FXOS FirepowerアプライアンスでのASAスマートライセンスのトラブルシューティング

内容

概要

このドキュメントでは、Firepower eXtensible Operating System（FXOS）適応型セキュリティアプライアンス（ASA）のスマートライセンスの機能について説明します。

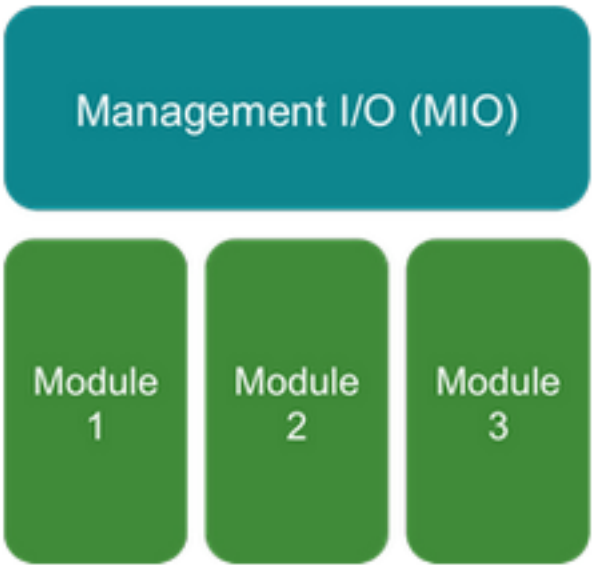
背景説明

FXOS のスマートライセンスは、シャーシに ASA がインストールされている場合に使用されます。Firepower Threat Defense（FTD）および Firepower Management Center（FMC）のスマートライセンスについては、「FMC および FTD スマートライセンスの登録とトラブルシューティング」を確認してください。

ここでは主に FXOS シャーシでダイレクト インターネット アクセスが可能な場合について説明します。FXOSシャーシがインターネットにアクセスできない場合は、サテライトサーバまたは Permanent License Reservation(PLR)を検討する必要があります。詳細については、FXOS コンフィギュレーション ガイドの「オフライン管理」を確認してください。

スマートライセンスのアーキテクチャ

シャーシコンポーネントの概要

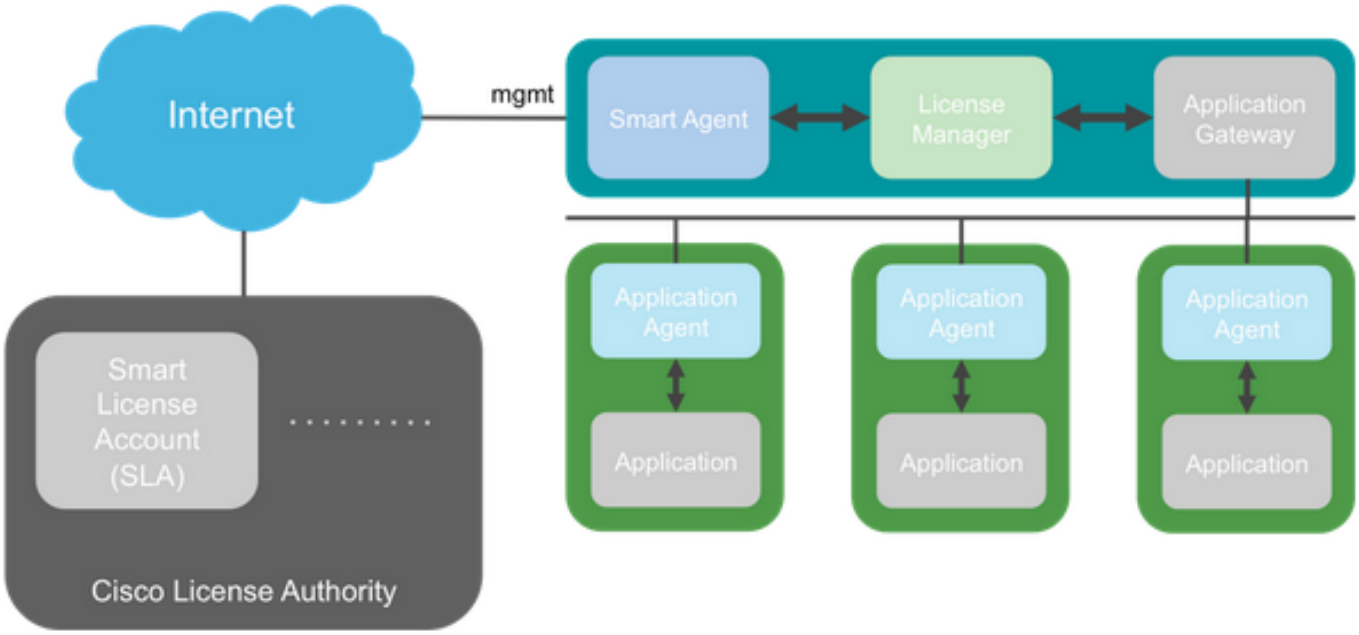


- スマートライセンスでは管理入出力（MIO）と個々のモジュールの両方が役割を果たす
- MIO 自体を機能させるためのライセンスは不要
- 各モジュールのSAアプリケーションにはライセンスが必要です。

FXOSスーパーバイザはMIOです。MIOには、次の3つの主要コンポーネントがあります。

- スマートエージェント
- ライセンス マネージャ
- AppAG

全体的なアーキテクチャ



用語

ターム	説明
シスコライセンス機関	スマートライセンス用のシスコのライセンスバックエンドで、すべて

	の製品ライセンス関連情報を保持します。これには、資格とデバイス情報が含まれます。
スマート ライセンス アカウント	アプライアンスのすべての権限を持つアカウント。
トークンID	IDは、アプライアンスの登録時にスマートライセンスアカウントを区別するために使用されます。
権限	ライセンスと同義です。個々のフィーチャまたはフィーチャ層全体に対応します。
製品認証キー（PAK）	古いライセンスメカニズムで、一台のアプライアンスと紐付けられます。

スマートエージェントの状態

都道府県	説明
未設定	スマートライセンスが有効になっていません.
不明	スマートライセンスは有効になっていますが、スマートエージェントがシスコに登録のための連絡をしていません.
登録済み	エージェントはシスコのライセンス機関に連絡し、登録済みです.
承認済み	エージェントが権限付与承認要求に応答して準拠ステータスを受信したとき。
コンプライアンス違反(OOC)	エージェントが権限付与承認要求に応答してOOCステータスを受信したとき。
認証が期限切れ	エージェントが 90 日間シスコと通信を行っていない場合に、この状態になります.

ASA の権限

サポートされている ASA の権限は次のとおりです。

- 標準層
- マルチコンテキスト
- 高度暗号化（3DES）
- モバイル/サービスプロバイダー（GTP）

コンフィギュレーション

次のドキュメントの指示に沿って設定してください。

- スマート ソフトウェア ライセンス（ASAv、ASA on Firepower）
- ASA のライセンス管理

各機能階層の設定に進む前に、以下を確認:

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

標準階層の設定

```
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
```

フェールオーバー (ハイ アベイラビリティ)

ASA コンフィギュレーション ガイドで説明されているように、各 Firepower ユニットを License Authority またはサテライトサーバーに登録する必要があります。ASA CLI で次のように確認します。

```
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
```

スタンバイユニット

```
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
```

ケーススタディ：FP2100でのASA HAライセンス

- 2100では、ASAはFXOS管理ではなく、ASAインターフェイスを介してCisco Smart Licensingポータル（クラウド）と通信します
- HA 構成の両方の ASA を Cisco Smart Licensing ポータル（クラウド）に登録する必要があります。

この場合、HTTP口ーカル認証は外部インターフェイスで使用されます。

```
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
```

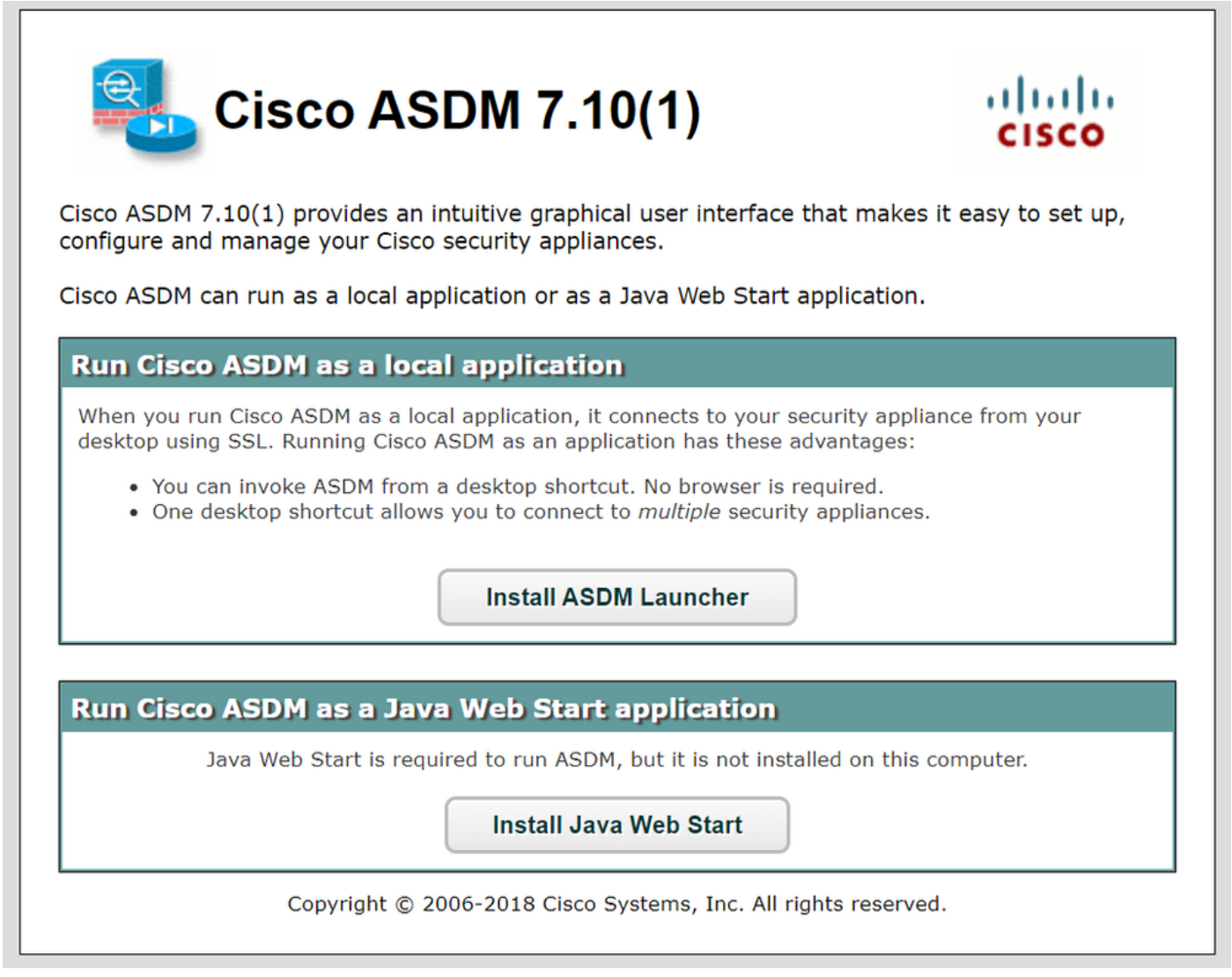
3DES/AES ライセンスが有効になっている場合のみ、ASDM を介して ASA に接続できます。まだ登録されていないASAの場合は、ASAに登録されているインターフェイスでのみ、 management-

only.設定ガイドによると、「強力な暗号化(3DES/AES)は、ASDMを起動できるように、ライセンス認証局またはサテライトサーバに接続する前に管理接続に使用できます。ASDM アクセスは、デフォルトの暗号化を適用する管理専用インターフェイスでのみ使用できることに注意してください。Through-the-boxトラフィックは、接続してStrong Encryptionライセンスを取得するまで許可されません。別のケースでは、次のように表示されます。

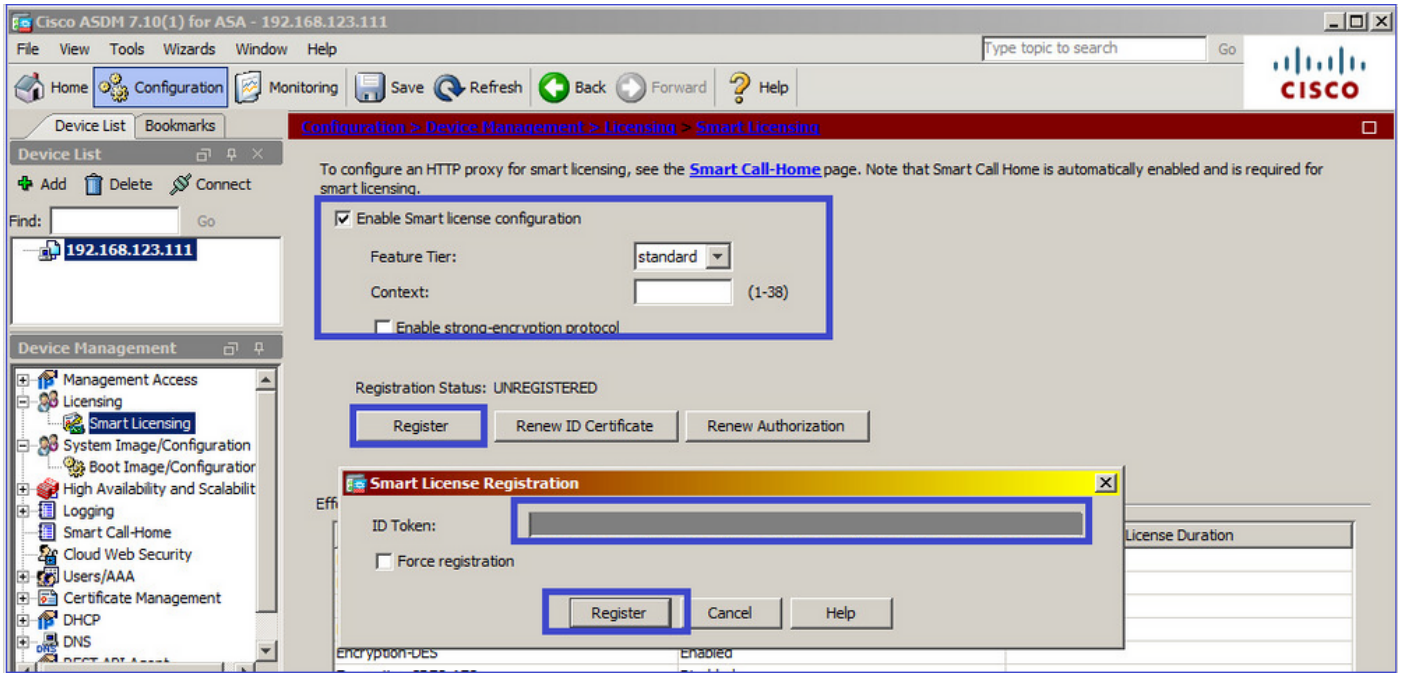
```
ciscoasa(config)# debug ssl 255
debug ssl enabled at level 255.
error:1408A0C1:SSL routines:ssl3_get_client_hello:no shared cipher
```

これを克服するために、ASA ではインターネットに接続されるインターフェイスが管理専用に設定されているため、ASDM との接続が可能です。

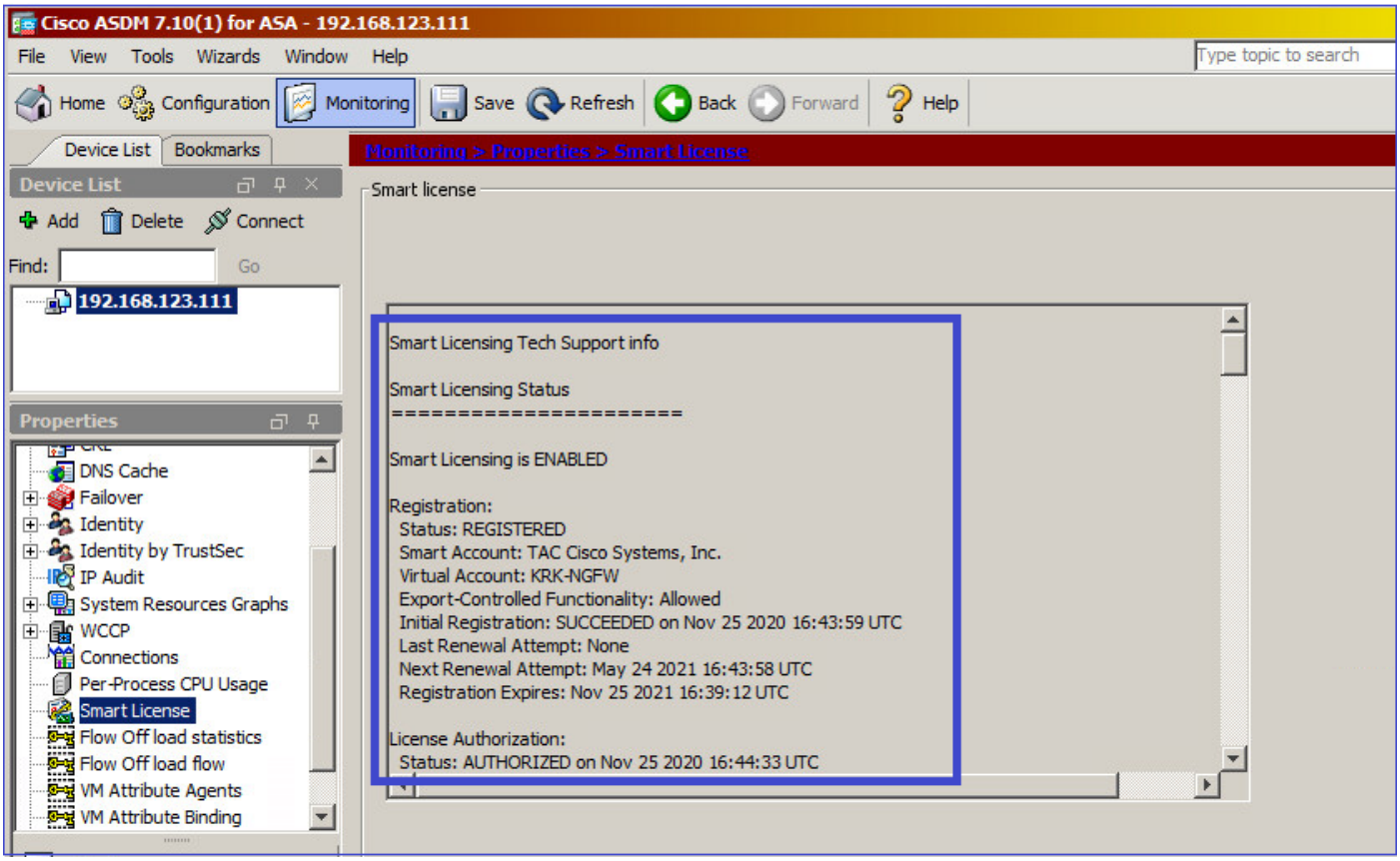
```
interface Ethernet1/2
management-only
nameif outside
security-level 100
ip address 192.168.123.111 255.255.255.0 standby 192.168.123.112
```



プライマリ ASA にスマートライセンスを設定します。



移動先 **Monitoring > Properties > Smart License** 登録のステータスを確認するには、次の手順に従います。



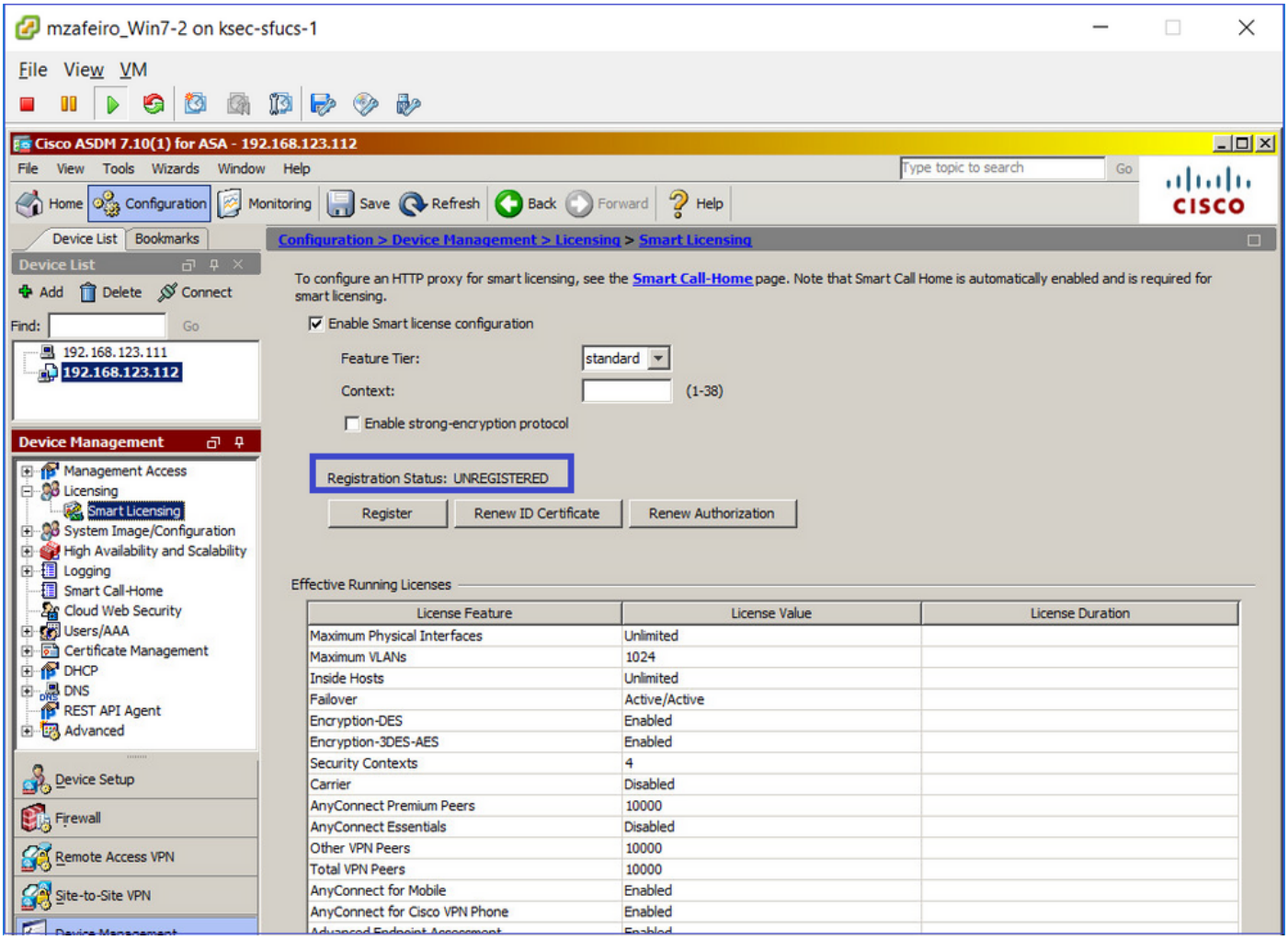
プライマリ ASA の CLI での確認

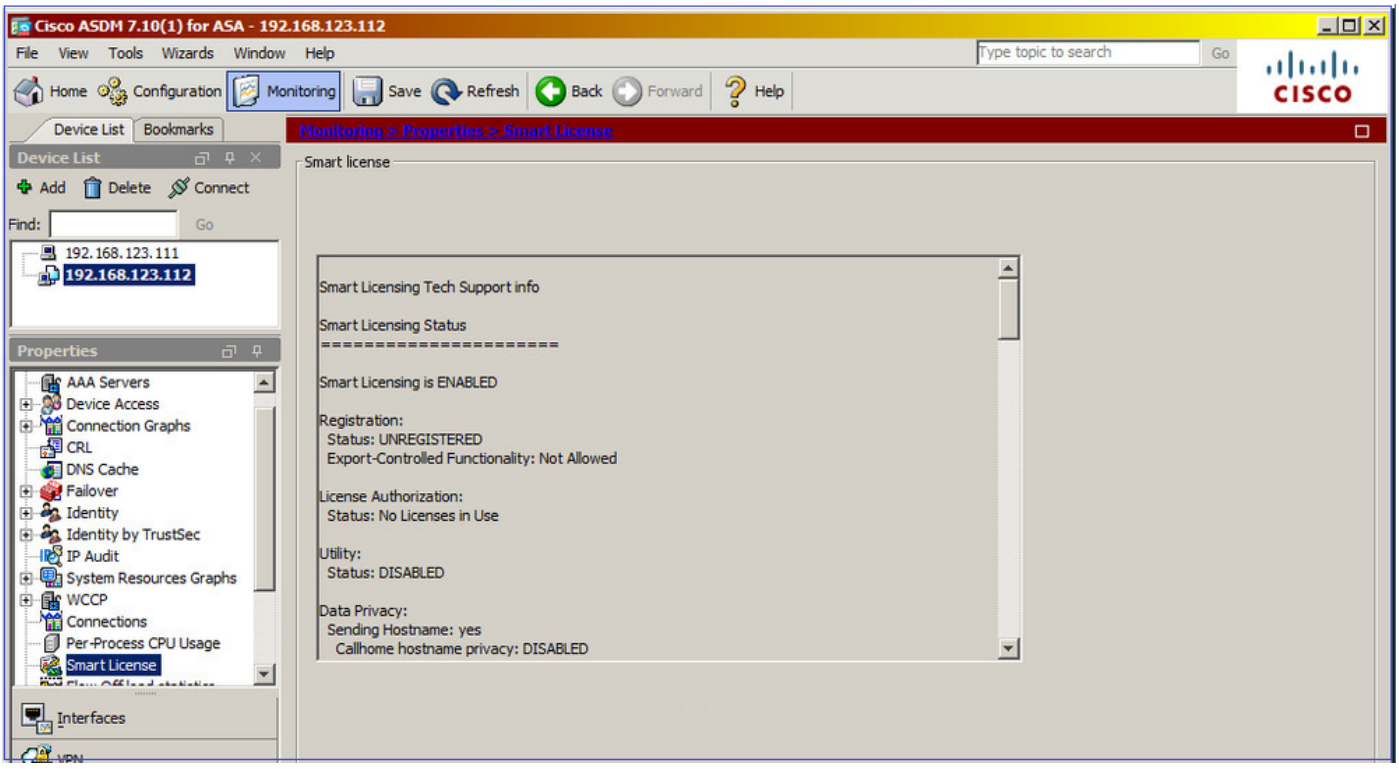
```
ciscoasa/pri/act# show license all

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
```

ASDM経由でスタンバイASAに接続します（これは、ASAがスタンバイIPで設定されている場合にのみ可能です）。スタンバイASAは次のように表示されます。 UNREGISTERED これは、スマートライセンシングポータルにまだ登録されていないため予想されます。





スタンバイ ASA の CLI で状態を確認します。

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

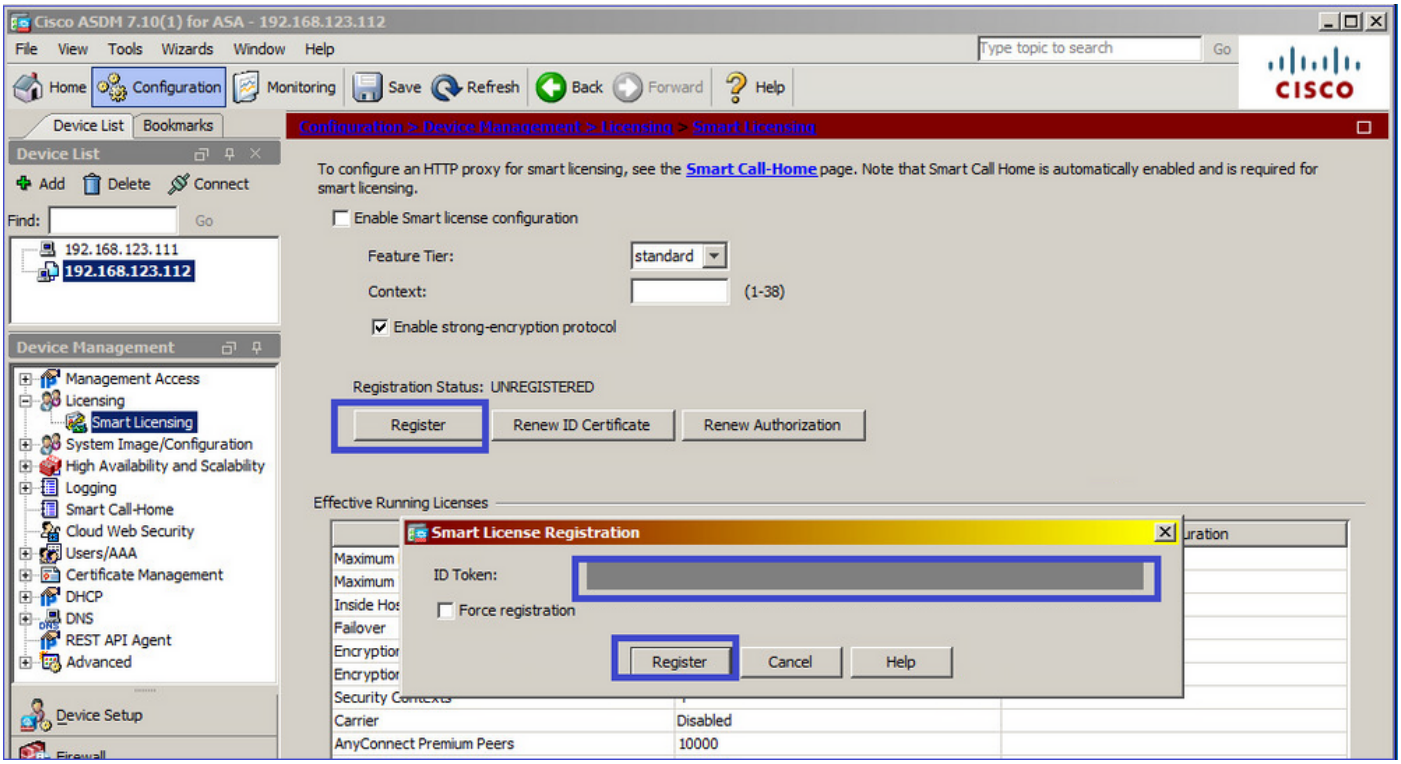
```
Smart Licensing Status
======================

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
```

スタンバイ ASA で有効になっているライセンス機能は次のとおりです。

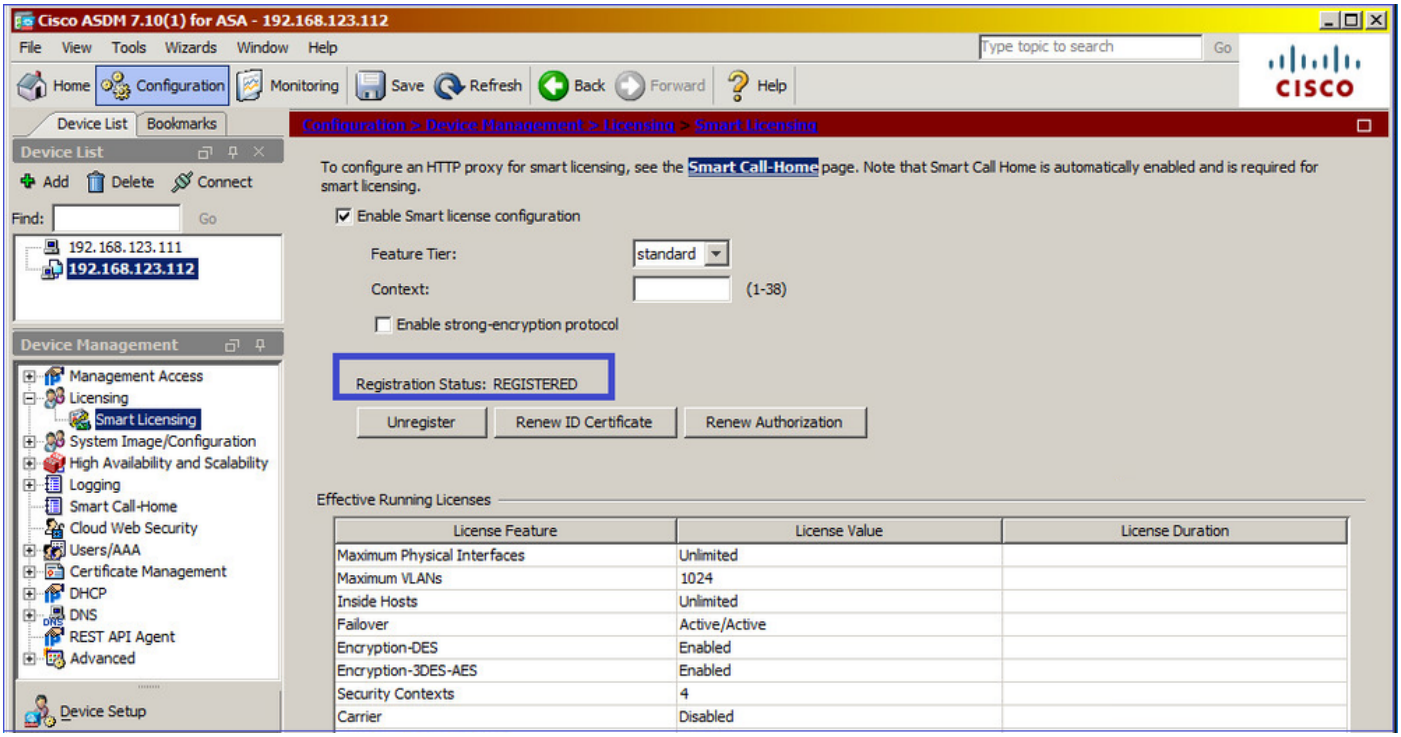
```
ciscoasa/sec/stby# show license features
Serial Number: JAD123456A
Export Compliant: NO

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
```

スタンバイ ASA を登録します。



スタンバイASAでの結果は、 REGISTERED:



スタンバイ ASA での CLI の確認

```
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 クラスタ

デバイスにライセンスの不一致がある場合、クラスタは形成されません。

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

クラスタが正しく設定されている場合の表示

```
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.
```

クラスタ制御ノード：

```
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
```

クラスタデータユニット：

```
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
```

検証とデバッグ

確認コマンドによるシャーシ（MIO）情報の要約:

```
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
```

設定の確認:

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

確認コマンドによる ASA 情報の要約:

```
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
```

確認コマンドによるシャーシ (MIO) 情報の出力例

```
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
```

確認コマンドによる ASA 情報の出力例

```
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
```

正常に登録された場合の表示

以下の出力は、シャーシマネージャのユーザーインターフェイス（UI）からの情報です。

```
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
```

承認期限切れ

出力は、シャーシマネージャのUIに表示されます。

```
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
```

シャーシ CLI からの出力例

未登録

```
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
```

登録の進行中

```
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
```

登録エラー

```
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
```

評価期間

```
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 シャーシ（MIO）での一般的なライセンスの問題

登録エラー：トークンが無効です

```
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."]}
```

推奨手順

1. Call Home URLがCSSMを指しているかどうかを確認します。
2. CSSM にログインし、CSSM からトークンが生成されているか、またはトークンの有効期限が切れているかを確認します。

登録エラー：製品はすでに登録されています

```
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."]}
```

推奨手順

1. CSSMにログインします。
2. 次の項目を確認します。 Product Instances タブをクリックします。
3. SNで古い登録インスタンスを見つけて削除します。
4. この問題は、次の2つの原因で発生する可能性があります。 時刻や日付が正しく設定されていない場合（NTPサーバが設定されていない場合など）に自動的に更新されない。サテライトと実稼働サーバを切り替える際の操作の順序が間違っている。たとえば、最初にURLを変更してから、「deregister」を発行する

登録エラー：日付オフセットが制限を超えています

```
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."]}
```

推奨手順

時刻と日付の設定をチェックして、NTPサーバが設定されていることを確認します。

登録エラー：ホストを解決できませんでした

```
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

推奨手順

1. callhome SLDest URLが正しいことを確認します(scope monitoring > scope callhome > show expand)
2. MIO DNSサーバの設定が正しいかどうかを確認します。たとえば、CLIから次のコマンドを実行します。

```
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.シャーシのCLIからpingを試みます。 **tools.cisco.com** 解決するかどうかを確認します。

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

4.シャーシのCLIからDNSサーバにpingを実行します。

```
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. capture on chassis(MIO)管理インターフェイスを有効にし（これはFP41xx/FP93xxでのみ適用可能です）、 **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
```

登録エラー：サーバの認証に失敗しました

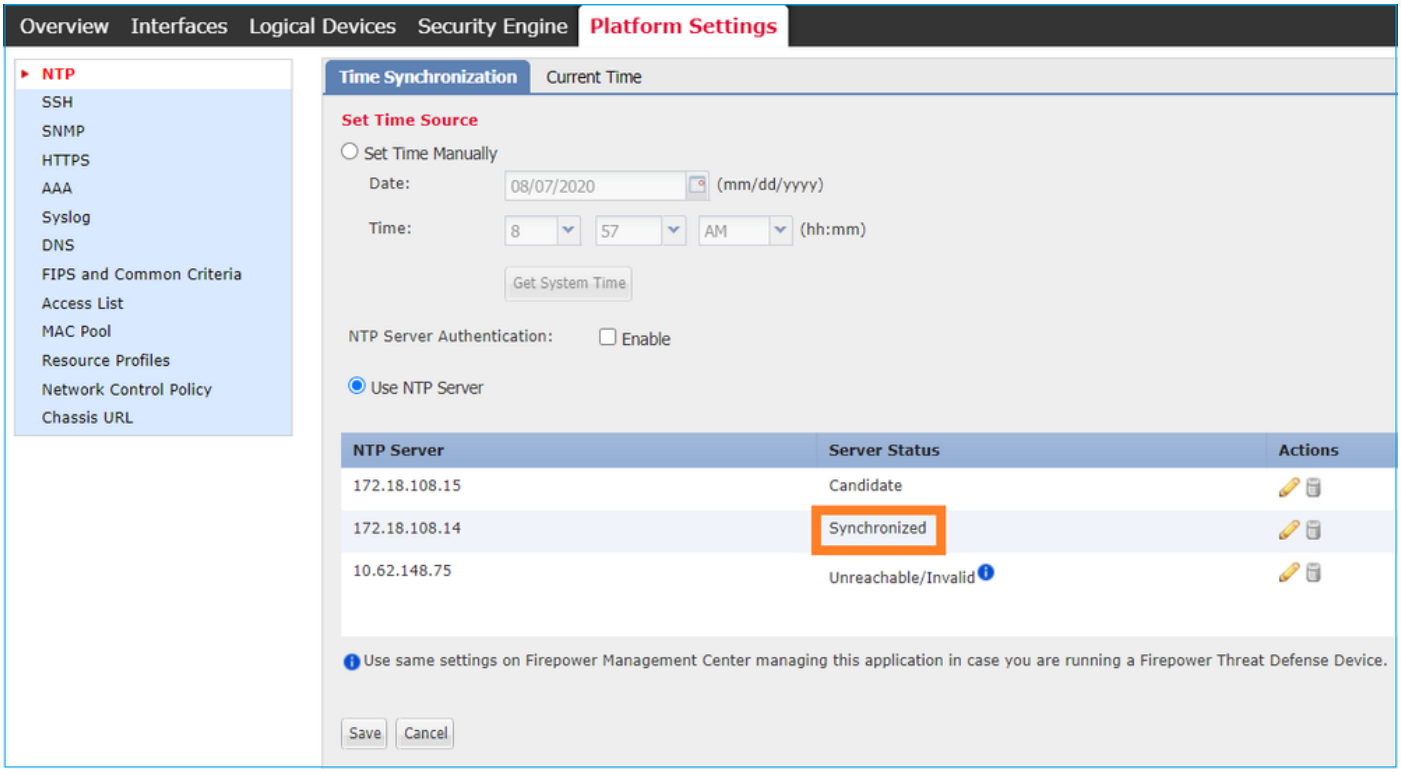
```
FPR4125-1# show license all

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
```

推奨手順

1. MIOトラストポイントCHdefaultに正しい証明書が設定されているかどうかを確認します。次に例を示します。

```
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. NTPサーバとタイムゾーンが正しく設定されていることを確認します。証明書の確認は、サーバーとクライアント間で同時に行う必要があります。そのためには NTP を使用して両者の時刻を同期します。たとえば、FXOS UIの確認は次のようになります。



CLI を使用した確認

```
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
```

キャプチャを有効にし、MIOとMIO間のTCP通信(HTTPS)を確認します。 **tools.cisco.com**.キャプチャにはいくつかのオプションがあります。

- FXOS UIへのHTTPSセッションを閉じてから、CLIでHTTPSのキャプチャフィルタを設定できます。次に例を示します。

```
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
```

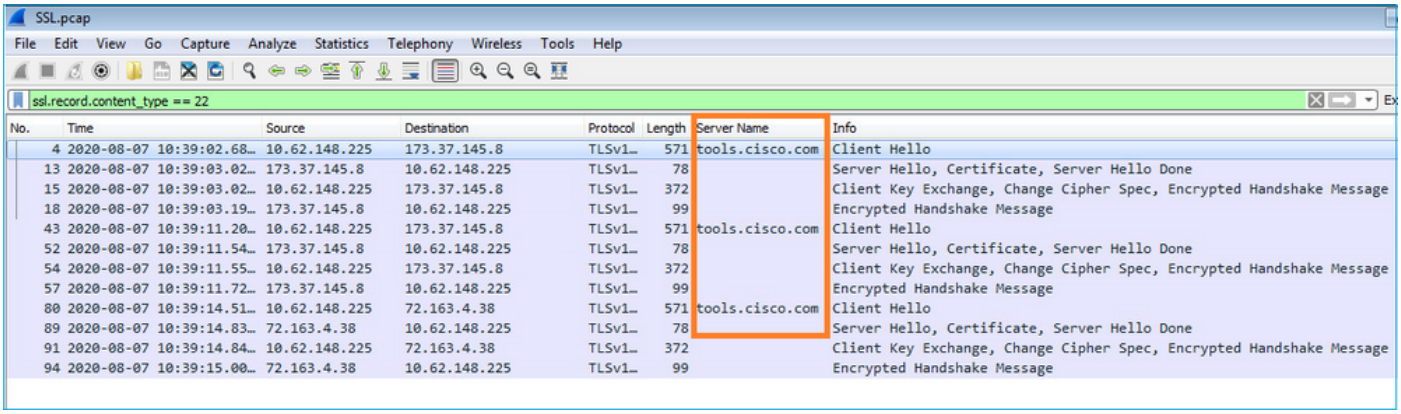
- また、FXOS UIを開いたままにしておきたい場合は、キャプチャで宛先IPを指定できます(72.163.4.38と173.37.145.8は **tools.cisco.com** このドキュメントの執筆時点でのサーバ)。なお、キャプチャは pcap 形式で保存し、Wireshark で内容を確認することを強くお勧めします。次の例は、登録が正常に完了した状態の出力です。

```
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
```

- pcap ファイルをリモートの FTP サーバーにエクスポートするには、次のコマンドを実行します。

```
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)#
```



登録エラー： HTTPトランスポートが失敗しました

```
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
```

推奨手順

1. Call-Home URL が正しいかを確認します。これは、FXOS UIまたはCLI(**scope monitoring > show callhome detail expand** ）。
2. キャプチャを有効にし、MIOとMIO間のTCP通信(HTTPS)を確認します。 **tools.cisco.com** このドキュメントの「サーバの認証に失敗した」セクションで示されているように。

登録エラー：ホストに接続できませんでした

```
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
```

推奨手順

1. プロキシ設定が有効になっている場合は、プロキシの URL とポートが正しいことを確認します。
2. キャプチャを有効にし、MIOとMIO間のTCP通信(HTTPS)を確認します。 **tools.cisco.com** このドキュメントの「サーバの認証に失敗した」セクションで示されているように。

登録エラー： HTTPサーバがエラーコード>= 400を返す

```
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
```

推奨手順

1. プロキシ設定が有効になっている場合は、プロキシサーバー管理者にその設定を問い合わせます。

2. キャプチャを有効にし、MIOとMIO間のTCP通信(HTTPS)を確認します。 **tools.cisco.com** このドキュメントの「サーバの認証に失敗した」セクションで示されているように。FXOS CLIから再登録を試みます（'force'オプション）。

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

登録エラー：バックエンド応答メッセージの解析に失敗しました

```
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
```

推奨手順

1.後で自動再試行を行います。すぐに再試行するには、'renew'を使用します。

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

2. call-home URLが正しいことを確認します。

ASA - 1000 および 2100 シリーズでのライセンスの問題

登録エラー：通信メッセージ送信エラー

```
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
```

推奨手順

1. DNS設定を確認します

```
ciscoasa# show run dns
```

2. pingを試みます。 **tools.cisco.com.**このケースでは管理インターフェイスを使用します。

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

3.ルーティングテーブルを確認します。

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

ライセンスが有効になっていることを確認します。次に例を示します。

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

4. IPアドレスを持つIPアドレスをルーティングするインターフェイスで、 **tools.cisco.com** （IPフィルタを使用せずにキャプチャを取得する場合は、不要なキャプチャノイズを回避するためにキャプチャを取得するときにASDMが開いていないことを確認してください）。

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

警告：パケットキャプチャはパフォーマンスに悪影響を及ぼす可能性があります。

5.登録プロセス中に一時的にSyslogレベル7（デバッグ）を有効にし、ASA Syslogメッセージを確認します。

```
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
```

もう一度登録を試します。

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

アドオン権限の特別な要件

- アドオン権限を構成する前に、有効な機能層の権限を取得する必要があります
- 機能層の権利をリリースする前に、すべてのアドオン権利をリリースする必要があります

再起動中の権限の状態

- 権限付与状態はフラッシュに保存されます。
- ブート時には、この情報がフラッシュから読み取られ、保存された強制モードに基づいてライセンスが設定されます
- スタートアップコンフィギュレーションは、キャッシュされた権限付与情報に基づいて適用されます
- 再起動のたびに資格が再度要求される

シスコ TAC サポートとの連携

FP4100 系/FP9300

このドキュメントで説明したすべての項目に障害が発生した場合は、シャーシのCLIから次の出力を収集し、Cisco TACにお問い合せください。

出力 1:

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

出力 2:

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

出力 3:

FXOS シャーシのサポートバンドル

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

出力4 (強く推奨)

Ethanalyzer によるシャーシ CLI からのキャプチャ

FP1000 シリーズ/FP2100 シリーズ

出力 1:

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

出力 2:

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

FAQ

FP2100 シリーズのシャーシ (FCM) GUI では、[ライセンス (Licensing)] タブはどこにありますか。
バージョン 9.13.x の時点で、FP2100 シリーズでは 2 つの ASA モードをサポートしています。

- アプライアンス
- Platform

アプライアンスモードには、シャーシ UI はありません。プラットフォームモードにはシャーシ UI がありますが、ライセンスの設定には ASA CLI か ASDM を利用します。
一方、FPR4100/9300 プラットフォームでは、ライセンスの設定は GUI か FXOS CLI を介して FCM で行う必要があり、ASA の権限は ASA CLI か ASDM からリクエストする必要があります。
参照:

- ASA のライセンス管理
- Firepower 4100/9300 の論理デバイス
- ライセンス：Smart Software Licensing(ASAv、ASA on Firepower)

- ASDM と Firepower Chassis Manager を使用した ASA プラットフォームモードでの展開

高度暗号化ライセンスを有効にするにはどうすればよいですか。
この機能は、FCM登録で使用されたトークンで、[Allow export-controlled functionality on the products registered with this token enabled]オプションがある場合に、自動的に有効になります。

FCMレベルのExport-Controlled FeaturesとASAレベルの関連するEncryption-3DES-AESが無効になっている場合、Strong Encryption License(GES)を有効にするにはどうすればよいですか。
トークンでこのオプションが有効になっていない場合は、FCMの登録を解除し、このオプションが有効になっているトークンに再登録します。

トークンの生成時に、このトークンに登録されている製品に対してエクスポート制御の機能を許可するオプションが使用できない場合は、どうすればよいですか。
シスコアカウントチームにお問い合わせください。

ASAレベルでStrong Encryption機能を設定する必要がありますか。
高度暗号化オプション機能は、FCM がバージョン 2.3.0 より前のサテライトサーバーと統合されている場合のみ必須ですが、これは高度暗号化を設定しなければならないことが想定される状況の 1 つに過ぎません。

FCM とスマートライセンスクラウド間のパスを許可する必要のある IP はどれですか。
FXOSは、アドレスhttps://tools.cisco.com/（ポート443）を使用してライセンスクラウドと通信します。このアドレス https://tools.cisco.com/ は、次の IP アドレスに解決されます。

- 72.163.4.38
- 173.37.145.8

違反エラーが発生するのはなぜですか。
次の状況では、デバイスがコンプライアンスから逸脱している可能性があります。

- 過剰使用（デバイスが使用できないライセンスを使用している）
- ライセンスの期限切れ – 時間ベースのライセンスの期限切れ
- 通信の欠如：デバイスは再認証のためにライセンス認証局に到達できません

お客様のアカウントがコンプライアンス違反の状態になっているか、またはコンプライアンス違反の状態に近づいているかどうかを確認するには、Firepowerのシャーシで現在使用されている権限を、スマートアカウントの権限と比較する必要があります。
コンプライアンス違反の状態では、特別なライセンスを必要とする機能の設定を変更できますが、その他の操作は影響を受けません。たとえば、標準のライセンス制限を超える既存のコンテキストは実行を継続でき、その構成を変更することもできますが、新しいコンテキストを追加することはできません。

ライセンスを追加した後も「Out of Compliance」エラーが表示されるのはなぜですか。
デフォルトでは、デバイスは権限を確認するために、License Authority と 30 日おきに通信します。手動でこの通信を行う場合は、次の手順に従います。

FPR1000 および 2100 プラットフォームでこの手順を実行するには、ASDM か CLI を使用します。

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

FPR4100 および 9300 プラットフォームの場合は、FXOS CLI を使用します。

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

ASA レベルで使用中になっているライセンスがないのはなぜですか。
ASA の権限が ASA レベルで設定されていることを、次のように確認します。

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

ASA 権限を設定したのにライセンスが使用されていない状態になっているのはなぜですか。
この状態になることが考えられるのは、ASA のアクティブ/スタンバイ構成によるフェールオーバーペアを展開し、スタンバイ側のデバイスでライセンスの使用状況を確認した場合です。コンフィギュレーションガイドに従って、設定はスタンバイユニットに複製されますが、スタンバイユニットは設定を使用せず、キャッシュされた状態のままになります。アクティブな装置のみサーバーからライセンスを要求します。ライセンスは単一のフェールオーバーライセンスにまとめられ、フェールオーバーのペアで共有されます。この集約ライセンスはスタンバイ ユニットにもキャッシュされ、将来アクティブなユニットとなったときに使用されます。参考：フェールオーバーまたはASAクラスタライセンス。

FCMがインターネットにアクセスできない場合は、どうすればよいですか。
代替手段として、Cisco Smart Software Manager オンプレミス (旧称 Cisco Smart Software Manager サテライト) を展開する方法があります。CSSM オンプレミスは Cisco Smart Licensing のコンポーネントの 1 つです。クラウドベースの Cisco Smart Software Manager と連携して動作し、ほぼリアルタイムの可視性を提供し、購入および使用するシスコライセンスの機能をレポートします。またセキュリティに厳格な組織にとっては、ダイレクトインターネット接続を使用することなく、インストールベースを管理するために Cisco SSM の機能のサブセットにアクセスする手段を得られます。

Cisco Smart Software Manager On-Premの詳細はどこで確認できますか。
FXOS コンフィギュレーション ガイドで詳細情報を提供しています。

- Firepower 4100/9300 シャーシのスマート ライセンス サテライト サーバの設定
- Smart Software Manager オンプレミスへの Firepower Chassis Manager 登録の設定

関連情報

- Cisco ASA シリーズ CLI コンフィギュレーション ガイド (一般的な操作)
- ASA のライセンス管理
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。