Risoluzione dei problemi di ASA Smart License sugli appliance FXOS Firepower

Sommario

Introduzione

In questo documento viene descritta la funzionalità Smart Licensing di Adaptive Security Appliance (ASA) su Firepower eXtensible Operating System (FXOS).

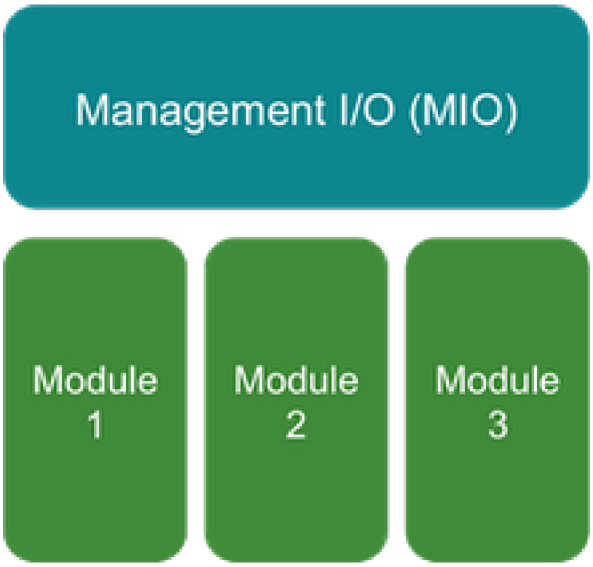
Premesse

Smart Licensing su FXOS viene usato quando sullo chassis è installata un'appliance ASA. Per Firepower Threat Defense (FTD) e Firepower Management Center (FMC), Smart Licensing controlla FMC e FTD Smart License Registration and Troubleshooting.

Questo documento descrive principalmente gli scenari in cui lo chassis FXOS ha accesso diretto a Internet. Se lo chassis FXOS non è in grado di accedere a Internet, è necessario prendere in considerazione un Satellite Server o una prenotazione permanente delle licenze (PLR). Per ulteriori dettagli sulla gestione offline, consultare la guida alla configurazione di FXOS.

Architettura di Smart Licensing

Panoramica generale dei componenti dello chassis:

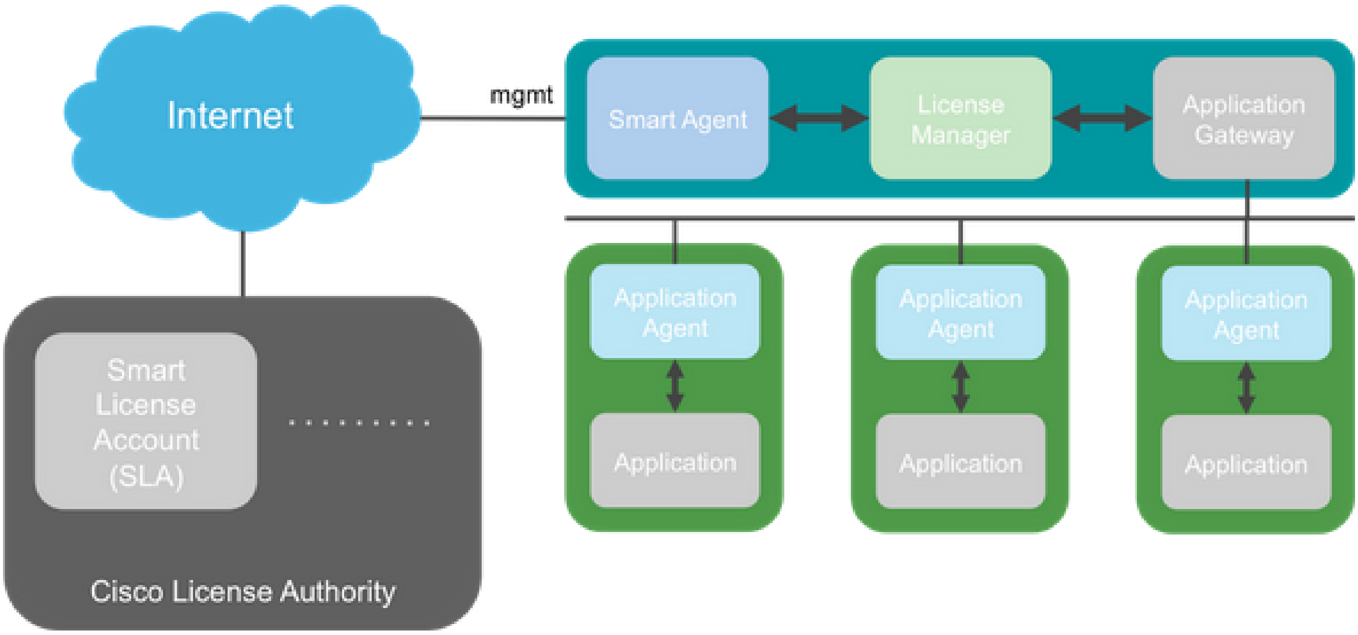


- Sia il modulo di input/output di gestione (MIO) che i singoli moduli svolgono un ruolo in Smart Licensing
- MIO non richiede alcuna licenza per il suo funzionamento
- Le applicazioni SA in ogni modulo devono essere concesse in licenza

Il supervisore FXOS è MIO. La MIO contiene tre componenti principali:

- Smart Agent
- Gestione licenze
- AppAG

Architettura generale



Nomenclatura

Termine	Descrizione

Cisco License Authority	Il back-end delle licenze Cisco per Smart Licensing. Gestisce tutte le informazioni relative alle licenze dei prodotti. Ciò include diritti e informazioni sui dispositivi.
Account Smart License	Account che dispone di tutti i diritti per l'accessorio.
ID token	Quando l'accessorio è registrato, viene utilizzato un identificatore per distinguere lo Smart License Account.
Diritto	Equivalente a una licenza. Corrisponde a una singola feature o a un intero livello di feature.
Chiave di attivazione del prodotto (PAK)	Il vecchio meccanismo di licenza. Legato a un singolo accessorio.

Stati di Smart Agent

State	Descrizione
Non configurato	Le licenze intelligenti non sono abilitate.
Non identificato	Le licenze Smart sono state abilitate, ma Smart Agent non ha ancora contattato Cisco per la registrazione.
Registrato	L'agente ha contattato l'autorità per le licenze Cisco e ha effettuato la registrazione.
Autorizzato	Quando un agente riceve uno stato di non conformità in risposta a una richiesta di autorizzazione dei diritti.
Non conforme (OOC)	Quando un agente riceve uno stato OOC in risposta a una richiesta di autorizzazione di adesione.
Autorizzazione scaduta	Se l'agente non comunica con Cisco da 90 giorni.

Diritti ASA

Di seguito sono riportati i diritti ASA supportati:

- Livello standard
- Contesto multiplo
- Crittografia avanzata (3DES)
- GTP (Mobile/Service Provider)

Configurazione

Seguire le istruzioni riportate nei seguenti documenti:

- Smart Software Licensing (ASAv, ASA su Firepower)
- Gestione delle licenze per l'appliance ASA

Prima di qualsiasi configurazione a livello di funzionalità:

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

Configura livello standard:

```
asa(config)# license smart
INFO: License(s) corresponding to an entitlement will be activated only after an entitlement
request has been authorized.
asa(config-smart-lic)# feature tier standard
asa(config-smart-lic)# show license all

Smart licensing enabled: Yes

Compliance status: In compliance

Overall licensed status: Authorized (3)

Entitlement(s):

Feature tier:
Tag: regid.2015-10.com.cisco.FIREPOWER_4100_ASA_STANDARD,1.0_7d7f5ee2-1398-4b0e-aced-
b3f7fb1cacfc
Version: 1.0
Enforcement mode: Authorized
Handle: 1
Requested time: Tue, 04 Aug 2020 07:58:13 UTC
Requested count: 1
Request status: Complete
```

```
Serial Number: FCH12345ABC

License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces : Unlimited
Maximum VLANs : 1024
Inside Hosts : Unlimited
Failover : Active/Active
Encryption-DES : Enabled
Encryption-3DES-AES : Enabled
Security Contexts : 10
Carrier : Disabled
AnyConnect Premium Peers : 20000
AnyConnect Essentials : Disabled
Other VPN Peers : 20000
Total VPN Peers : 20000
AnyConnect for Mobile : Enabled
AnyConnect for Cisco VPN Phone : Enabled
Advanced Endpoint Assessment : Enabled
Shared License : Disabled
Total TLS Proxy Sessions : 15000
Clustetext
```

Failover (alta disponibilità)

Come documentato nella guida alla configurazione dell'ASA, ciascuna unità Firepower deve essere registrata presso l'autorità di licenza o il server satellite. Verifica dalla CLI dell'ASA:

```
asa# show failover | include host
        This host: Primary - Active
       Other host: Secondary - Standby Ready

asa# show license all

Smart licensing enabled: Yes

Compliance status: In compliance

Overall licensed status: Authorized (3)

Entitlement(s):

Feature tier:
       Tag: regid.2015-10.com.cisco.FIREPOWER_4100_ASA_STANDARD,1.0_7d7f5ee2-1398-4b0e-aced-
b3f7fb1cacfc
       Version: 1.0
       Enforcement mode: Authorized
       Handle: 1
       Requested time: Tue, 04 Aug 2020 07:58:13 UTC
       Requested count: 1
       Request status: Complete

Serial Number:  FCH12345ABC

License mode: Smart Licensing

Licensed features for this platform:
```

```
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 1024
Inside Hosts                      : Unlimited
Failover                          : Active/Active
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Enabled
Security Contexts                 : 10
Carrier                           : Disabled
AnyConnect Premium Peers          : 20000
AnyConnect Essentials             : Disabled
Other VPN Peers                   : 20000
Total VPN Peers                   : 20000
AnyConnect for Mobile             : Enabled
AnyConnect for Cisco VPN Phone    : Enabled
Advanced Endpoint Assessment      : Enabled
Shared License                    : Disabled
Total TLS Proxy Sessions          : 15000
Cluster                           : Enabled

Failover cluster licensed features for this platform:
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 1024
Inside Hosts                      : Unlimited
Failover                          : Active/Active
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Enabled
Security Contexts                 : 20
Carrier                           : Disabled
AnyConnect Premium Peers          : 20000
AnyConnect Essentials             : Disabled
Other VPN Peers                   : 20000
Total VPN Peers                   : 20000
AnyConnect for Mobile             : Enabled
AnyConnect for Cisco VPN Phone    : Enabled
Advanced Endpoint Assessment      : Enabled
Shared License                    : Disabled
Total TLS Proxy Sessions          : 15000
Cluster                           : Enabled
```

L'unità di standby:

```
asa# show failover | i host
       This host: Secondary - Standby Ready
       Other host: Primary - Active

asa# show license all

Smart licensing enabled: Yes

Compliance status: In compliance

Overall licensed status: Not applicable in standby state

No entitlements in use

Serial Number:  FCH12455DEF

License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 1024
Inside Hosts                      : Unlimited
Failover                          : Active/Active
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Disabled
Security Contexts                 : 10
Carrier                           : Disabled
AnyConnect Premium Peers          : 20000
AnyConnect Essentials             : Disabled
Other VPN Peers                   : 20000
Total VPN Peers                   : 20000
AnyConnect for Mobile             : Enabled
AnyConnect for Cisco VPN Phone    : Enabled
Advanced Endpoint Assessment      : Enabled
Shared License                    : Disabled
Total TLS Proxy Sessions          : 15000
Cluster                           : Enabled

Failover cluster licensed features for this platform:
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 1024
Inside Hosts                      : Unlimited
Failover                          : Active/Active
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Enabled
Security Contexts                 : 20
Carrier                           : Disabled
AnyConnect Premium Peers          : 20000
AnyConnect Essentials             : Disabled
Other VPN Peers                   : 20000
Total VPN Peers                   : 20000
AnyConnect for Mobile             : Enabled
AnyConnect for Cisco VPN Phone    : Enabled
Advanced Endpoint Assessment      : Enabled
Shared License                    : Disabled
Total TLS Proxy Sessions          : 15000
Cluster                           : Enabled
```

Caso di studio: licenza ASA HA su FP2100

- Sul modello 2100, l'ASA comunica con il portale Cisco Smart Licensing (cloud) tramite le interfacce ASA, non tramite la gestione FXOS
- Ènecessario registrare entrambe le appliance ASA sul portale Cisco Smart Licensing (cloud)

In questo caso, l'autenticazione locale HTTP viene utilizzata su un'interfaccia esterna:

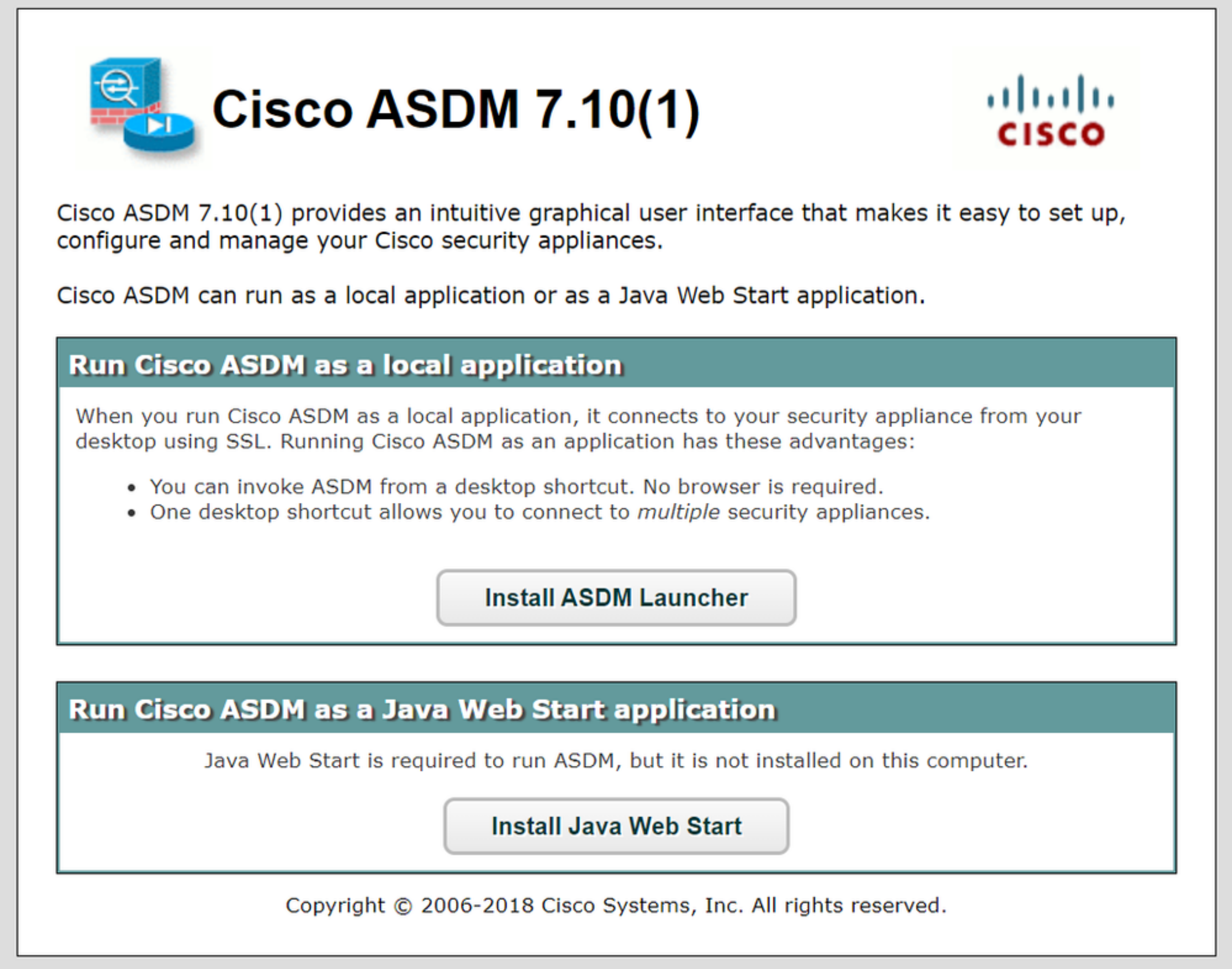
```
ciscoasa(config)# show run http
http server enable
http 0.0.0.0 0.0.0.0 outside
ciscoasa(config)# show run aaa
aaa authentication http console LOCAL
ciscoasa(config)# show run username
username cisco password ***** pbkdf2
```

Èpossibile connettersi all'appliance ASA solo tramite ASDM se è stata abilitata una licenza 3DES/AES. Per un'ASA non ancora registrata, questa operazione è possibile solo su un'interfaccia management-only. In base alla guida alla configurazione: "La crittografia avanzata (3DES/AES) è disponibile per le connessioni di gestione prima della connessione all'autorità di licenza o al server satellite, in modo da poter avviare ASDM. L'accesso ASDM è disponibile solo sulle interfacce di sola gestione con crittografia predefinita. Il traffico diretto non è consentito fino a quando non ci si connette e non si ottiene la licenza "Strong Encryption". In un caso diverso si ottiene:

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

Per risolvere il problema, sull'interfaccia con connessione Internet è stata configurata solo la gestione dell'ASA, quindi è possibile la connessione ASDM:

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



Cisco ASDM 7.10(1)

Cisco ASDM 7.10(1) provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco security appliances.

Cisco ASDM can run as a local application or as a Java Web Start application.

Run Cisco ASDM as a local application

When you run Cisco ASDM as a local application, it connects to your security appliance from your desktop using SSL. Running Cisco ASDM as an application has these advantages:

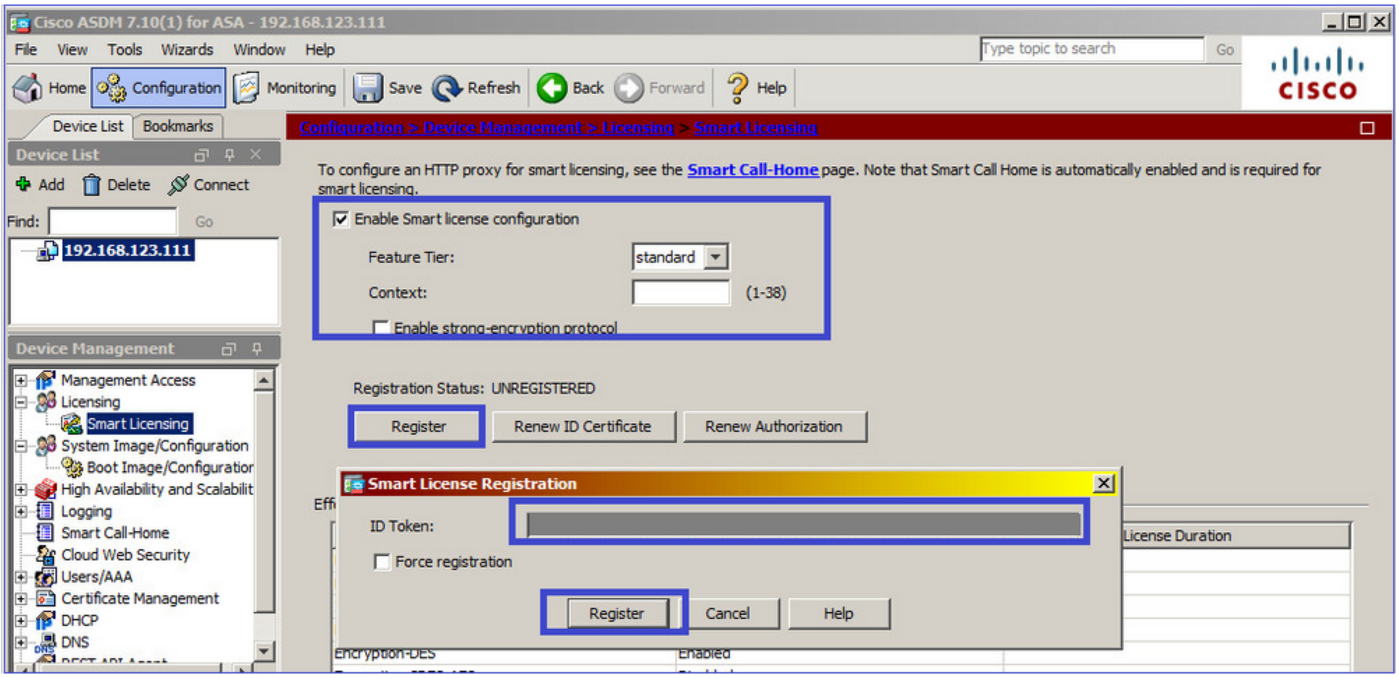
- You can invoke ASDM from a desktop shortcut. No browser is required.
- One desktop shortcut allows you to connect to *multiple* security appliances.

Run Cisco ASDM as a Java Web Start application

Java Web Start is required to run ASDM, but it is not installed on this computer.

Copyright © 2006-2018 Cisco Systems, Inc. All rights reserved.

Configurare Smart Licensing sull'appliance ASA primaria:



To configure an HTTP proxy for smart licensing, see the Smart Call-Home page. Note that Smart Call Home is automatically enabled and is required for smart licensing.

☑ Enable Smart license configuration

Feature Tier: standard

Context: (1-38)

□ Enable strong-encryption protocol

Registration Status: UNREGISTERED

Register | Renew ID Certificate | Renew Authorization

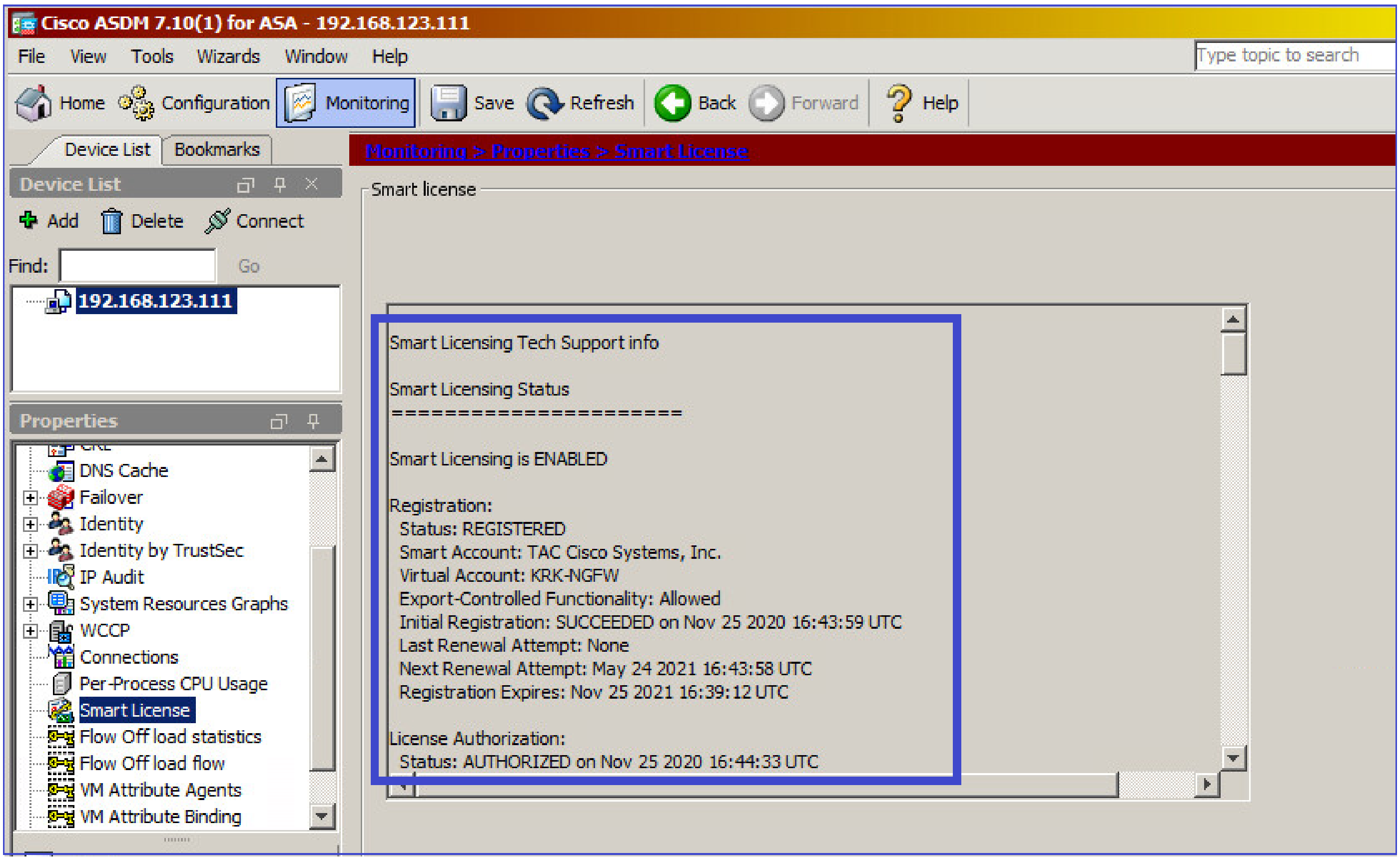
Smart License Registration

ID Token:

□ Force registration

Register | Cancel | Help

Passa a **Monitoring > Properties > Smart License** per controllare lo stato della registrazione:



```
Smart Licensing Tech Support info

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

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: TAC Cisco Systems, Inc.
  Virtual Account: KRK-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 16:44:33 UTC
```

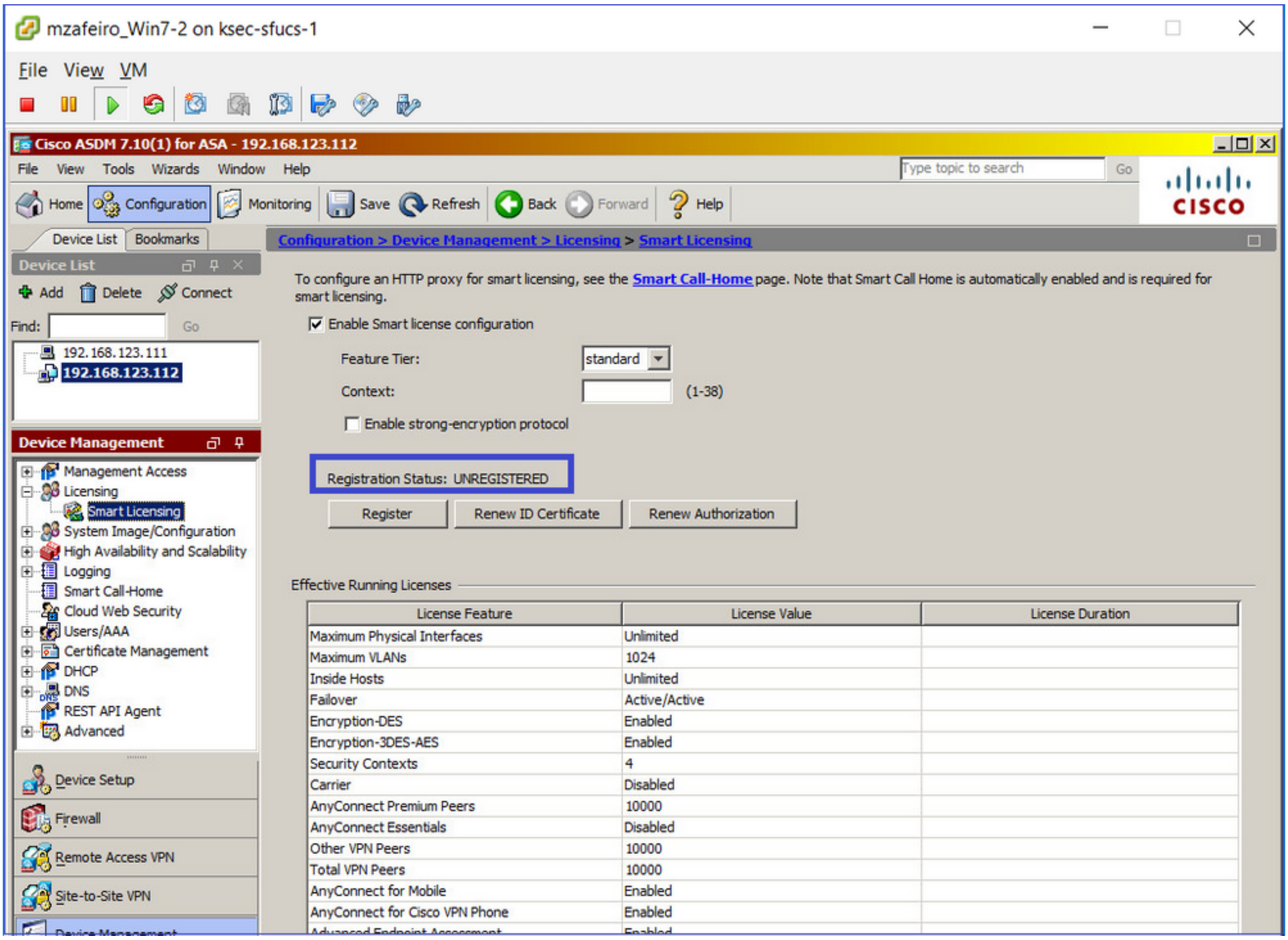
Verifica CLI ASA principale:

```
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
```

Collegare l'appliance ASA in standby tramite ASDM (ciò è possibile solo se l'ASA è stata configurata con un IP in standby). L'ASA di standby viene visualizzata come UNREGISTERED poiché non è ancora stato registrato sul portale di Smart Licensing:



To configure an HTTP proxy for smart licensing, see the Smart Call-Home page. Note that Smart Call Home is automatically enabled and is required for smart licensing.

☑ Enable Smart license configuration

Feature Tier: standard

Context: (1-38)

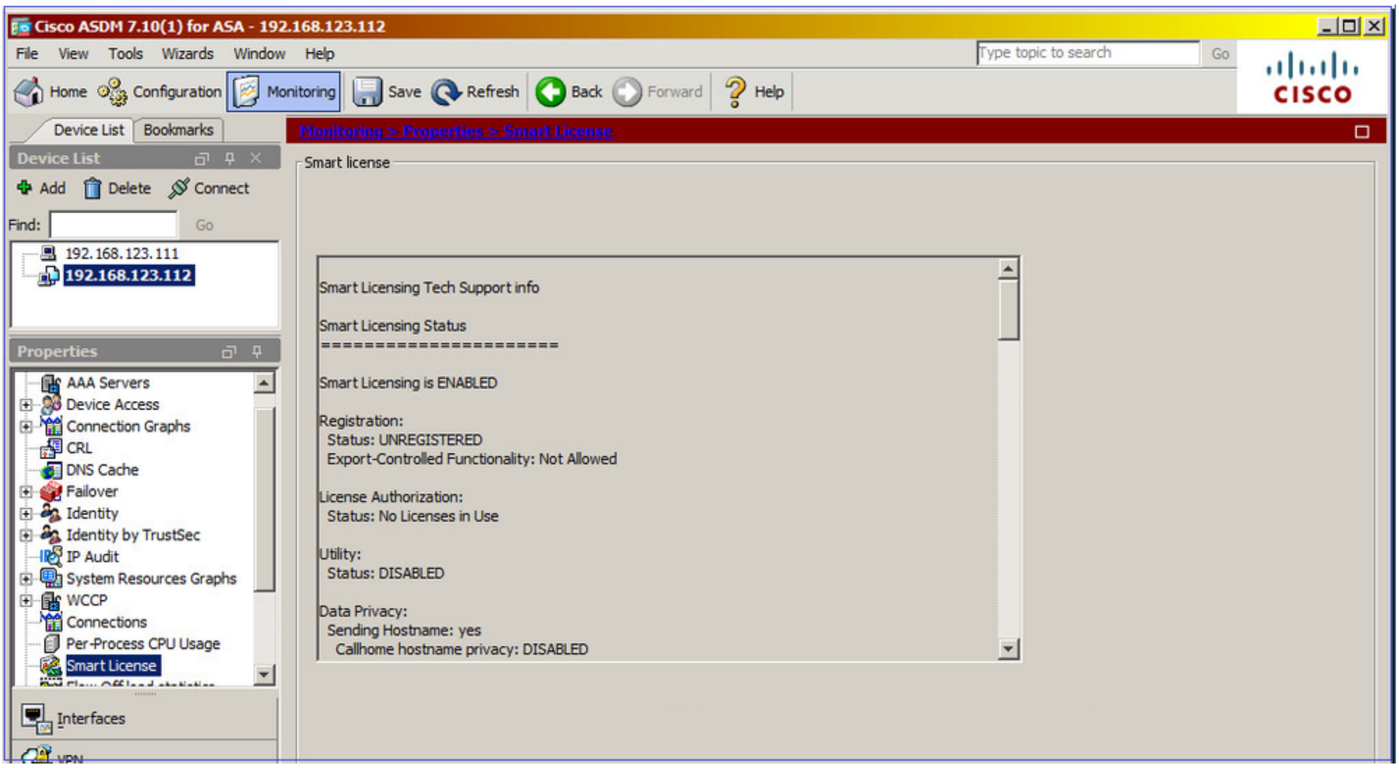
□ Enable strong-encryption protocol

Registration Status: UNREGISTERED

Register | Renew ID Certificate | Renew Authorization

Effective Running Licenses

License Feature	License Value	License Duration
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	



```
Smart Licensing Tech Support info

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
```

La CLI dell'ASA in standby mostra:

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

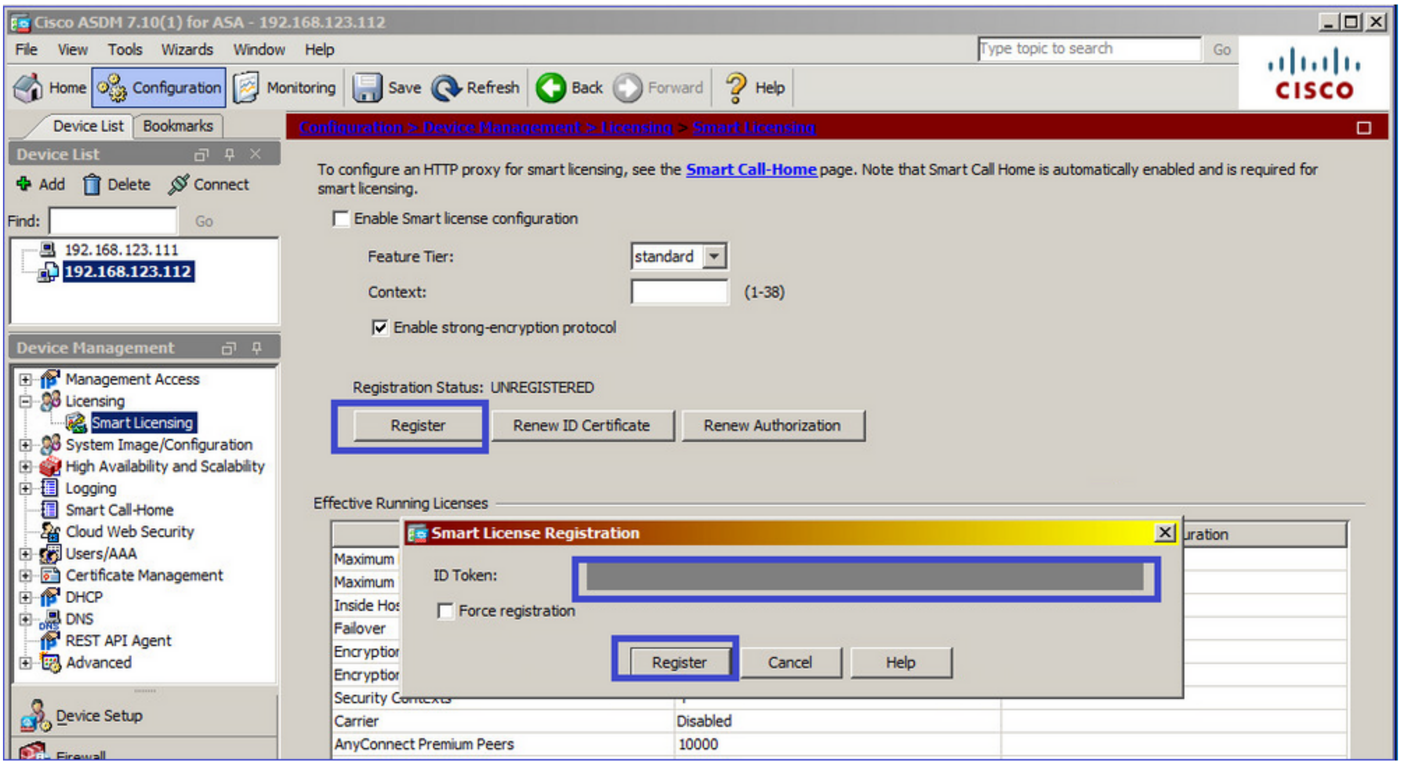
```
Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
Status: UNREGISTERED
Export-Controlled Functionality: Not Allowed

License Authorization:
Status: No Licenses in Use

Utility:
Status: DISABLED

Data Privacy:
Sending Hostname: yes
Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
Type: Callhome

License Usage
==============

No licenses in use

Product Information
===================
UDI: PID:FPR-2140,SN:JAD123456A

Agent Version
=============
Smart Agent for Licensing: 4.3.6_rel/38
ciscoasa/sec/stby# show run license
license smart
feature tier standard
```

Le funzionalità della licenza sono abilitate sull'appliance ASA in standby:

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

License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces : Unlimited
Maximum VLANs : 1024
Inside Hosts : Unlimited
Failover : Active/Active
Encryption-DES : Enabled
Encryption-3DES-AES : Disabled
Security Contexts : 2
Carrier : Disabled
AnyConnect Premium Peers : 10000
AnyConnect Essentials : Disabled
Other VPN Peers : 10000
Total VPN Peers : 10000
```

```
AnyConnect for Mobile : Enabled
AnyConnect for Cisco VPN Phone : Enabled
Advanced Endpoint Assessment : Enabled
Shared License : Disabled
Total TLS Proxy Sessions : 10000
Cluster : Disabled


Failover cluster licensed features for this platform:
Maximum Physical Interfaces : Unlimited
Maximum VLANs : 1024
Inside Hosts : Unlimited
Failover : Active/Active
Encryption-DES : Enabled
Encryption-3DES-AES : Enabled
Security Contexts : 4
Carrier : Disabled
AnyConnect Premium Peers : 10000
AnyConnect Essentials : Disabled
Other VPN Peers : 10000
Total VPN Peers : 10000
AnyConnect for Mobile : Enabled
AnyConnect for Cisco VPN Phone : Enabled
Advanced Endpoint Assessment : Enabled
Shared License : Disabled
Total TLS Proxy Sessions : 10000
Cluster : Disabled
```

Registrare l'appliance ASA in standby:



Configuration > Device Management > Licensing > Smart Licensing

To configure an HTTP proxy for smart licensing, see the Smart Call-Home page. Note that Smart Call Home is automatically enabled and is required for smart licensing.

□ Enable Smart license configuration

Feature Tier: standard

Context: (1-38)

☑ Enable strong-encryption protocol

Registration Status: UNREGISTERED

Register | Renew ID Certificate | Renew Authorization

Effective Running Licenses

Smart License Registration

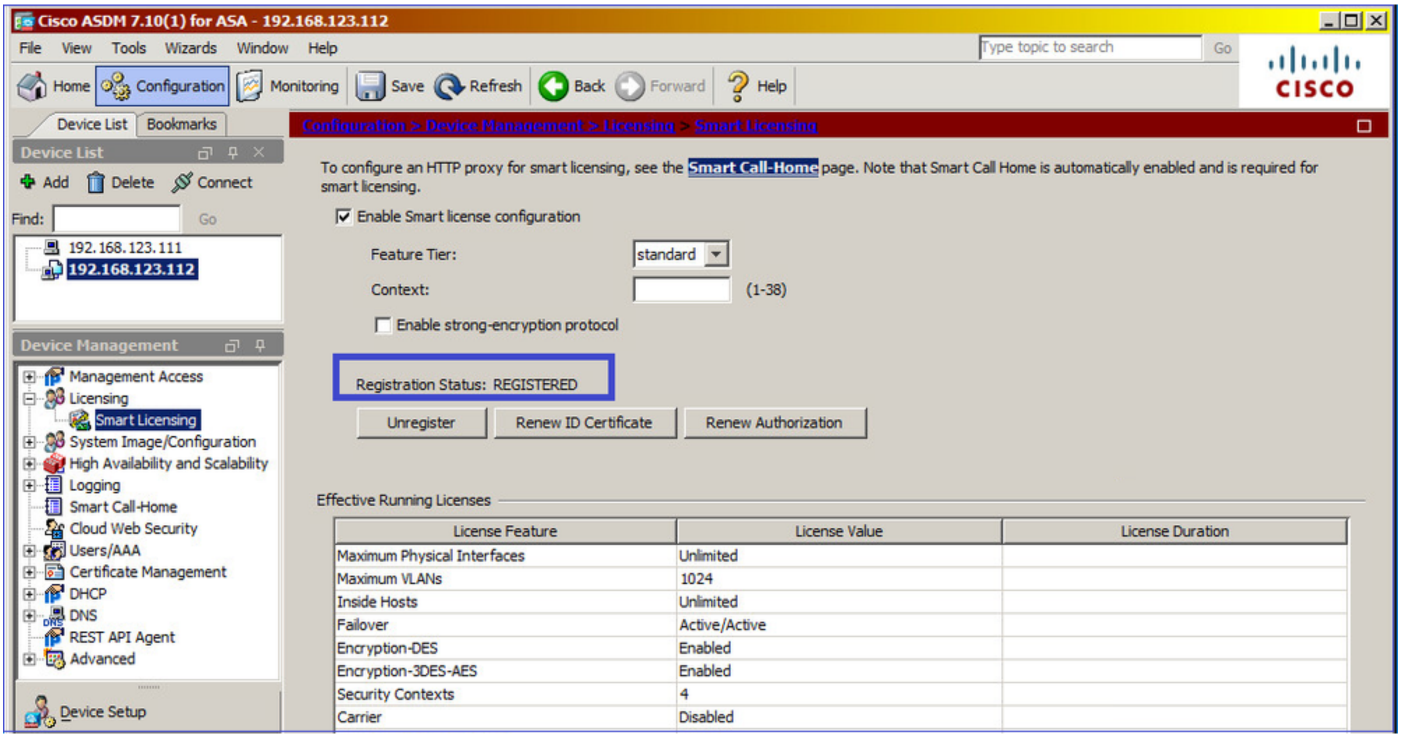
ID Token: [redacted]

□ Force registration

Register | Cancel | Help

		uration
Maximum		
Maximum		
Inside Hos		
Failover		
Encryption		
Encryption		
Security Contexts		
Carrier	Disabled	
AnyConnect Premium Peers	10000	

Il risultato sull'appliance ASA in standby è che è REGISTERED:



To configure an HTTP proxy for smart licensing, see the Smart Call-Home page. Note that Smart Call Home is automatically enabled and is required for smart licensing.

☑ Enable Smart license configuration

Feature Tier: standard

Context: (1-38)

□ Enable strong-encryption protocol

Registration Status: REGISTERED

Effective Running Licenses

License Feature	License Value	License Duration
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	

Verifica CLI su ASA in standby:

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

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

Smart Licensing is ENABLED

Registration:
Status: REGISTERED
Smart Account: Cisco Systems, Inc.
Virtual Account: NGFW
Export-Controlled Functionality: Allowed
Initial Registration: SUCCEEDED on Nov 25 2020 17:06:51 UTC
Last Renewal Attempt: None
Next Renewal Attempt: May 24 2021 17:06:51 UTC
Registration Expires: Nov 25 2021 17:01:47 UTC

License Authorization:
Status: AUTHORIZED on Nov 25 2020 17:07:28 UTC
Last Communication Attempt: SUCCEEDED on Nov 25 2020 17:07:28 UTC
Next Communication Attempt: Dec 25 2020 17:07:28 UTC
Communication Deadline: Feb 23 2021 17:02:15 UTC

Utility:
Status: DISABLED

Data Privacy:
Sending Hostname: yes
Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
Type: Callhome
```

```
License Usage
==============

No licenses in use

Product Information
===================
UDI: PID:FPR-2140,SN:JAD123456AX

Agent Version
=============
Smart Agent for Licensing: 4.3.6_rel/38

ciscoasa/sec/stby# show license feature
Serial Number: JAD123456A
Export Compliant: YES

License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces : Unlimited
Maximum VLANs : 1024
Inside Hosts : Unlimited
Failover : Active/Active
Encryption-DES : Enabled
Encryption-3DES-AES : Enabled
Security Contexts : 2
Carrier : Disabled
AnyConnect Premium Peers : 10000
AnyConnect Essentials : Disabled
Other VPN Peers : 10000
Total VPN Peers : 10000
AnyConnect for Mobile : Enabled
AnyConnect for Cisco VPN Phone : Enabled
Advanced Endpoint Assessment : Enabled
Shared License : Disabled
Total TLS Proxy Sessions : 10000
Cluster : Disabled


Failover cluster licensed features for this platform:
Maximum Physical Interfaces : Unlimited
Maximum VLANs : 1024
Inside Hosts : Unlimited
Failover : Active/Active
Encryption-DES : Enabled
Encryption-3DES-AES : Enabled
Security Contexts : 4
Carrier : Disabled
AnyConnect Premium Peers : 10000
AnyConnect Essentials : Disabled
Other VPN Peers : 10000
Total VPN Peers : 10000
AnyConnect for Mobile : Enabled
AnyConnect for Cisco VPN Phone : Enabled
Advanced Endpoint Assessment : Enabled
Shared License : Disabled
Total TLS Proxy Sessions : 10000
Cluster : Disabled
```

Cluster ASA

Se le licenze dei dispositivi non corrispondono, il cluster non è formato:

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

Configurazione cluster completata:

```
asa(config)# cluster group GROUP1
asa(cfg-cluster)# enable
Removed all entitlements except per-unit entitlement configuration before joining cluster as
data unit.

Detected Cluster Control Node.
Beginning configuration replication from Control Node.
.
Cryptochecksum (changed): ede485ad d7fb9644 2847deaf ba16830b
End configuration replication from Control Node.
```

Nodo di controllo cluster:

```
asa# show cluster info | i state
   This is "unit-1-1" in state CONTROL_NODE
   Unit "unit-2-1" in state DATA_NODE

asa# show license all

Smart licensing enabled: Yes

Compliance status: In compliance

Overall licensed status: Authorized (3)

Entitlement(s):

Feature tier:
       Tag: regid.2015-10.com.cisco.FIREPOWER_4100_ASA_STANDARD,1.0_7d7f5ee2-1398-4b0e-aced-
b3f7fb1cacfc
       Version: 1.0
       Enforcement mode: Authorized
       Handle: 2
       Requested time: Mon, 10 Aug 2020 08:12:38 UTC
       Requested count: 1
       Request status: Complete

Serial Number:  FCH12345ABC

License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 1024
Inside Hosts                      : Unlimited
Failover                          : Active/Active
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Enabled
```

```
Security Contexts                 : 10
Carrier                           : Disabled
AnyConnect Premium Peers          : 20000
AnyConnect Essentials             : Disabled
Other VPN Peers                   : 20000
Total VPN Peers                   : 20000
AnyConnect for Mobile             : Enabled
AnyConnect for Cisco VPN Phone    : Enabled
Advanced Endpoint Assessment      : Enabled
Shared License                    : Disabled
Total TLS Proxy Sessions          : 15000
Cluster                           : Enabled

Failover cluster licensed features for this platform:
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 1024
Inside Hosts                      : Unlimited
Failover                          : Active/Active
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Enabled
Security Contexts                 : 20
Carrier                           : Disabled
AnyConnect Premium Peers          : 20000
AnyConnect Essentials             : Disabled
Other VPN Peers                   : 20000
Total VPN Peers                   : 20000
AnyConnect for Mobile             : Enabled
AnyConnect for Cisco VPN Phone    : Enabled
Advanced Endpoint Assessment      : Enabled
Shared License                    : Disabled
Total TLS Proxy Sessions          : 15000
Cluster                           : Enabled
```

Unità dati cluster:

```
asa# show cluster info | i state
   This is "unit-2-1" in state DATA_NODE
   Unit "unit-1-1" in state CONTROL_NODE

asa# show license all

Smart licensing enabled: Yes

Compliance status: In compliance

Overall licensed status: Authorized (3)

Entitlement(s):

Strong encryption:
       Tag: regid.2015-10.com.cisco.FIREPOWER_4100_ASA_ENCRYPTION,1.0_052986db-c5ad-40da-97b1-
ee0438d3b2c9
       Version: 1.0
       Enforcement mode: Authorized
       Handle: 3
       Requested time: Mon, 10 Aug 2020 07:29:45 UTC
       Requested count: 1
       Request status: Complete

Serial Number:  FCH12345A6B
```

```
License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 1024
Inside Hosts                      : Unlimited
Failover                          : Active/Active
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Enabled
Security Contexts                 : 10
Carrier                           : Disabled
AnyConnect Premium Peers          : 20000
AnyConnect Essentials             : Disabled
Other VPN Peers                   : 20000
Total VPN Peers                   : 20000
AnyConnect for Mobile             : Enabled
AnyConnect for Cisco VPN Phone    : Enabled
Advanced Endpoint Assessment      : Enabled
Shared License                    : Disabled
Total TLS Proxy Sessions          : 15000
Cluster                           : Enabled

Failover cluster licensed features for this platform:
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 1024
Inside Hosts                      : Unlimited
Failover                          : Active/Active
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Enabled
Security Contexts                 : 20
Carrier                           : Disabled
AnyConnect Premium Peers          : 20000
AnyConnect Essentials             : Disabled
Other VPN Peers                   : 20000
Total VPN Peers                   : 20000
AnyConnect for Mobile             : Enabled
AnyConnect for Cisco VPN Phone    : Enabled
Advanced Endpoint Assessment      : Enabled
Shared License                    : Disabled
Total TLS Proxy Sessions          : 15000
Cluster                           : Enabled
```

Verifica e debug

Riepilogo dei comandi di verifica per lo chassis (MIO):

```
FPR4125# show license all
FPR4125# show license techsupport
FPR4125# scope monitoring
FPR4125 /monitoring # scope callhome
FPR4125 /monitoring/callhome # show expand
FPR4125# scope system
FPR4125 /system # scope services
FPR4125 /system/services # show dns
FPR4125 /system/services # show ntp-server
FPR4125# scope security
FPR4125 /security # show trustpoint
FPR4125# show clock
```

```
FPR4125# show timezone
FPR4125# show license usage
```

Verifica della configurazione:

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

Riepilogo dei comandi di verifica ASA:

```
asa# show run license
asa# show license all
asa# show license entitlement
asa# show license features
asa# show tech-support license
asa# debug license 255
```

Output di esempio dei comandi di verifica dello chassis (MIO)

```
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
```

Output di esempio dei comandi di verifica dell'ASA

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

asa# show license all

Smart licensing enabled: Yes

Compliance status: In compliance

Overall licensed status: Authorized (3)

Entitlement(s):

Feature tier:
       Tag: regid.2015-10.com.cisco.FIREPOWER_4100_ASA_STANDARD,1.0_7d7f5ee2-1398-4b0e-aced-
b3f7fb1cacfc
       Version: 1.0
       Enforcement mode: Authorized
       Handle: 1
       Requested time: Tue, 04 Aug 2020 07:58:13 UTC
       Requested count: 1
       Request status: Complete

Serial Number:  FCH12345ABC
```

```
License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 1024
Inside Hosts                      : Unlimited
Failover                          : Active/Active
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Enabled
Security Contexts                 : 10
Carrier                           : Disabled
AnyConnect Premium Peers          : 20000
AnyConnect Essentials             : Disabled
Other VPN Peers                   : 20000
Total VPN Peers                   : 20000
AnyConnect for Mobile             : Enabled
AnyConnect for Cisco VPN Phone    : Enabled
Advanced Endpoint Assessment      : Enabled
Shared License                    : Disabled
Total TLS Proxy Sessions          : 15000
Cluster                           : Enabled

asa# show license entitlement

Entitlement(s):

Feature tier:
       Tag: regid.2015-10.com.cisco.FIREPOWER_4100_ASA_STANDARD,1.0_7d7f5ee2-1398-4b0e-aced-
b3f7fb1cacfc
       Version: 1.0
       Enforcement mode: Authorized
       Handle: 1
       Requested time: Tue, 04 Aug 2020 07:58:13 UTC
       Requested count: 1
       Request status: Complete

asa# show license features
Serial Number:  FCH12345ABC

License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 1024
Inside Hosts                      : Unlimited
Failover                          : Active/Active
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Enabled
Security Contexts                 : 10
Carrier                           : Disabled
AnyConnect Premium Peers          : 20000
AnyConnect Essentials             : Disabled
Other VPN Peers                   : 20000
Total VPN Peers                   : 20000
AnyConnect for Mobile             : Enabled
AnyConnect for Cisco VPN Phone    : Enabled
Advanced Endpoint Assessment      : Enabled
Shared License                    : Disabled
Total TLS Proxy Sessions          : 15000
Cluster                           : Enabled

asa#  show tech-support license
```

```
Smart licensing enabled: Yes

Compliance status: In compliance

Overall licensed status: Authorized (3)

Entitlement(s):

Feature tier:
       Tag: regid.2015-10.com.cisco.FIREPOWER_4100_ASA_STANDARD,1.0_7d7f5ee2-1398-4b0e-aced-
b3f7fb1cacfc
       Version: 1.0
       Enforcement mode: Authorized
       Handle: 1
       Requested time: Tue, 04 Aug 2020 07:58:13 UTC
       Requested count: 1
       Request status: Complete
```

Registrazione completata

L'output viene generato dall'interfaccia utente di gestione dello chassis:

```
Smart Licensing is ENABLED

Utility:
Status: DISABLED

Data Privacy:
Sending Hostname: yes
Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
Type: Callhome

Registration:
Status: REGISTERED
Smart Account: TAC Cisco Systems, Inc.
Virtual Account: EU TAC
Export-Controlled Functionality: ALLOWED
Initial Registration: SUCCEEDED on Dec 10 2018 23:30:02 UTC
Last Renewal Attempt: SUCCEEDED on Mar 12 2020 23:16:11 UTC
Next Renewal Attempt: Sep 08 2020 23:16:10 UTC
Registration Expires: Mar 12 2021 23:11:09 UTC

License Authorization:
Status: AUTHORIZED on Jul 05 2020 17:49:15 UTC
Last Communication Attempt: SUCCEEDED on Jul 05 2020 17:49:15 UTC
Next Communication Attempt: Aug 04 2020 17:49:14 UTC
Communication Deadline: Oct 03 2020 17:44:13 UTC

License Conversion:
Automatic Conversion Enabled: True
Status: Not started

Export Authorization Key:
Features Authorized:
<none>

Cisco Success Network: DISABLED
```

Autorizzazione scaduta

L'output viene generato dall'interfaccia utente del gestore dello chassis:

```
Smart Licensing is ENABLED

Utility:
Status: DISABLED

Data Privacy:
Sending Hostname: yes
Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
Type: Callhome

Registration:
Status: REGISTERED
Smart Account: Cisco SVS temp - request access through licensing@cisco.com
Virtual Account: Sample Account
Export-Controlled Functionality: ALLOWED
Initial Registration: SUCCEEDED on Nov 22 2019 08:17:30 UTC
Last Renewal Attempt: FAILED on Aug 04 2020 07:32:08 UTC
Failure reason: Agent received a failure status in a response message. Please check the Agent
log file for the detailed message.
Next Renewal Attempt: Aug 04 2020 08:33:48 UTC
Registration Expires: Nov 21 2020 08:12:20 UTC

License Authorization:
Status: AUTH EXPIRED on Aug 04 2020 07:10:16 UTC
Last Communication Attempt: FAILED on Aug 04 2020 07:10:16 UTC
Failure reason: Data and signature do not match
Next Communication Attempt: Aug 04 2020 08:10:14 UTC
Communication Deadline: DEADLINE EXCEEDED

License Conversion:
Automatic Conversion Enabled: True
Status: Not started

Export Authorization Key:
Features Authorized:
<none>

Last Configuration Error
=========================
Command : register idtoken
ZDA2MjFlODktYjllMS00NjQwLTk0MmUtYmVkYWU2NzIyZjYwLTE1ODIxODY2%0AMzEwODV8K2RWVTNURGFIK0tDYUhOSjg3b
jFsdytwbU1SUi81N20rQTVPN2lT%0AdEtvYz0%3D%0A
Error : Smart Agent already registered

Cisco Success Network: DISABLED
```

Output di esempio dalla CLI dello chassis

UNREGISTERED

```
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
```

Registrazione in corso

```
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
```

Errore di registrazione

```
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
```

Periodo di valutazione

```
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
```

Problemi di licenza comuni sullo chassis FXOS (MIO)

Errore di registrazione: token non valido

```
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%0ANDk0NjR8NkJJdWZpQzRDbmtPR0xBWlVpUzZqMjlySnl5QUczT2M0YVVI
vcmxm%0ATGczND0%3D%0B' is not valid."]}
```

Fasi consigliate

1. Verificare se l'URL del servizio di call-home punta a CSM.
2. Accedere al CSM e verificare se il token è stato generato da lì o se è scaduto.

Errore di registrazione: prodotto già registrato

```
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."]}
```

Fasi consigliate

1. Accedere al modulo CSM.
2. Controllare la Product Instances in TUTTI gli account virtuali.
3. Individuare la vecchia istanza di registrazione in base al numero di serie e rimuoverla.
4. Il problema potrebbe essere causato dai due motivi seguenti: Errore durante il rinnovo automatico quando l'ora e la data non sono configurate correttamente, ad esempio non è configurato alcun server NTP.Ordine errato delle operazioni quando si passa da un Satellite a un Server di Produzione, ad esempio, modificare prima l'URL e poi eseguire il comando 'deregistration' (Annulla registrazione)

Errore di registrazione: offset data oltre il limite

```
FPR4125-1# show license all

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

Smart Licensing is ENABLED

Registration:
 Status: UNREGISTERED - REGISTRATION FAILED
 Export-Controlled Functionality: Not Allowed
 Initial Registration: FAILED on Aug 07 01:30:00 2020 UTC
Failure reason: {"timestamp":["The device date '1453329321505' is offset beyond the allowed
tolerance limit."]}
```

Passaggio consigliato

Controllare la configurazione data/ora per assicurarsi che sia configurato un server NTP.

Errore di registrazione: impossibile risolvere l'host

```
FPR4125-1# show license all

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

Smart Licensing is ENABLED

Registration:
 Status: REGISTERING - REGISTRATION IN PROGRESS
 Export-Controlled Functionality: NOT ALLOWED
 Initial Registration: FAILED on Aug 07 2020 06:58:46 UTC
   Failure reason: Failed to resolve host
 Next Registration Attempt: Aug 07 2020 07:16:42 UTC
```

```
Registration Error: Failed to resolve host
```

Fasi consigliate

1. Verificare che l'URL di callhome SLDest sia corretto (scope monitoring > scope callhome > show expand)
2. Verificare che la configurazione del server DNS MIO sia corretta, ad esempio da CLI:

```
FPR4125-1# scope system
FPR4125-1 /system # scope services
FPR4125-1 /system/services # show dns
Domain Name Servers:
   IP Address: 172.31.200.100
```

3. Provare a eseguire il ping dalla CLI dello chassis per **tools.cisco.com** e vedere se risolve:

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

4. Provare a eseguire il ping dalla CLI dello chassis sul server DNS:

```
FPR4125-1# connect local-mgmt
FPR4125-1(local-mgmt)# ping 172.31.200.100
PING 172.31.200.100 (172.31.200.100) from 10.62.148.225 eth0: 56(84) bytes of data.
^C
--- 172.31.200.100 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3001ms
```

5. Abilitare l'acquisizione sull'interfaccia di gestione (MIO) dello chassis (applicabile solo su FP41xx/FP93xx) e controllare la comunicazione DNS durante l'esecuzione di un test ping su **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
```

Errore di registrazione: impossibile autenticare il server

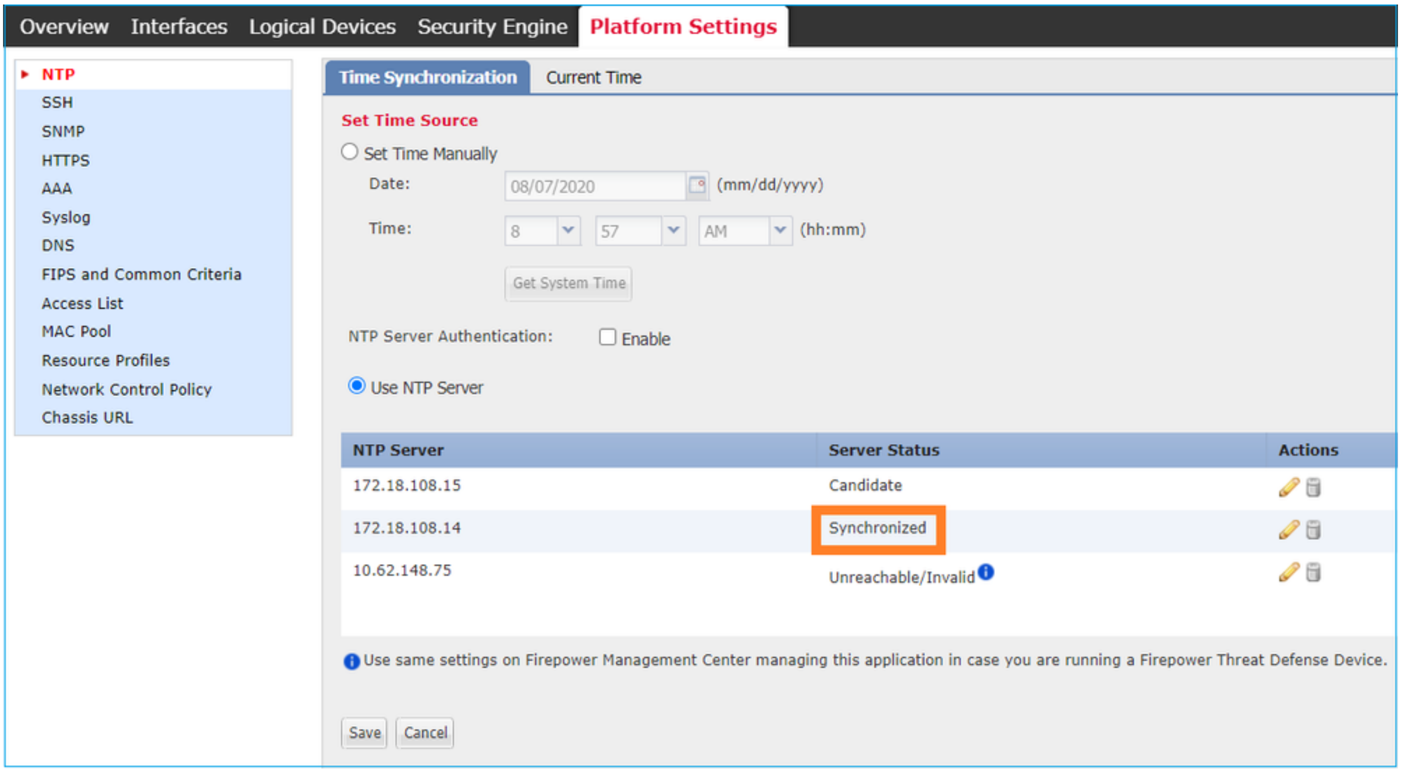
```
FPR4125-1# show license all

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
```

Fasi consigliate

1. Verificare se il certificato del canale di trust MIO predefinito è corretto, ad esempio:

```
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. Verificare che il server NTP e il fuso orario siano impostati correttamente. La verifica del certificato richiede lo stesso tempo tra server e client. A tale scopo, utilizzare il protocollo NTP per sincronizzare l'ora. Ad esempio, la verifica dell'interfaccia utente FXOS:



Set Time Source

○ Set Time Manually

Date: 08/07/2020 (mm/dd/yyyy)

Time: 8 57 AM (hh:mm)

NTP Server Authentication: □ Enable

● Use NTP Server

NTP Server	Server Status	Actions
172.18.108.15	Candidate	
172.18.108.14	Synchronized	
10.62.148.75	Unreachable/Invalid	

Use same settings on Firepower Management Center managing this application in case you are running a Firepower Threat Defense Device.

Verifica CLI

```
FPR4125-1# scope system
FPR4125-1 /system # scope services
FPR4125-1 /system/services # show ntp-server

NTP server hostname:
   Name                                                       Time Sync Status
   ------------------------------------------------------ ----------------
   10.62.148.75                                             Unreachable Or Invalid Ntp Server
    172.18.108.14                                              Time Synchronized
   172.18.108.15                                             Candidate
```

Abilitare un'acquisizione e controllare la comunicazione TCP (HTTPS) tra la MIO e il **tools.cisco.com.** Di seguito sono indicate alcune opzioni:

- Èpossibile chiudere la sessione HTTPS all'interfaccia utente FXOS e quindi impostare un filtro di acquisizione su CLI per HTTPS, ad esempio:

```
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
```

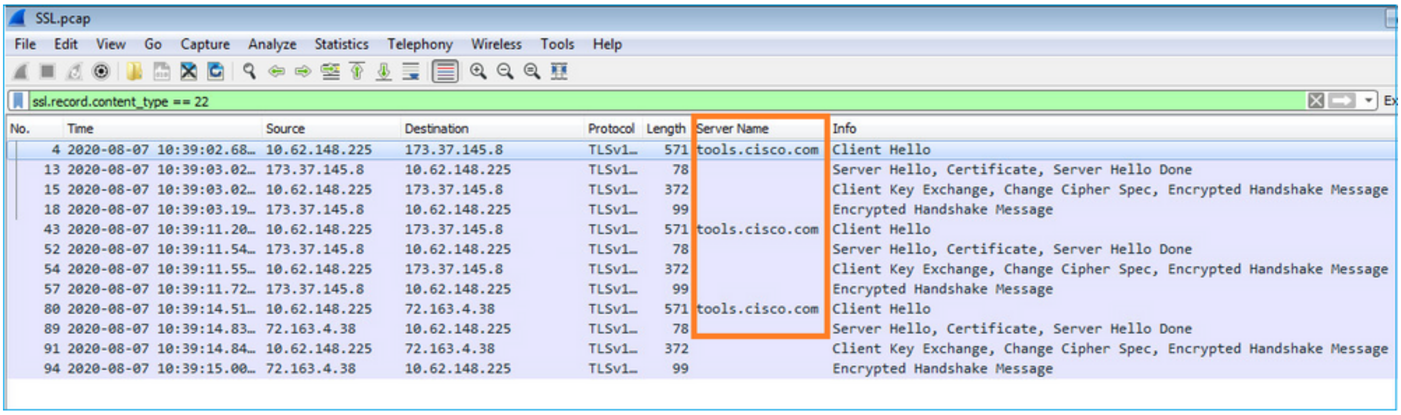
- Inoltre, se si desidera mantenere aperta l'interfaccia utente FXOS, è possibile specificare nell'acquisizione gli IP di destinazione (72.163.4.38 e 173.37.145.8 sono **tools.cisco.com** al momento della scrittura). Si consiglia inoltre di salvare la cattura in formato pcap e di controllarla in Wireshark. Questo è un esempio di registrazione riuscita:

```
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
```

- Per esportare il file pcap in un server FTP remoto:

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

1 56936 Aug 07 08:39:35 2020 SSL.pcap
1    29 May 06 17:48:02 2020 blade_debug_plugin
1    19 May 06 17:48:02 2020 bladelog
1    16 Dec 07 17:24:43 2018 cores
2  4096 Dec 07 17:28:46 2018 debug_plugin/
1    31 Dec 07 17:24:43 2018 diagnostics
2  4096 Dec 07 17:22:28 2018 lost+found/
1    25 Dec 07 17:24:31 2018 packet-capture
2  4096 Sep 24 07:05:40 2019 techsupport/

Usage for workspace://
3999125504 bytes total
284364800 bytes used
3509907456 bytes free
FPR4125-1(local-mgmt)# copy workspace:///SSL.pcap ftp://ftp_user@10.62.148.41/SSL.pcap
Password:
FPR4125-1(local-mgmt)#
```


SSL.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssl.record.content_type == 22

No.	Time	Source	Destination	Protocol	Length	Server Name	Info
4	2020-08-07 10:39:02.68…	10.62.148.225	173.37.145.8	TLSv1…	571	tools.cisco.com	Client Hello
13	2020-08-07 10:39:03.02…	173.37.145.8	10.62.148.225	TLSv1…	78		Server Hello, Certificate, Server Hello Done
15	2020-08-07 10:39:03.02…	10.62.148.225	173.37.145.8	TLSv1…	372		Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
18	2020-08-07 10:39:03.19…	173.37.145.8	10.62.148.225	TLSv1…	99		Encrypted Handshake Message
43	2020-08-07 10:39:11.20…	10.62.148.225	173.37.145.8	TLSv1…	571	tools.cisco.com	Client Hello
52	2020-08-07 10:39:11.54…	173.37.145.8	10.62.148.225	TLSv1…	78		Server Hello, Certificate, Server Hello Done
54	2020-08-07 10:39:11.55…	10.62.148.225	173.37.145.8	TLSv1…	372		Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
57	2020-08-07 10:39:11.72…	173.37.145.8	10.62.148.225	TLSv1…	99		Encrypted Handshake Message
80	2020-08-07 10:39:14.51…	10.62.148.225	72.163.4.38	TLSv1…	571	tools.cisco.com	Client Hello
89	2020-08-07 10:39:14.83…	72.163.4.38	10.62.148.225	TLSv1…	78		Server Hello, Certificate, Server Hello Done
91	2020-08-07 10:39:14.84…	10.62.148.225	72.163.4.38	TLSv1…	372		Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
94	2020-08-07 10:39:15.00…	72.163.4.38	10.62.148.225	TLSv1…	99		Encrypted Handshake Message

Errore di registrazione: trasporto HTTP non riuscito

```
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
```

Fasi consigliate

1. Verificare che l'URL della funzione call-home sia corretto. È possibile verificare questa condizione dall'interfaccia utente di FXOS o dalla CLI (**scope monitoring > show callhome detail expand**).
2. Abilitare un'acquisizione e controllare la comunicazione TCP (HTTPS) tra la MIO e il **tools.cisco.com** come illustrato nella sezione 'Autenticazione del server non riuscita' di questo documento.

Errore di registrazione: impossibile connettersi all'host

```
FPR4125-1# show license all

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

Smart Licensing is ENABLED

Registration:
Status: UNREGISTERED - REGISTRATION FAILED
 Export-Controlled Functionality: Not Allowed
 Initial Registration: FAILED on Aug 07 2020 06:58:46 UTC
 Failure reason: Couldn't connect to host
```

Fasi consigliate

1. Se è abilitata una configurazione proxy, verificare che l'URL e la porta proxy siano configurati correttamente.
2. Abilitare un'acquisizione e controllare la comunicazione TCP (HTTPS) tra la MIO e il **tools.cisco.com** come illustrato nella sezione 'Autenticazione del server non riuscita' di questo documento.

Errore di registrazione: il server HTTP restituisce il codice di errore >= 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
```

Fasi consigliate

1. Se è abilitata una configurazione proxy, contattare l'amministratore del server proxy per informazioni sulle impostazioni proxy.

2. Abilitare un'acquisizione e controllare la comunicazione TCP (HTTPS) tra la MIO e il **tools.cisco.com** come illustrato nella sezione 'Autenticazione del server non riuscita' di questo documento. Provare a registrarsi nuovamente (opzione ‘force’) dalla CLI di FXOS:

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

Errore di registrazione: analisi del messaggio di risposta back-end non riuscita

```
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
```

Fasi consigliate

1. Riprova automaticamente in seguito. Utilizzare 'renew' per riprovare immediatamente.

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

2. Verificare che l'URL del call-home sia corretto.

Problemi di licenza sull'appliance ASA - serie 1xxx/21xx

Errore di registrazione: errore di invio del messaggio di comunicazione

```
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
```

Fasi consigliate

1. Controllare le impostazioni DNS

```
ciscoasa# show run dns
```

2. Tentare il ping **tools.cisco.com.** In questo caso, viene utilizzata l'interfaccia di gestione:

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

3. Controllare la tabella di routing:

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

Assicurarsi di avere una licenza abilitata, ad esempio:

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

4. Abilitare l'acquisizione sull'interfaccia che instrada verso **tools.cisco.com** (se si esegue l'acquisizione senza alcun filtro IP, accertarsi di non avere ASDM aperto quando si esegue l'acquisizione per evitare disturbi di acquisizione non necessari).

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

> **Avviso**: l'acquisizione dei pacchetti può avere un impatto negativo sulle prestazioni.

5. Abilitare temporaneamente il syslog di livello 7 (debug) e controllare i messaggi ASA Syslog durante il processo di registrazione:

```
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
```

Riprovare a eseguire la registrazione:

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

Requisiti speciali per i diritti aggiuntivi

- Prima di configurare i diritti per i componenti aggiuntivi, è necessario acquisire un diritto livello funzionalità valido
- Tutti i diritti del componente aggiuntivo devono essere rilasciati prima del rilascio del diritto al livello funzionalità

Stato del diritto durante l'operazione di riavvio

- Gli stati dei diritti vengono salvati nella memoria flash
- Durante il tempo di avvio, queste informazioni vengono lette dalla memoria flash e le licenze vengono impostate in base alla modalità di imposizione salvata
- La configurazione di avvio viene applicata in base alle informazioni sui diritti memorizzate nella cache
- I diritti vengono richiesti di nuovo dopo ogni riavvio

Contatta il supporto Cisco TAC

FP41xx/FP9300

Se tutti gli elementi menzionati in questo documento hanno esito negativo, raccogliere gli output dalla CLI dello chassis e contattare Cisco TAC:

Uscita 1

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

Output 2:

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

Output 3:

Pacchetto di supporto per chassis FXOS

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

Output 4 (consigliato):

Acquisizione di Ethanalyzer dalla CLI dello chassis

FP1xxx/FP21xx

Uscita 1

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

Output 2:

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

Domande frequenti

Sul FP21xx, dov'è la scheda Licensing (Licenze) sull'interfaccia grafica dello chassis (FCM)?
A partire dalla versione 9.13.x, FP21xx supporta 2 modalità ASA:

- Appliance
- Piattaforma

In modalità Appliance non è presente l'interfaccia utente dello chassis. In modalità piattaforma, è disponibile un'interfaccia utente dello chassis, ma la licenza è configurata dalla CLI di ASA o da ASDM.
D'altra parte, sulle piattaforme FPR4100/9300, la licenza deve essere configurata in FCM tramite GUI o FXOS CLI e i diritti ASA devono essere richiesti da ASA CLI o ASDM.
Riferimenti:

- Gestione delle licenze per l'appliance ASA

- Dispositivi logici per Firepower 4100/9300
- Licenze: Smart Software Licensing (ASAv, ASA su Firepower)
- Implementazione della modalità piattaforma ASA con ASDM e Firepower Chassis Manager

Come è possibile abilitare una licenza di crittografia avanzata?

Questa funzionalità viene attivata automaticamente se il token utilizzato nella registrazione FCM ha l'opzione Consenti funzionalità di controllo dell'esportazione sui prodotti registrati con questo token abilitato.

Come è possibile abilitare una licenza di crittografia avanzata se le funzionalità controllate dall'esportazione a livello di FCM e la relativa funzionalità di crittografia-3DES-AES a livello di ASA sono disabilitate?

Se per il token questa opzione non è abilitata, annullare la registrazione di FCM e registrarlo nuovamente con un token che ha questa opzione abilitata.

Cosa è possibile fare se l'opzione per consentire la funzionalità di controllo delle esportazioni sui prodotti registrati con questo token non è disponibile quando si genera il token?

Rivolgersi al team Cisco che gestisce gli account.

È obbligatorio configurare la funzione di crittografia avanzata a livello di appliance ASA?

L'opzione di crittografia avanzata è obbligatoria solo se FCM è integrato con un server satellite precedente alla versione 2.3.0. Si tratta di un unico scenario in cui è necessario configurare questa funzionalità.

Quali IP devono essere consentiti nel percorso tra FCM e Smart Licensing Cloud?

FXOS utilizza l'indirizzo https://tools.cisco.com/ (porta 443) per comunicare con il cloud di licenze. L'indirizzo https://tools.cisco.com/ viene risolto nei seguenti indirizzi IP:

- 72.163.4.38
- 173.37.145.8

Perché si verifica un errore di mancata conformità?

Il dispositivo può non essere conforme in queste situazioni:

- Sovrautilizzo (il dispositivo usa licenze non disponibili)
- Scadenza licenza - Una licenza con limiti di tempo è scaduta
- Mancata comunicazione - Il dispositivo non può raggiungere l'autorità di licenza per la riautorizzazione

Per verificare se l'account è in uno stato non conforme o se si avvicina a uno stato non conforme, è necessario confrontare i diritti attualmente in uso dallo chassis Firepower con quelli presenti nello Smart Account.
In uno stato di non conformità, è possibile apportare modifiche alla configurazione delle funzionalità che richiedono licenze speciali, ma l'operazione non viene in altro modo modificata. Ad esempio, oltre i contesti di limite di licenza Standard già esistenti, è possibile continuare a eseguire e modificarne la configurazione, ma non è possibile aggiungere un nuovo contesto.

Perché si verifica ancora un errore di non conformità dopo l'aggiunta delle licenze?

Per impostazione predefinita, il dispositivo comunica con l'autorità di licenza ogni 30 giorni per verificare i diritti. Se si desidera attivarlo manualmente, è necessario eseguire la procedura seguente:

Per le piattaforme FPR100/2100, deve essere eseguito tramite ASDM o CLI:

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

Per le piattaforme FPR4100/9300, deve essere eseguito tramite la CLI di FXOS:

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

Perché non vi sono licenze in uso sul livello ASA?

Verificare che i diritti ASA siano stati configurati a livello di ASA, ad esempio:

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

Perché le licenze non sono ancora in uso anche dopo la configurazione di un diritto ASA?

Questo stato è previsto se è stata distribuita una coppia di failover ASA attivo/standby e si controlla l'utilizzo della licenza sul dispositivo di standby.
Come indicato nella guida alla configurazione, la configurazione viene replicata sull'unità in standby, ma quest'ultima non utilizza la configurazione; rimane in stato di cache. Solo l'unità attiva richiede le licenze al server. Le licenze vengono aggregate in una singola licenza di failover condivisa dalla coppia di failover e questa licenza aggregata viene memorizzata anche sull'unità di standby da utilizzare se diventerà l'unità attiva in futuro. Per riferimento: licenze di failover o cluster ASA.

Cosa è possibile fare se FCM non ha accesso a Internet?

In alternativa, è possibile distribuire Cisco Smart Software Manager On-Prem (in precedenza Cisco Smart Software Manager Satellite). Questo è un componente di Cisco Smart Licensing che funziona in combinazione con Cisco Smart Software Manager. Offre visibilità e funzionalità di report quasi in tempo reale delle licenze Cisco acquistate e usate. Offre inoltre alle organizzazioni che operano nel campo della sicurezza un modo per accedere a un sottoinsieme delle funzionalità di Cisco SSM senza utilizzare una connessione Internet diretta per gestire la propria base di installazione.

Dove è possibile trovare ulteriori informazioni su Cisco Smart Software Manager On-Prem?

Queste informazioni sono disponibili nella Guida alla configurazione di FXOS:

- Configurazione di un server satellite Smart License per lo chassis Firepower 4100/9300
- Configurazione della registrazione di Firepower Chassis Manager su Smart Software Manager in locale

Informazioni correlate

- Guida alla configurazione della CLI per le operazioni generali della serie Cisco ASA
- Gestione delle licenze per l'appliance ASA
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l&rsquo;accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).