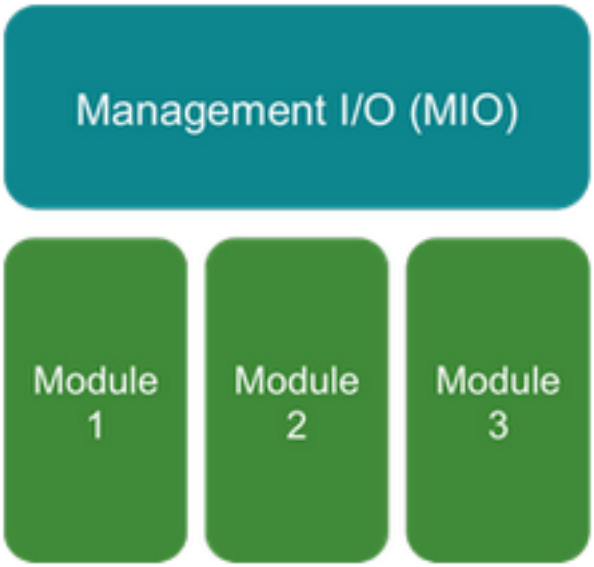
背景資訊

當機箱上安裝了ASA時，會使用FXOS上的智慧許可。對於Firepower威脅防禦(FTD)和Firepower管理中心(FMC)，智慧許可檢查[FMC和FTD智慧許可證註冊和故障排除。](#)

本檔案主要介紹FXOS機箱可以直接存取網際網路的案例。如果您的FXOS機箱無法訪問網際網路，則需要考慮衛星伺服器或永久許可證保留(PLR)。有關離線管理的詳細資訊，請檢視FXOS[配置指南。](#)

智慧許可架構

機箱元件的簡要概述：

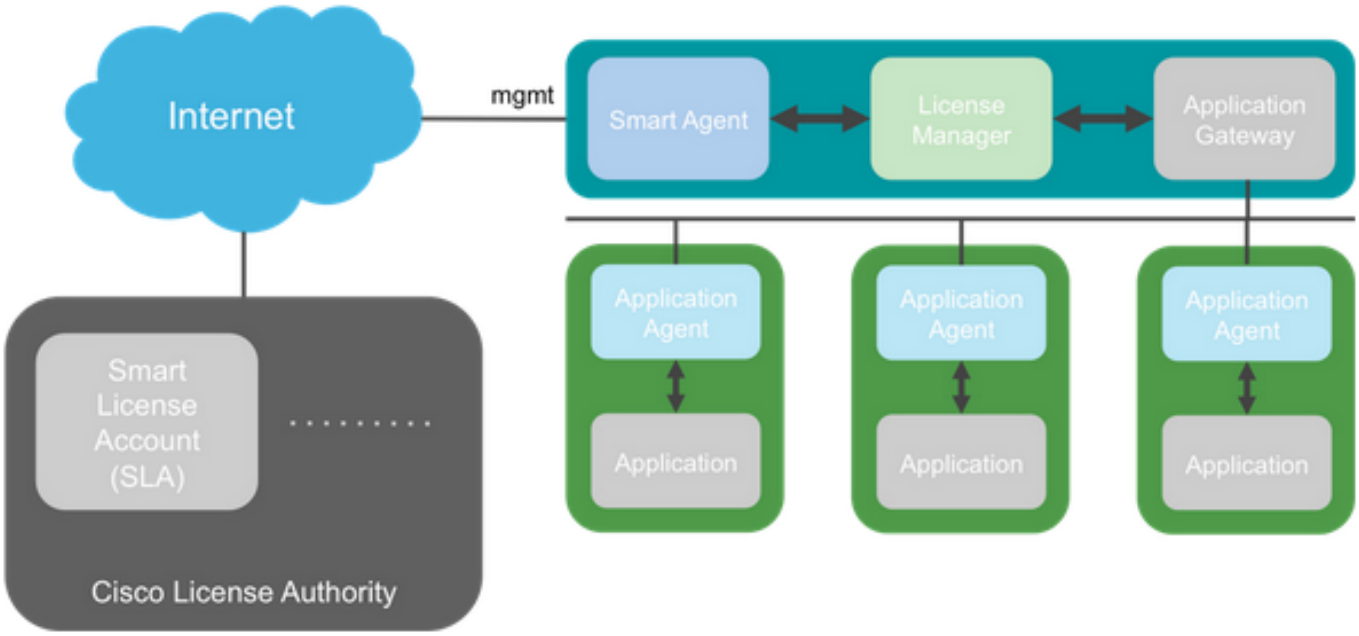


- 管理輸入/輸出(MIO)和單個模組都在智慧許可中扮演著角色
- MIO本身運行不需要任何許可證
- 每個模組上的SA應用程式都需要獲得許可

FXOS管理引擎是MIO。MIO包含三個主要元件：

- 智慧代理
- 許可證管理器
- AppAG

整體架構



命名法

字詞	說明
思科授權單位	思科智慧許可許可證後端。維護所有產品許可相關資訊。其中包括授權和裝置資訊。
智慧許可證帳戶	具有裝置的所有權利的帳戶。
令牌ID	註冊裝置時，識別符號用於區分智慧許可證帳戶。
權利	相當於許可證。對應於單個功能或整個功能層。
產品啟用金鑰(PAK)	較舊的許可機制。連線到單個裝置。

智慧代理狀態

狀態	說明
未配置	未啟用智慧許可。
未識別	已啟用智慧許可，但智慧代理尚未聯絡思科進行註冊。
已註冊	代理已聯絡思科許可頒發機構並已註冊。
已獲授權的	當代理收到不合規狀態以響應授權授權請求時。
不合規(OOC)	當代理收到OOC狀態以響應授權請求時。
授權已過期	如果座席在90天內未與思科通訊。

ASA權利

以下是受支援的ASA權利：

- 標準層
- 多情景
- 強加密(3DES)
- 行動/服務供應商(GTP)

組態

請遵循以下文檔中的說明：

- 智慧軟體許可（ASAv、Firepower上的ASA）
- 適用於ASA的許可證管理

在任何功能層配置之前：

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

配置標準層：

```
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
```

故障轉移（高可用性）

如ASA配置指南所述，每個Firepower裝置都必須向許可證頒發機構或衛星伺服器註冊。從ASA

CLI驗證：

```
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
```

備用裝置：

```
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
```

案例研究：FP2100上的ASA HA許可證

- 在2100上，ASA通過ASA介面（而不是FXOS管理）與思科智慧許可門戶（雲）通訊
- 您需要將兩個ASA註冊到思科智慧許可門戶（雲）

在這種情況下，HTTP本地身份驗證用於外部介面：

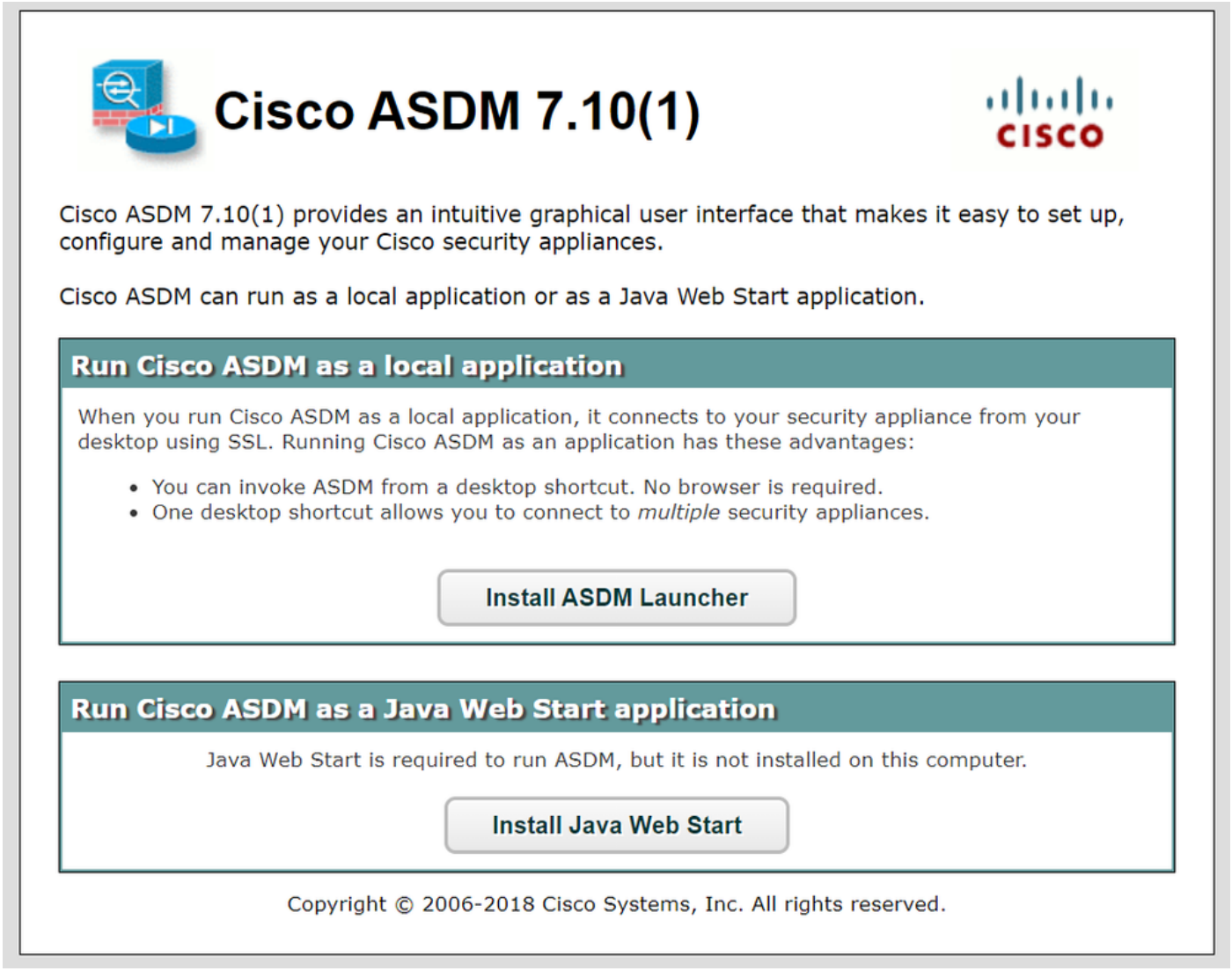
```
ciscoasa(config)# show run http
http server enable
http 0.0.0.0 0.0.0.0 outside
ciscoasa(config)# show run aaa
aaa authentication http console LOCAL
ciscoasa(config)# show run username
username cisco password ***** pbkdf2
```

如果啟用3DES/AES許可證，則只能通過ASDM連線到ASA。對於尚未註冊的ASA，這只能在已註冊的 management-only.根據配置指南：「在連線到許可證頒發機構或衛星伺服器之前，管理連線可以使用強加密(3DES/AES)，這樣您就可以啟動ASDM。請注意，ASDM訪問僅在具有預設加密的僅管理介面上可用。在連線並獲得強加密許可證之前，不允許通過機箱流量。」在其他情況下，您會得到：

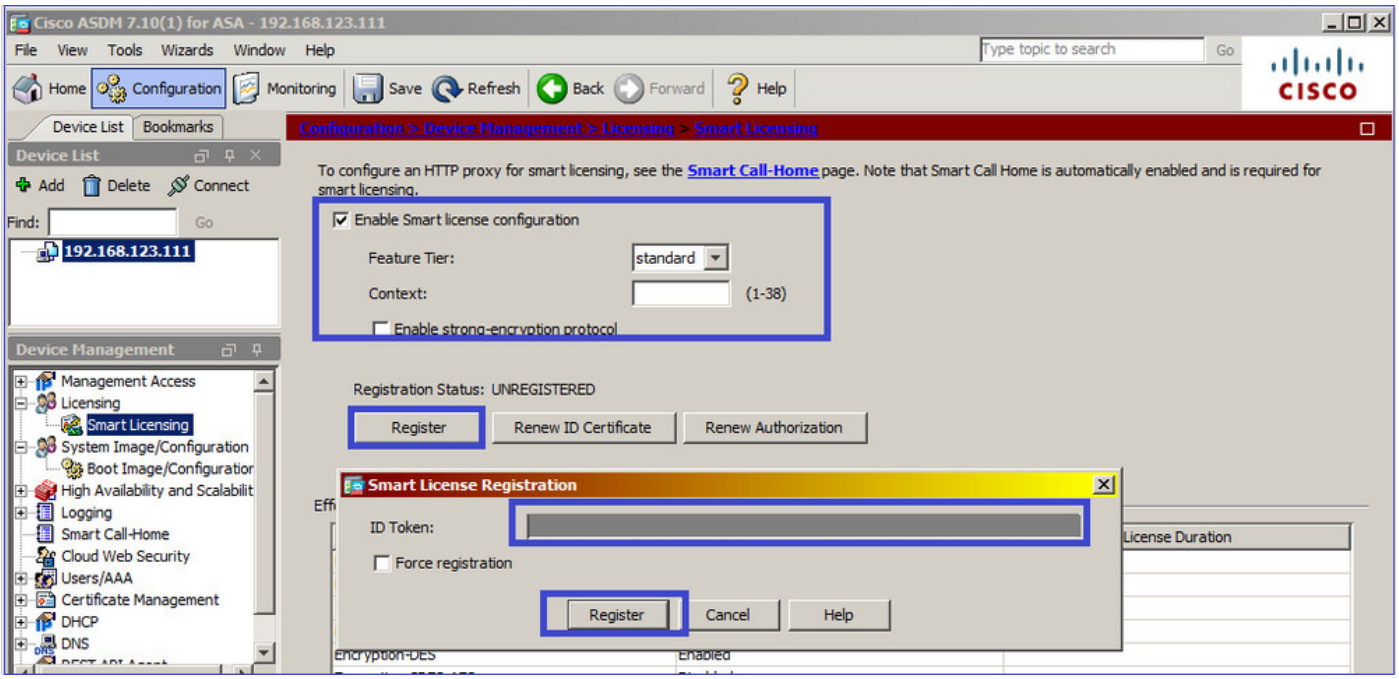
```
ciscoasa(config)# debug ssl 255
debug ssl enabled at level 255.
error:1408A0C1:SSL routines:ssl3_get_client_hello:no shared cipher
```

要克服ASA在面向網際網路的介面上僅配置了管理功能，因此可以進行ASDM連線：

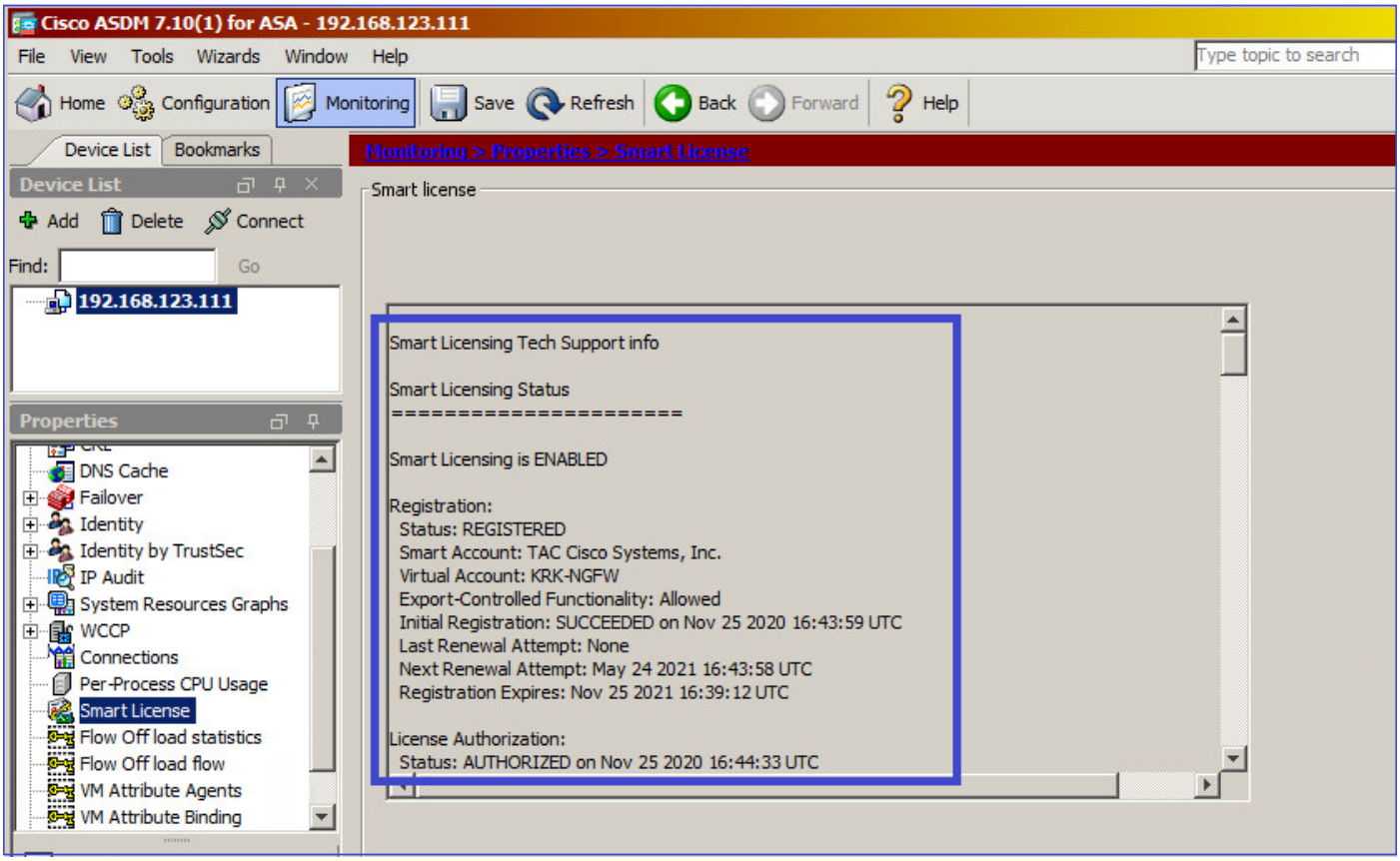
```
interface Ethernet1/2
management-only
nameif outside
security-level 100
ip address 192.168.123.111 255.255.255.0 standby 192.168.123.112
```



在主ASA上配置智慧許可：



導航至 **Monitoring > Properties > Smart License** 檢查註冊狀態：



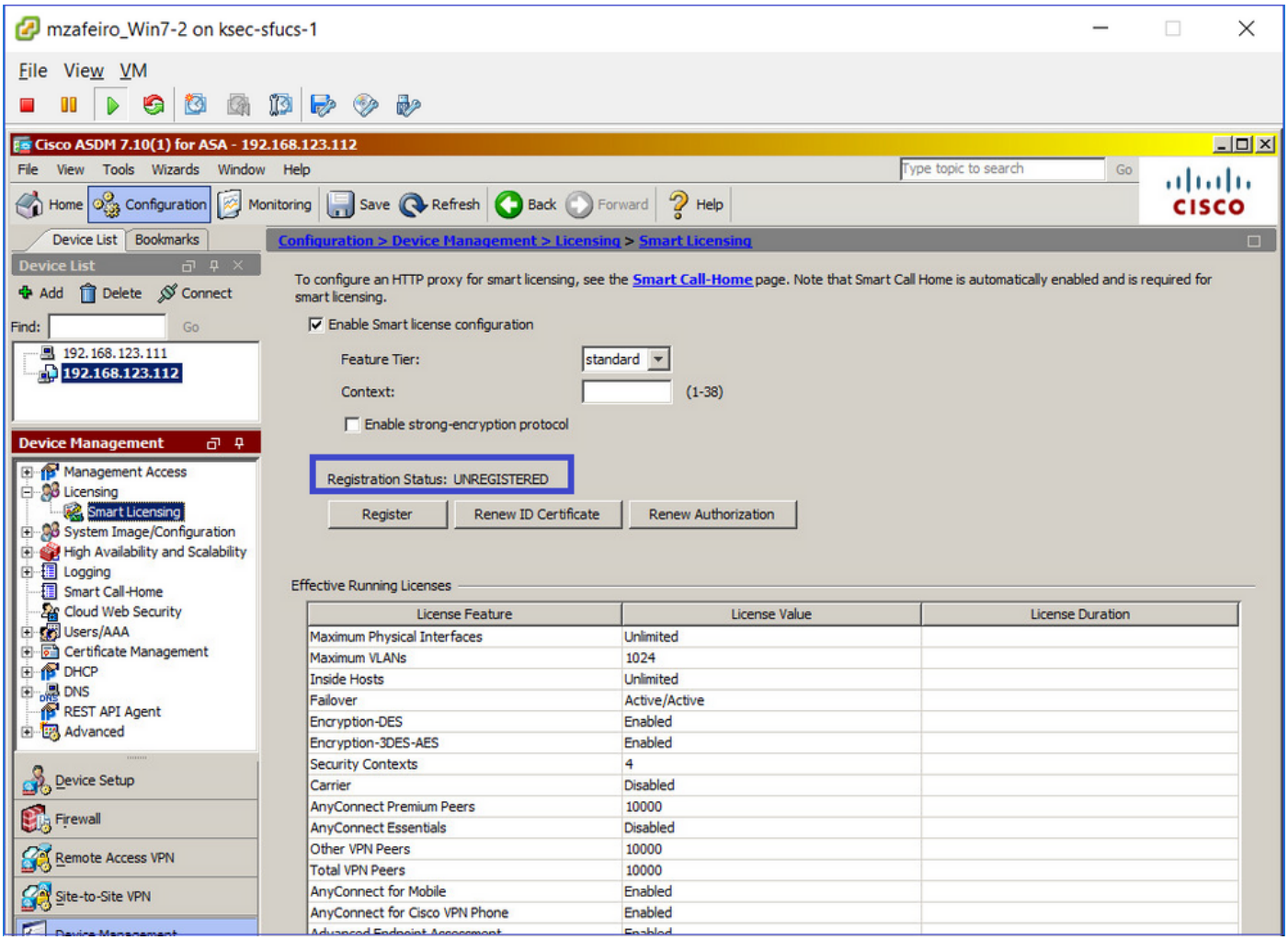
主要ASA CLI驗證：

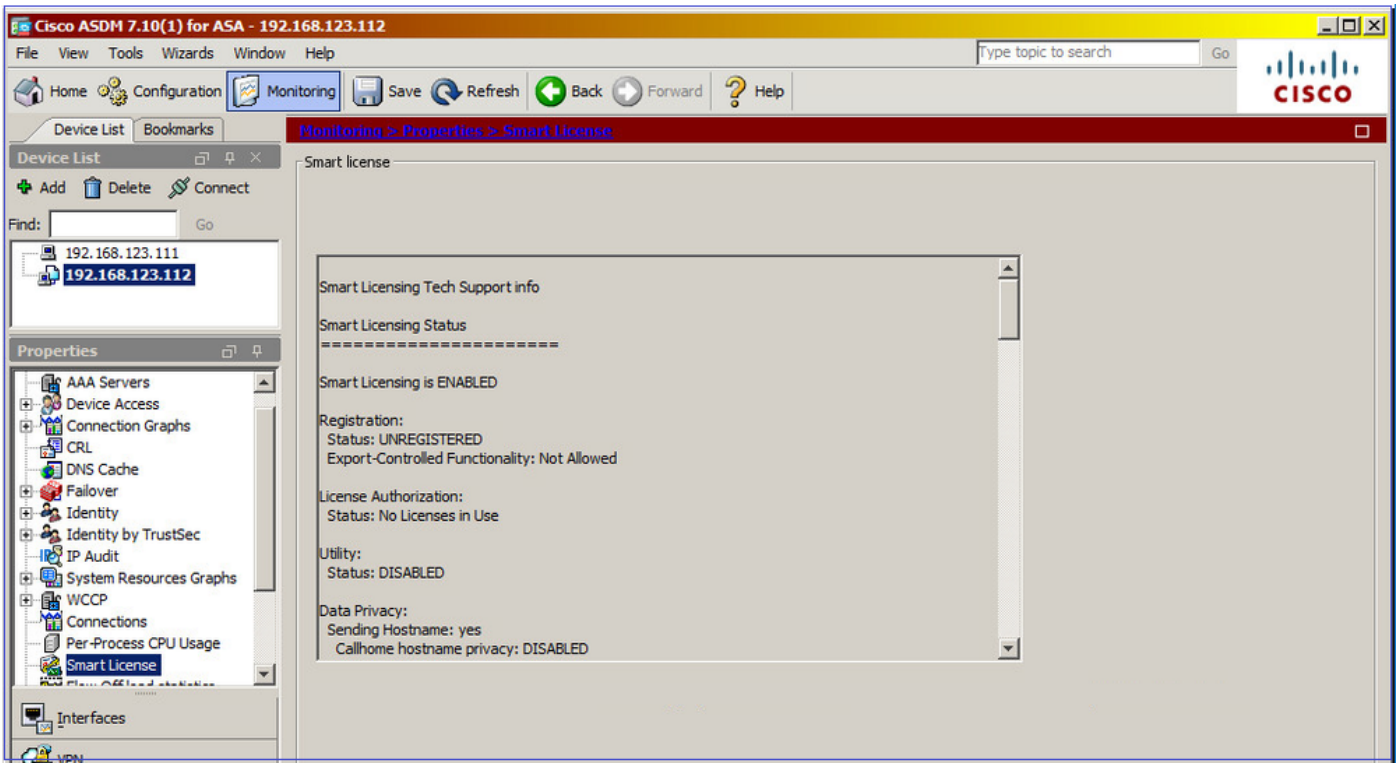
```
ciscoasa/pri/act# show license all

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
```

通過ASDM連線到備用ASA（僅當已為ASA配置了備用IP時才可能如此）。備用ASA顯示為UNREGISTERED 這是預期結果，因為它尚未註冊到智慧許可門戶：





備用ASA CLI顯示：

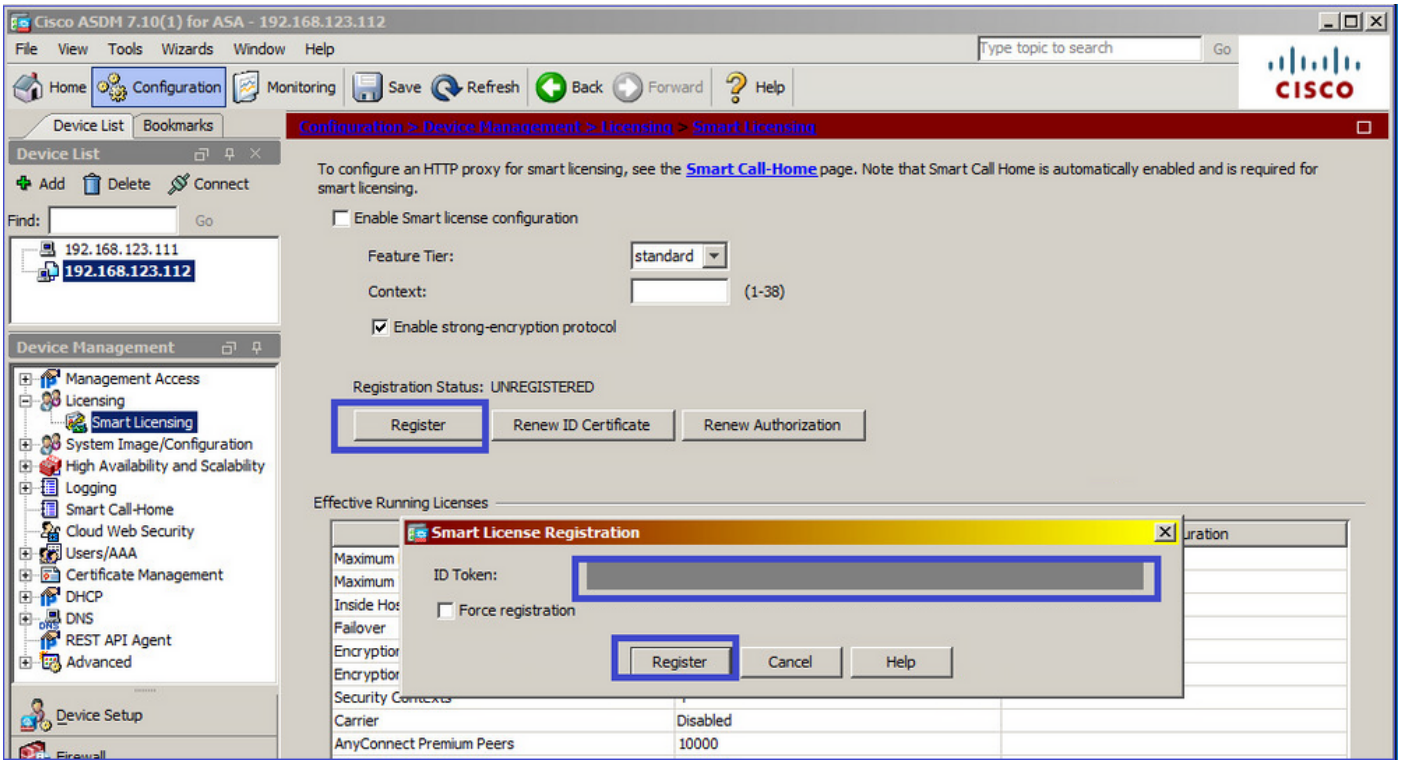
```
ciscoasa/sec/stby# show license all

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
```

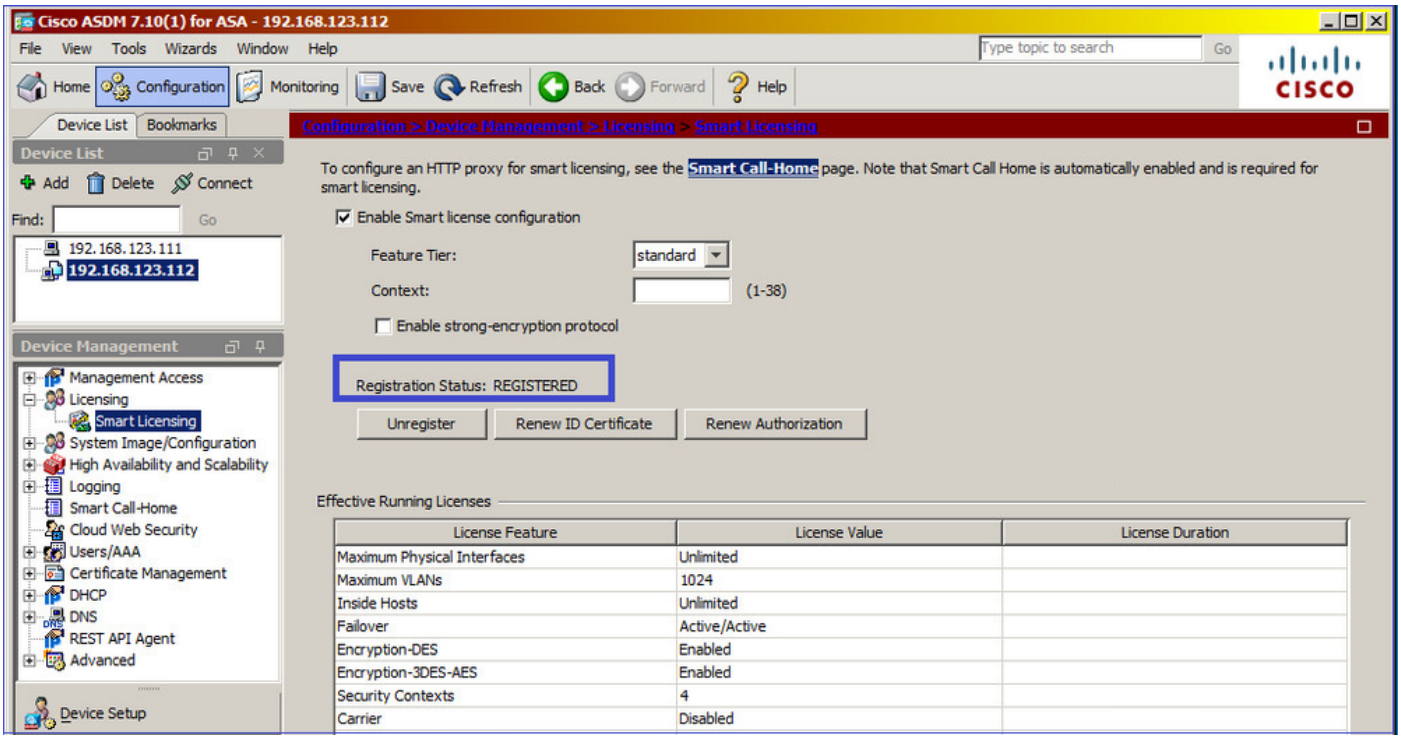
在備用ASA上啟用的許可證功能：

```
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
```

註冊備用ASA:



備用ASA的結果是 REGISTERED:



待命ASA上的CLI驗證：

```
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

如果裝置的許可證不匹配，則不會形成群集：

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

成功的群集設定：

```
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.
```

群集控制節點：

```
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
```

群集資料單元：

```
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
```

驗證與偵錯

機箱(MIO)驗證命令摘要：

```
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
```

組態驗證：

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

ASA驗證命令摘要：

```
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
```

機箱(MIO)驗證命令的輸出示例

```
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
```

驗證命令的ASA輸出示例

```
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
```

成功註冊

輸出來自機箱管理器使用者介面(UI):

```
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
```

過期的授權

輸出來自機箱管理器UI:

```
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
```

機箱CLI的輸出示例

未註冊

```
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
```

正在註冊

```
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
```

註冊錯誤

```
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
```

評估期

```
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
```

FXOS機箱(MIO)上的常見許可證問題

註冊錯誤：無效令牌

```
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."]}
```

建議步驟

1. 檢查call-home URL是否指向CSSM。
2. 登入CSSM，並檢查權杖是否由此產生，或權杖是否過期。

註冊錯誤：產品已註冊

```
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."]}
```

建議步驟

1. 登入CSSM。
2. 請檢視 Product Instances 頁籤。
3. 通過SN查詢舊註冊例項並將其刪除。
4. 此問題可能是以下兩種原因造成的： 未能在時間/日期設定不正確時自動續訂，例如未配置NTP伺服器。在衛星和生產伺服器之間切換時，操作順序錯誤，例如，先更改URL，然後發出「取消註冊」

註冊錯誤：日期偏移量超出限制

```
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."]}
```

建議步驟

檢查時間/日期配置，確保配置了NTP伺服器。

註冊錯誤：無法解析主機

```
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
```

建議步驟

1. 檢查callhome SLDest URL是否正確(scope monitoring > scope callhome > show expand)
2. 檢查MIO DNS伺服器配置是否正確，例如，從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.嘗試從機箱CLI對 **tools.cisco.com** 並檢視它是否解決：

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

4.嘗試從機箱CLI對DNS伺服器執行ping:

```
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.啟用機箱(MIO)管理介面上的捕獲（僅適用於FP41xx/FP93xx），並在您對運行ping測試時檢查

DNS通訊 **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
```

註冊錯誤：無法驗證伺服器

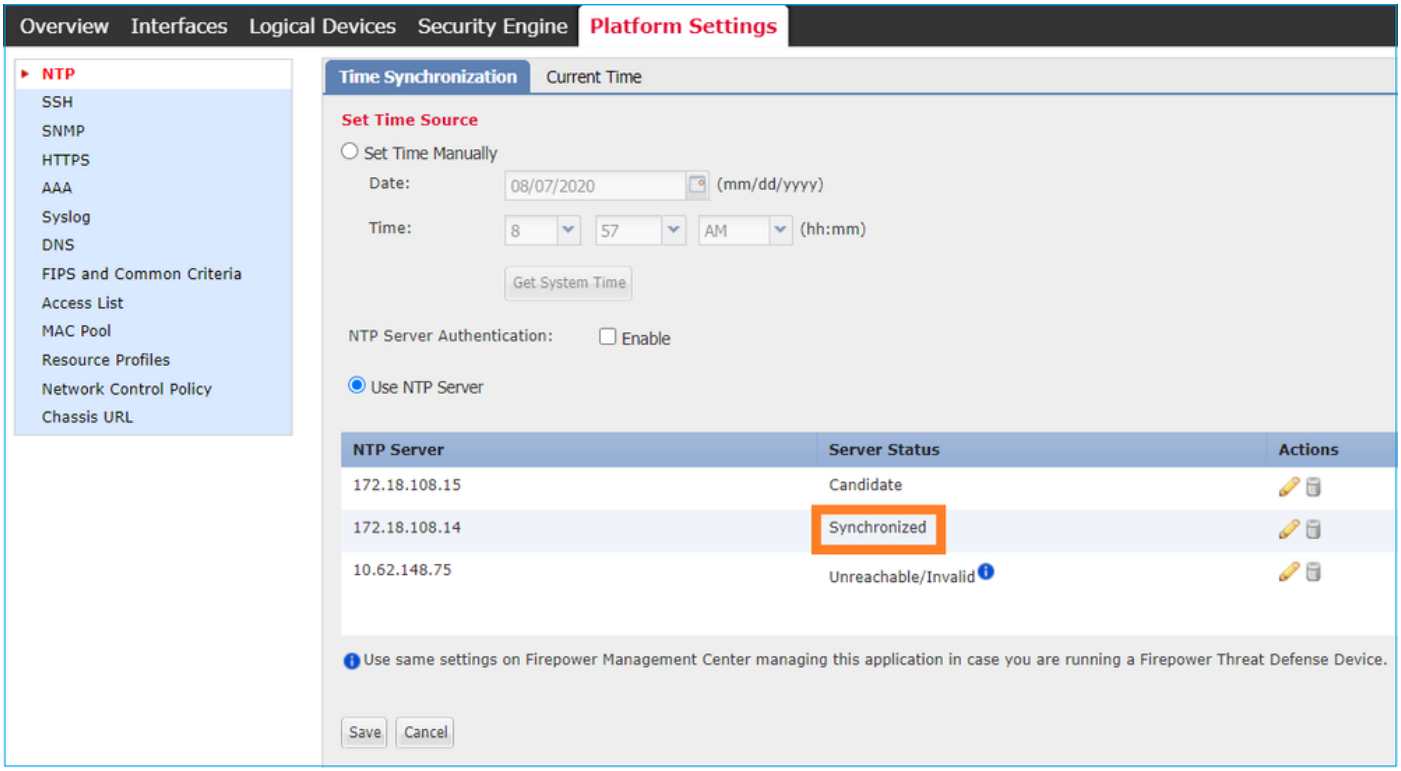
```
FPR4125-1# show license all

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
```

建議步驟

1.檢查MIO信任點CHdefault是否具有正確的證書，例如：

```
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.檢查NTP伺服器和時區是否設定正確。伺服器與客戶端之間的證書驗證需要相同時間。為此，請使用NTP同步時間。例如，FXOS UI驗證：



CLI 驗證

```
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
```

啟用捕獲並檢查MIO和 tools.cisco.com.在此您有幾種選擇：

- 您可以關閉到FXOS UI的HTTPS會話，然後在CLI上為HTTPS設定捕獲篩選器，例如：

```
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
```

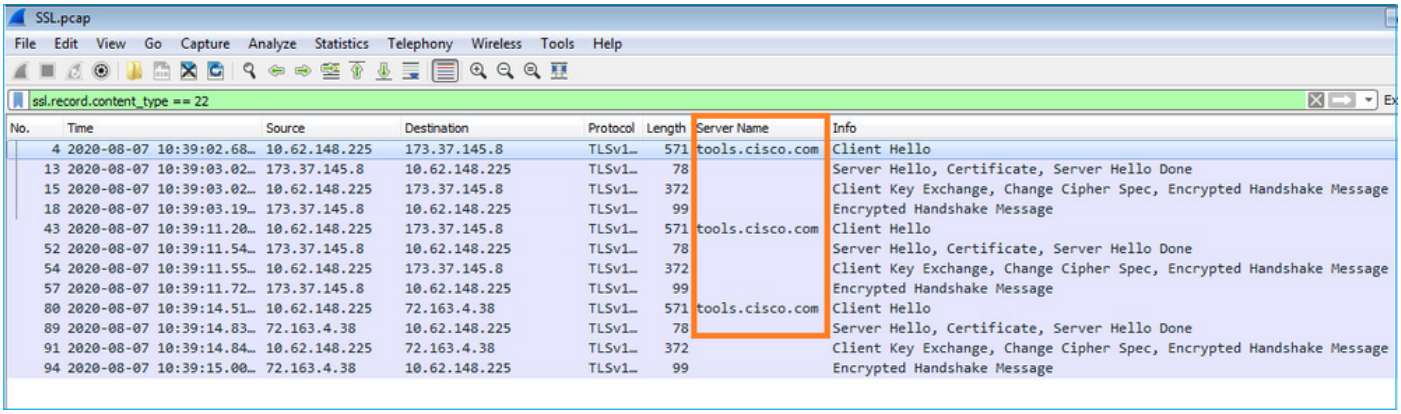
```
2017-01-12 13:09:44.609599  72.163.4.38 -> 10.62.148.37 SSL Continuation Data
2017-01-12 13:09:44.609610 10.62.148.37 -> 72.163.4.38  TCP 43278 > https [ACK] Seq=518 Ack=2737
Win=10944 Len=0 TSV=206433902 TSER=2933962264
```

- 此外，如果要保持FXOS UI開啟，可以在捕獲中指定目標IP(72.163.4.38和173.37.145.8是 **tools.cisco.com** 伺服器)。強烈建議以pcap格式儲存捕獲並在Wireshark中檢查它。以下是成功註冊的示例：

```
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
```

- 將pcap檔案匯出到遠端FTP伺服器：

```
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)#
```



註冊錯誤： HTTP傳輸失敗

```
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
```

建議步驟

1. 檢查call-home URL是否正確。您可以從FXOS UI或CLI(**scope monitoring > show callhome detail expand**)。
2. 啟用捕獲並檢查MIO和 **tools.cisco.com** 如本檔案的「無法驗證伺服器」一節所示。

註冊錯誤：無法連線到主機

```
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
```

建議步驟

1. 如果啟用代理配置，請檢查代理URL和埠是否配置正確。

2. 啟用捕獲並檢查MIO和 **tools.cisco.com** 如本檔案的「無法驗證伺服器」一節所示。

註冊錯誤： HTTP伺服器返回錯誤代碼>= 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
```

建議步驟

1. 如果已啟用代理配置，請聯絡代理伺服器管理員瞭解代理設定。
2. 啟用捕獲並檢查MIO和 **tools.cisco.com** 如本檔案的「無法驗證伺服器」一節所示。嘗試從FXOS CLI重新註冊（「force」選項）：

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

註冊錯誤：分析後端響應消息失敗

```
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
```

建議步驟

1.稍後自動重試嘗試。請使用「續約」立即重試。

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

2.檢查call-home URL是否正確。

ASA上的許可證問題 — 1xxx/21xx系列

註冊錯誤：通訊消息傳送錯誤

```
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
```

建議步驟

1.檢查DNS設定

```
ciscoasa# show run dns
```

2.嘗試ping **tools.cisco.com**.在此案例中，使用管理介面：

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

3.檢查路由表：

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

確保已啟用許可證，例如：

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

```
 feature strong-encryption
```

4.在路由到路由器的介面上啟用捕獲 **tools.cisco.com** （如果您在沒有任何IP過濾器的情況下捕獲資料，請確保在進行捕獲時未開啟ASDM以避免不必要的捕獲雜訊）。

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

警告：資料包捕獲可能會對效能產生不利影響。

5.在註冊過程中臨時啟用系統日誌級別7（調試）並檢查ASA系統日誌消息：

```
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
```

嘗試重新註冊：

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

附加權利的特殊要求

- 在配置任何附加權利之前，需要獲取有效的功能層權利
- 在釋放功能層權利之前，需要釋放所有附加權利

重新啟動操作期間的權利狀態

- 權利狀態儲存在快閃記憶體中
- 在啟動期間，將從快閃記憶體中讀取此資訊，並根據儲存的實施模式設定許可證
- 啟動配置將基於此快取的授權資訊應用
- 每次重新啟動後都會再次請求授權

聯絡Cisco TAC支援

FP41xx/FP9300

如果本文檔中提到的所有專案均失敗，則從機箱CLI收集這些輸出並聯絡思科TAC:

輸出1:

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

輸出2:

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

產出3:

FXOS機箱支援套件

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

產出4（強烈建議）：

Ethanalyzer從機箱CLI捕獲

FP1xxx/FP21xx

輸出1:

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

輸出2:

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

常見問題(FAQ)

在FP21xx上，機箱(FCM)GUI上的Licensing（許可）頁籤位於何處？

自9.13.x起，FP21xx支援2個ASA模式：

- 裝置
- 平台

在裝置模式下，沒有機箱UI。在平台模式下，有一個機箱UI，但從ASA CLI或ASDM配置許可證。另一方面，在FPR4100/9300平台上，必須在FCM中通過GUI或FXOS CLI配置許可證，並且必須從ASA CLI或ASDM請求ASA授權。
參考資料：

- 適用於ASA的許可證管理
- Firepower 4100/9300的邏輯裝置
- 許可證：智慧軟體許可（ASAv、Firepower上的ASA）
- 採用ASDM和Firepower機箱管理器的ASA平台模式部署

如何啟用強加密許可證？
如果FCM註冊中使用的令牌具有在啟用該令牌後註冊的產品上允許匯出控制功能的選項，則會自動啟用此功能。

如果FCM級別上的匯出控制功能和ASA級別上的相關Encryption-3DES-AES被禁用，如何啟用強加密許可證？
如果令牌未啟用此選項，請取消註冊FCM，然後使用已啟用此選項的令牌再次註冊。

生成令牌時，如果註冊到此令牌的產品上的「允許匯出控制功能」選項不可用，該怎麼辦？
請聯絡您的思科客戶團隊。

在ASA級別上配置強加密功能是強制性的嗎？
僅當FCM與2.3.0之前的衛星伺服器整合時，功能強加密選項才是強制性的。只有當您必須設定此功能時，才會出現這種情況。

在FCM和智慧許可雲之間的路徑中必須允許哪些IP?
FXOS使用地址https://tools.cisco.com/（埠443）與許可雲通訊。地址https://tools.cisco.com/將解析為以下IP地址：

- 72.163.4.38
- 173.37.145.8

為什麼會出現Out of Compliance錯誤？
在以下情況下，裝置可能會不符合要求：

- 過度使用（裝置使用不可用的許可證）
- 許可證過期 — 基於時間的許可證已過期
- 缺少通訊 — 裝置無法聯絡授權機構進行重新授權

要驗證您的帳戶是否處於或接近不合規狀態，必須將Firepower機箱當前使用的授權與智慧帳戶中的授權進行比較。
在不合規狀態下，可以對需要特殊許可證的功能進行配置更改，但操作不會受到影響。例如，超過標准許可證限制後，已經存在的上下文將繼續運行，您可以修改其配置，但不能新增新上下文。

為什麼新增許可證後仍會出現「Out of Compliance」錯誤？

預設情況下，裝置每30天與許可證頒發機構通訊一次，以檢查授權。如果要手動觸發它，必須執行以下步驟：

對於FPR1000/2100平台，必須通過ASDM或CLI完成：

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

對於FPR4100/9300平台，必須通過FXOS CLI完成：

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

為什麼在ASA級別沒有使用許可證？
確保在ASA級別上配置了ASA權利，例如：

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

為什麼即使在配置ASA授權之後，許可證仍未被使用？
如果您部署了ASA主用/備用故障轉移對，並檢查備用裝置上的許可證使用情況，則此狀態為預期狀態。
根據《配置指南》，配置會複製到備用裝置，但備用裝置不使用配置；它仍保持快取狀態。只有活動裝置才從伺服器請求許可證。許可證會聚合到由故障轉移對共用的單個故障轉移許可證中，並且此聚合許可證也快取到備用裝置上，以便在備用裝置將來成為活動裝置時使用。供參考：故障切換或ASA集群許可證。

如果FCM無法訪問Internet，您可以做什麼？
或者，您可以部署Cisco Smart Software Manager On-Prem（以前稱為Cisco Smart Software Manager衛星）。這是思科智慧許可的一個元件，與思科智慧軟體管理器配合使用。它為您購買和使用的思科許可證提供近乎即時的可視性和報告功能。它還為安全敏感型組織提供了一種訪問思科SSM功能子集的方法，而無需使用直接網際網路連線來管理其客戶群。

在哪裡可以找到有關思科智慧軟體管理器內部版本的更多資訊？
您可以在FXOS配置指南中找到此資訊：

- 為Firepower 4100/9300機箱配置智慧許可證衛星伺服器
- 將Firepower機箱管理器註冊配置為本地智慧軟體管理器

相關資訊

- Cisco ASA系列常規操作CLI配置指南
- 適用於ASA的許可證管理
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。