Fehlerbehebung bei ASA Smart License auf FXOS FirePOWER Appliances

Inhalt

Einleitung

In diesem Dokument wird die Adaptive Security Appliance (ASA) Smart Licensing-Funktion für FirePOWER eXtensible Operating System (FXOS) beschrieben.

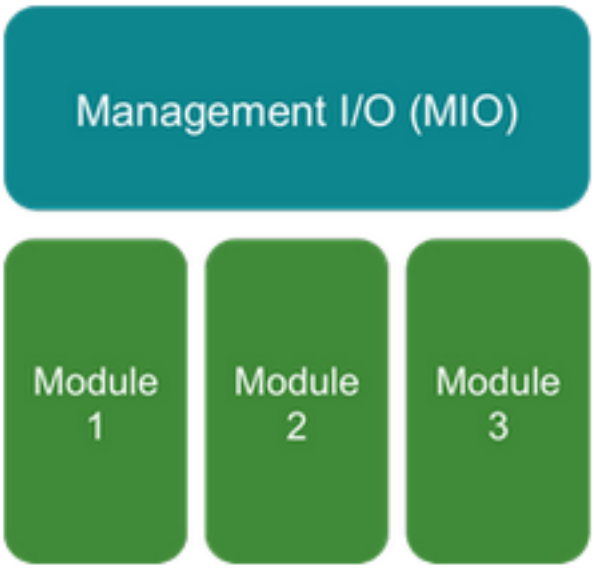
Hintergrundinformationen

Smart Licensing auf FXOS wird verwendet, wenn eine ASA auf dem Chassis installiert ist. Für Firepower Threat Defense (FTD) und Firepower Management Center (FMC) überprüfen Smart Licensing die Registrierung und Fehlerbehebung von FMC- und FTD Smart License.

In diesem Dokument werden hauptsächlich Szenarien behandelt, in denen das FXOS-Gehäuse über einen direkten Internetzugang verfügt. Wenn Ihr FXOS-Chassis nicht auf das Internet zugreifen kann, müssen Sie entweder einen Satellitenserver oder eine permanente Lizenzreservierung (Permanent License Reservation, PLR) in Betracht ziehen. Weitere Informationen zur Offline-Verwaltung finden Sie im FXOS-Konfigurationsleitfaden.

Smart Licensing-Architektur

Eine grobe Übersicht über die Gehäusekomponenten:

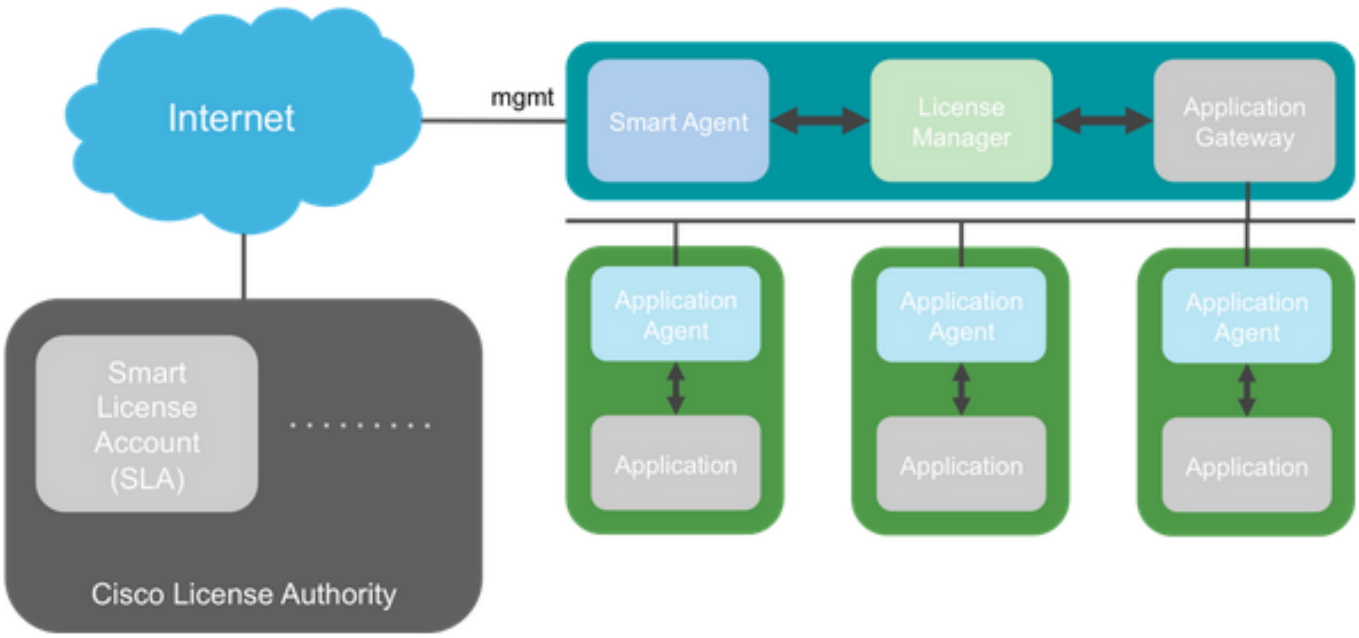


- Sowohl Management Input/Output (MIO) als auch einzelne Module spielen bei Smart Licensing eine wichtige Rolle.
- MIO selbst benötigt keine Lizenzen für den Betrieb.
- SA-Anwendung(en) auf jedem Modul muss lizenziert werden

Der FXOS-Supervisor ist die MIO. Die MIO besteht aus drei Hauptkomponenten:

- Intelligenter Agent
- Lizenzmanager
- Anwendungs-AG

Gesamtarchitektur



Nomenklatur

Begriff	Beschreibung

Cisco Lizenzbehörde	Das Cisco Lizenz-Backend für Smart Licensing. Speichert alle Informationen zu Produktlizenzen. Dazu gehören auch Berechtigungen und Geräteinformationen.
Smart License-Konto	Ein Konto, das über alle Berechtigungen für die Appliance verfügt.
Token-ID	Ein Bezeichner wird verwendet, um das Smart License-Konto zu unterscheiden, wenn die Appliance registriert wird.
Berechtigung	Entspricht einer Lizenz. Entspricht einer einzelnen Funktion oder einer gesamten Funktionsebene.
Produktaktivierungsschlüssel (PAK)	Der ältere Lizenzierungsmechanismus. An eine einzige Appliance gebunden.

Smart Agent-Status

Status	Beschreibung
Nicht konfiguriert	Smart Licensing ist nicht aktiviert.
Nicht identifiziert	Smart Licensing wurde aktiviert, aber der Smart Agent hat sich noch nicht bei Cisco gemeldet, um sich zu registrieren.
Registriert	Der Agent hat sich mit der Cisco Lizenzierungsbehörde in Verbindung gesetzt und sich registriert.
Autorisiert	Wenn ein Agent aufgrund einer Berechtigungs-Autorisierungsanfrage einen Compliance-Status erhält.
Nicht konform (OOC)	Wenn ein Agent als Antwort auf eine Berechtigungs-Autorisierungsanfrage einen OOC-Status erhält.
Autorisierung abgelaufen	Wenn der Support-Mitarbeiter 90 Tage lang nicht mit Cisco kommuniziert hat.

ASA-Berechtigungen

Folgende ASA-Berechtigungen werden unterstützt:

- Standard-Tier
- Mehrere Kontexte
- Starke Verschlüsselung (3DES)
- Mobilfunk-/Dienstanbieter (GTP)

Konfiguration

Befolgen Sie die Anweisungen in diesen Dokumenten:

- Smart Software-Lizenzierung (ASAv, ASA mit Firepower)
- Lizenzmanagement für die ASA

Vor jeder Konfiguration der Funktionsebene:

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

Standardstufe konfigurieren:

```
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 (hohe Verfügbarkeit)

Wie im ASA-Konfigurationsleitfaden dokumentiert, muss jede FirePOWER-Einheit bei der License Authority oder einem Satellitenserver registriert sein. Verifizierung über die ASA CLI:

```
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
```

Das Standby-Gerät:

```
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
```

Anwenderbericht: ASA HA-Lizenz für FP2100

- 2100 kommuniziert die ASA über die ASA-Schnittstellen mit dem Cisco Smart Licensing-Portal (Cloud) und nicht mit dem FXOS-Management
- Sie müssen beide ASAs im Cisco Smart Licensing-Portal (Cloud) registrieren.

In diesem Fall wird die lokale HTTP-Authentifizierung auf einer externen Schnittstelle verwendet:

```
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
```

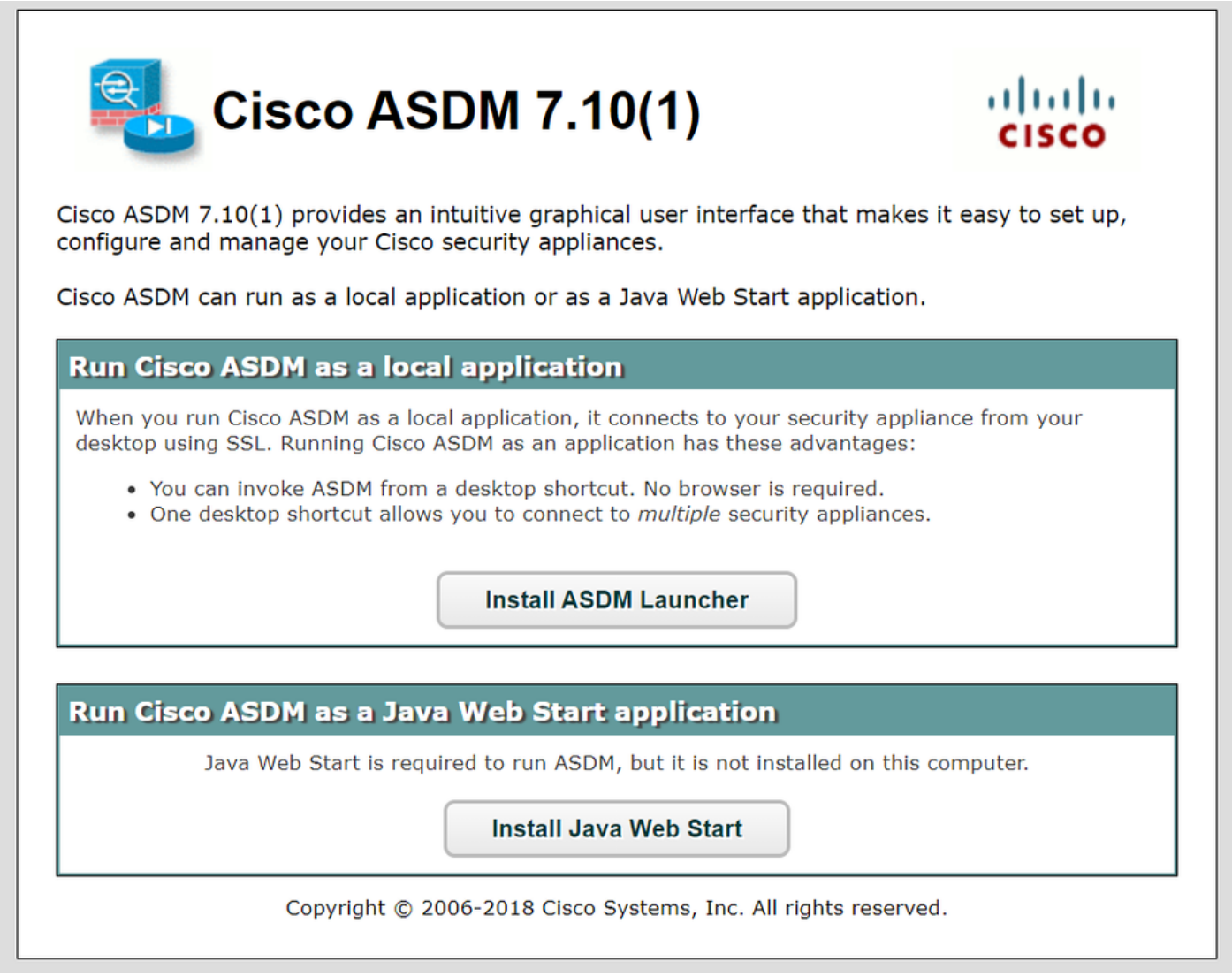
Sie können über ASDM nur eine Verbindung zur ASA herstellen, wenn eine 3DES/AES-Lizenz aktiviert ist. Für eine ASA, die noch nicht registriert ist, ist dies nur auf einer Schnittstelle möglich, die management-only. Konfigurationsanleitung: "Strong Encryption (3DES/AES) steht für

Managementverbindungen zur Verfügung, bevor Sie eine Verbindung zum License Authority- oder Satellite-Server herstellen, um ASDM zu starten. Beachten Sie, dass der ASDM-Zugriff nur auf Management-Schnittstellen mit der Standardverschlüsselung verfügbar ist. Durchgehender Datenverkehr ist erst dann zulässig, wenn Sie eine Verbindung herstellen und die Strong Encryption-Lizenz erwerben." In einem anderen Fall erhalten Sie:

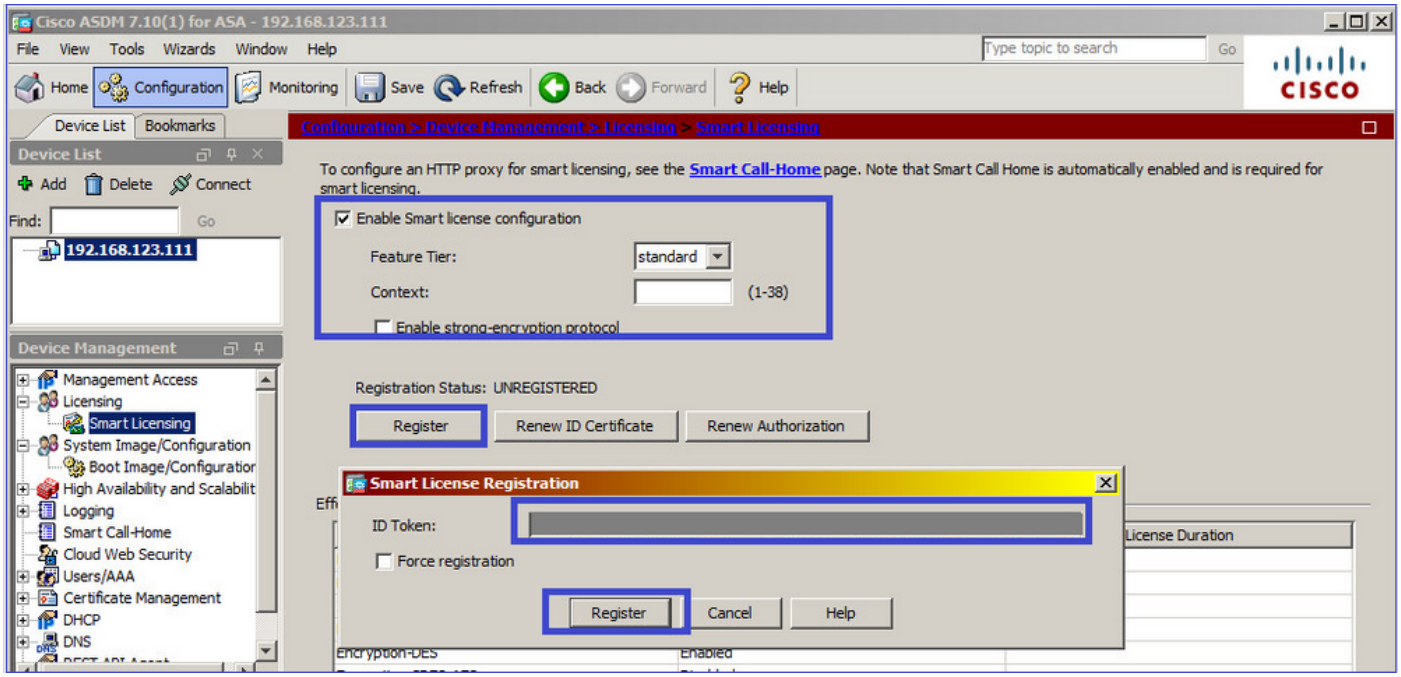
```
ciscoasa(config)# debug ssl 255
debug ssl enabled at level 255.
error:1408A0C1:SSL routines:ssl3_get_client_hello:no shared cipher
```

Um zu verhindern, dass die ASA nur über eine Management-Konfiguration auf der Internet-Schnittstelle verfügt, ist eine ASDM-Verbindung möglich:

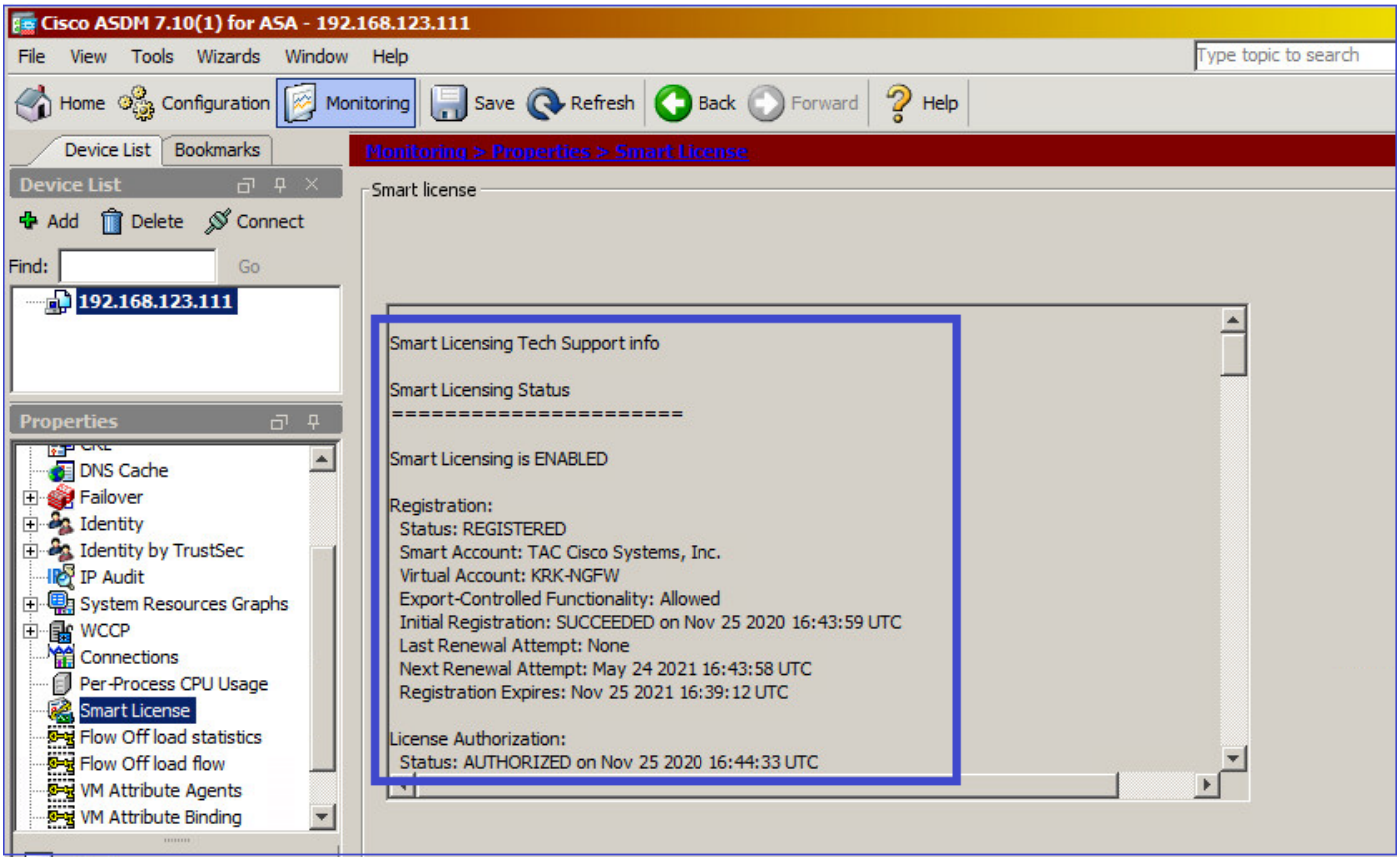
```
interface Ethernet1/2
management-only
nameif outside
security-level 100
ip address 192.168.123.111 255.255.255.0 standby 192.168.123.112
```



Konfigurieren Sie Smart Licensing auf der primären ASA:



Navigieren Sie zu **Monitoring > Properties > Smart License** um den Status der Registrierung zu überprüfen:



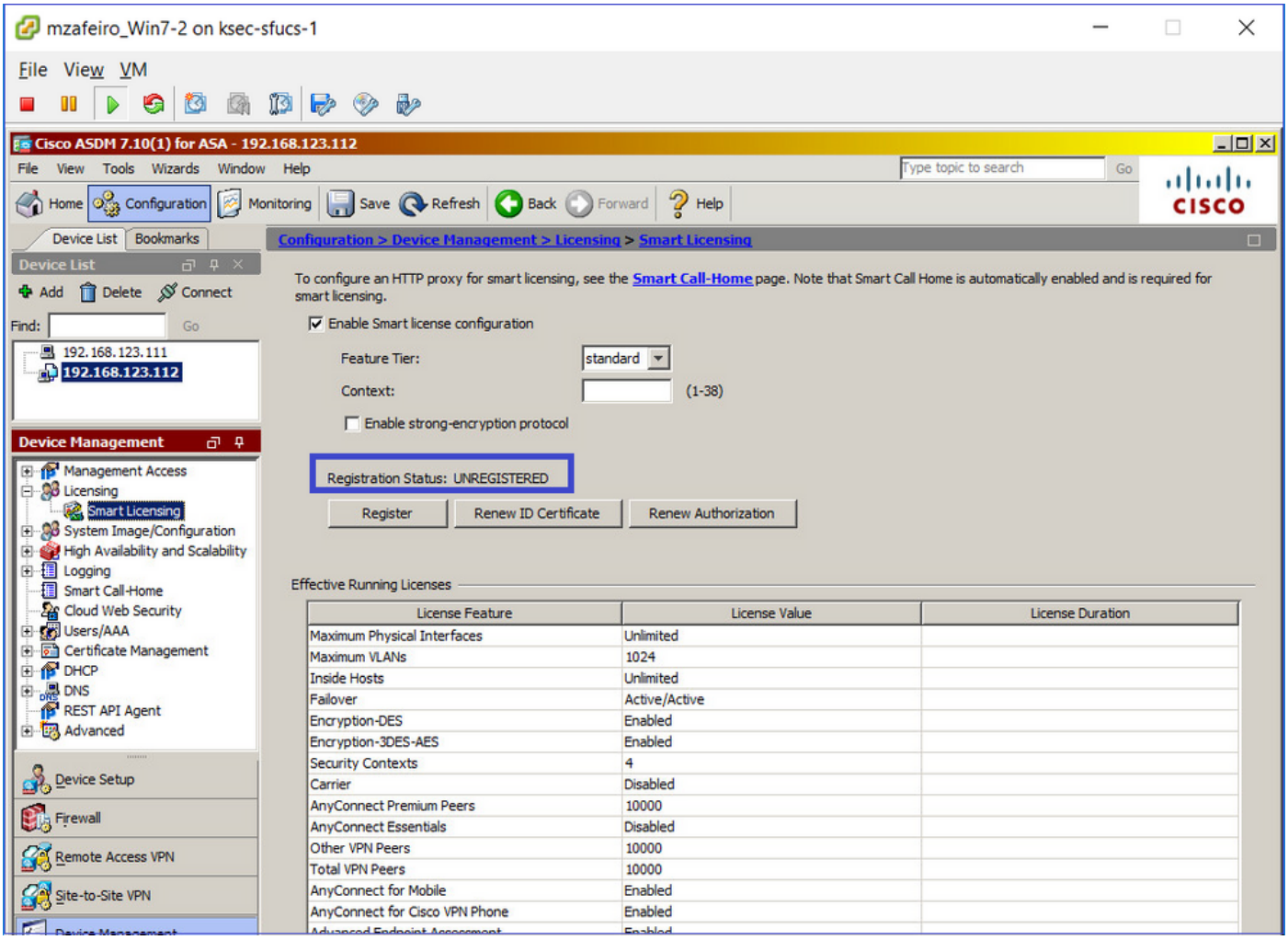
Primäre ASA CLI-Verifizierung:

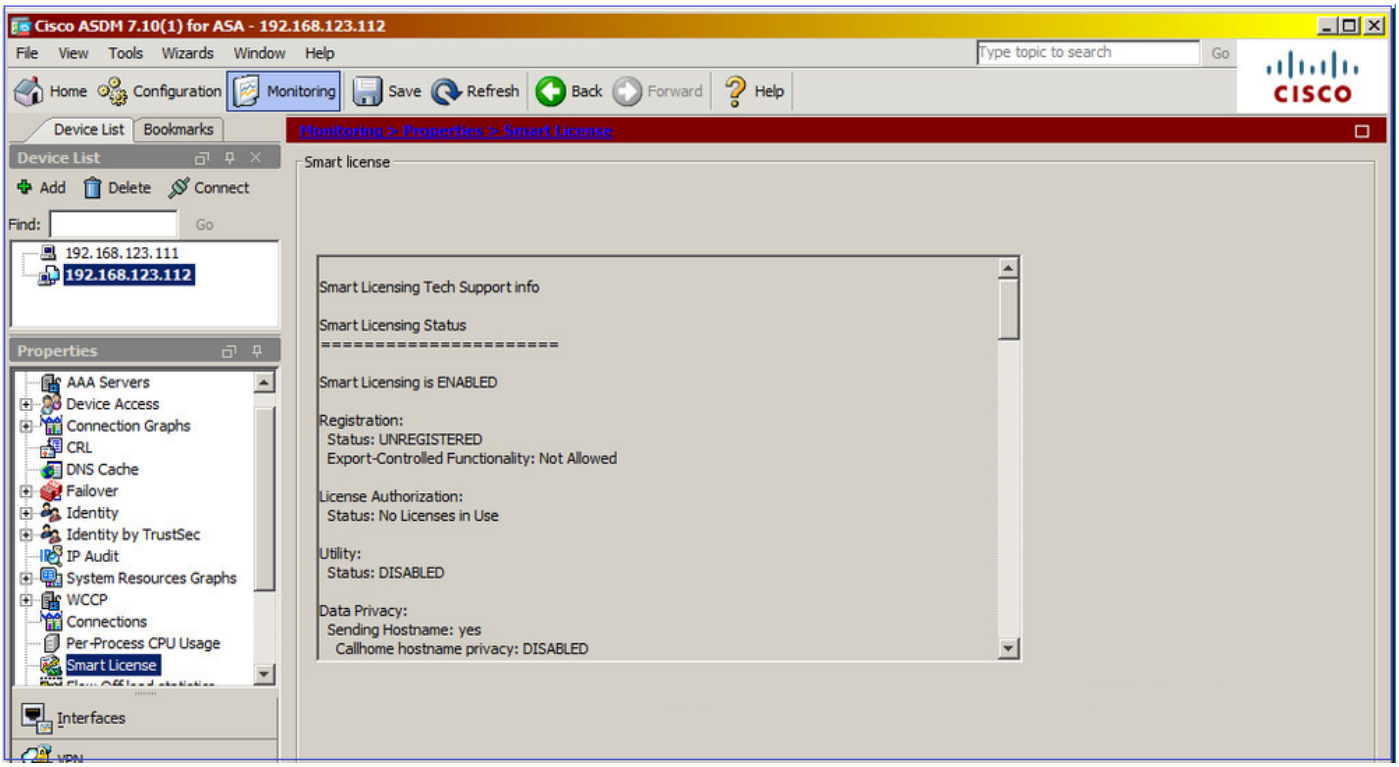
```
ciscoasa/pri/act# show license all

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
```

Verbinden Sie sich über ASDM mit der Standby-ASA (dies ist nur möglich, wenn die ASA mit einer Standby-IP konfiguriert wurde). Die Standby-ASA wird angezeigt als UNREGISTERED und dies wird erwartet, da es noch nicht beim Smart Licensing-Portal registriert wurde:





Die Standby-ASA-CLI bietet Folgendes:

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

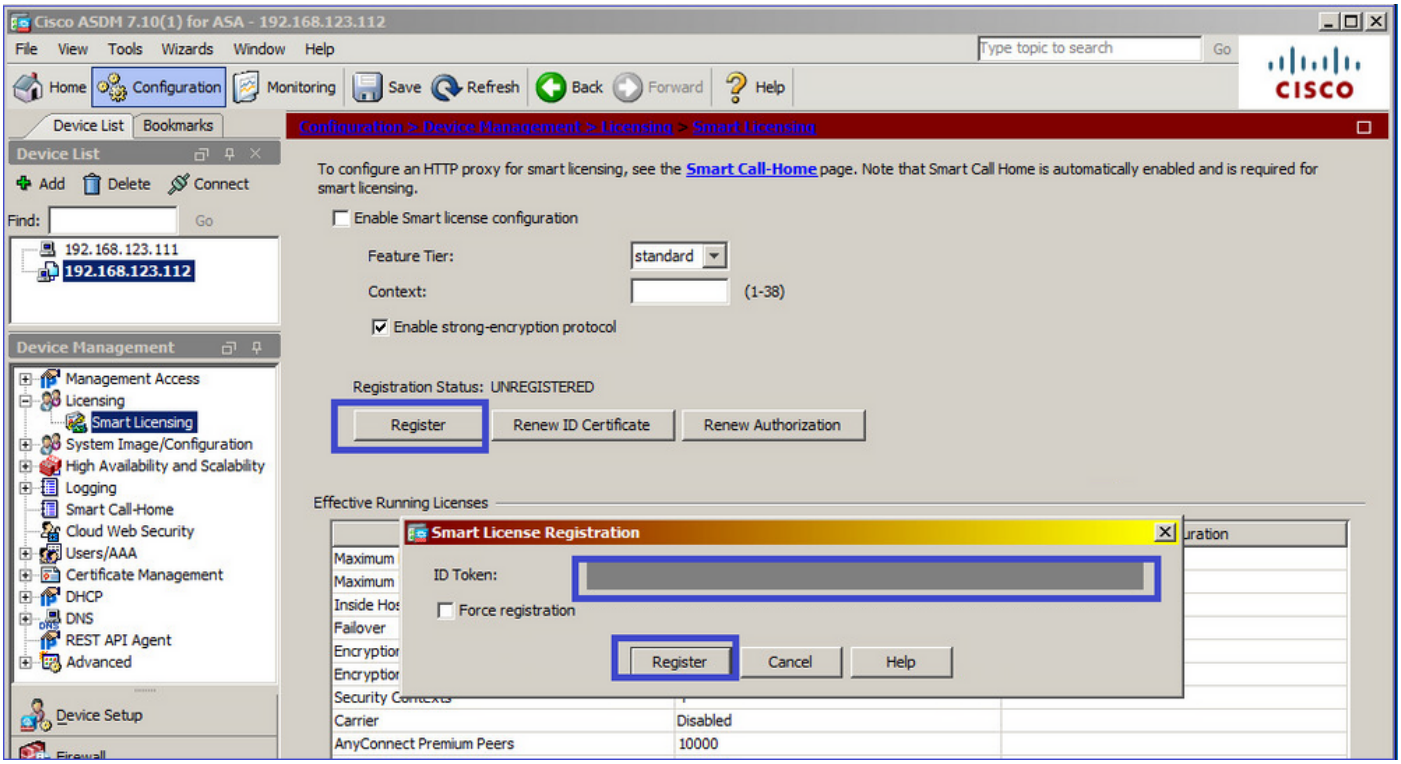
```
Smart Licensing Status
======================

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
```

Die auf der Standby-ASA aktivierten Lizenzfunktionen:

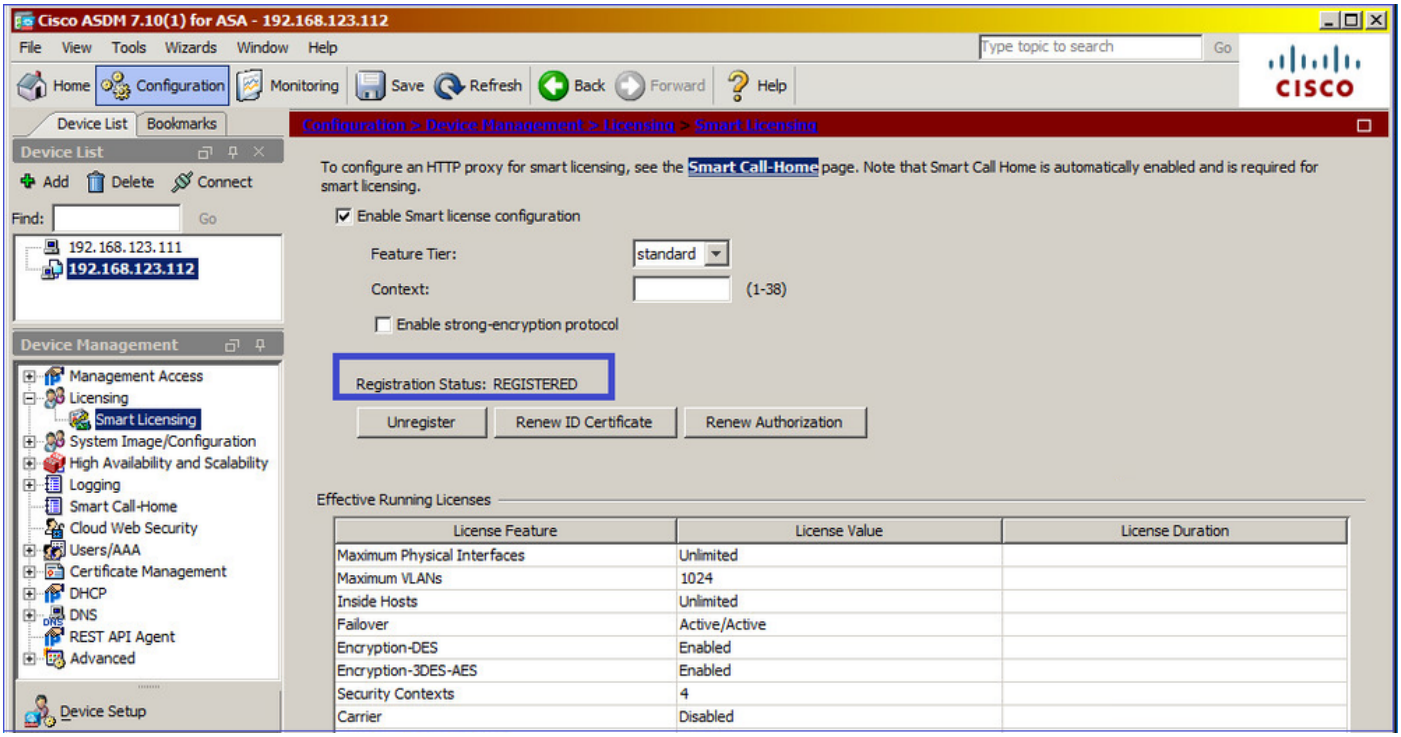
```
ciscoasa/sec/stby# show license features
Serial Number: JAD123456A
Export Compliant: NO

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
```

Standby-ASA registrieren:



Auf Standby-ASA-Geräten ist dies REGISTERED:



CLI-Verifizierung auf Standby-ASA:

```
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-Cluster

Wenn die Lizenzkonflikte zwischen den Geräten bestehen, wird der Cluster nicht gebildet:

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

Eine erfolgreiche Cluster-Einrichtung:

```
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.
```

Cluster-Steuerungsknoten:

```
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
```

Cluster-Dateneinheit:

```
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
```

Überprüfung und Debuggen

Chassis (MIO) - Zusammenfassung der Verifizierungsbefehle:

```
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
```

Konfigurationsverifizierung:

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

ASA - Zusammenfassung der Verifizierungsbefehle:

```
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
```

Chassis (MIO) - Beispielausgänge für Verifizierungsbefehle

```
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
```

ASA-Beispielausgänge für Verifizierungsbefehle

```
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
```

Registrierung erfolgreich

Die Ausgabe stammt aus der Benutzeroberfläche des Chassis-Managers:

```
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
```

Abgelaufene Autorisierung

Die Ausgabe stammt aus der Benutzeroberfläche des Chassis-Managers:

```
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
```

Beispielausgänge aus der Chassis-CLI

UNREGISTERED (Nicht registriert)

```
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
```

Registrierung läuft

```
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
```

Registrierungsfehler

```
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
```

Evaluierungszeitraum

```
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
```

Häufige Lizenzprobleme bei FXOS-Chassis (MIO)

Registrierungsfehler: Ungültiges Token

```
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."]}
```

Empfohlene Schritte

1. Überprüfen Sie, ob die Call-Home-URL auf CSSM verweist.
2. Melden Sie sich beim CSSM an, und überprüfen Sie, ob das Token von dort generiert wurde oder ob das Token abgelaufen ist.

Registrierungsfehler: Produkt bereits registriert

```
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."]}
```

Empfohlene Schritte

1. Melden Sie sich beim CSSM an.
2. Überprüfen Sie Product Instances in ALLEN virtuellen Konten.
3. Suchen Sie die alte Registrierungsinstanz nach SN, und entfernen Sie sie.
4. Dieses Problem kann durch die folgenden beiden Ursachen verursacht werden: Die automatische Verlängerung wird nicht durchgeführt, wenn Uhrzeit/Datum nicht ordnungsgemäß eingerichtet sind, z. B. wenn kein NTP-Server konfiguriert ist.Falsche Reihenfolge beim Umschalten zwischen einem Satelliten- und einem Produktionsserver. Ändern Sie beispielsweise zuerst die URL, und geben Sie dann "deregister" aus.

Registrierungsfehler: Offset des Datums über das Limit hinaus

```
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."]}
```

Empfohlener Schritt

Überprüfen Sie die Zeit-/Datumskonfiguration, um sicherzustellen, dass ein NTP-Server konfiguriert ist.

Registrierungsfehler: Fehler beim Auflösen des Hosts

```
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
```

Empfohlene Schritte

1. Überprüfen Sie, ob die SLDest-URL für den Anruf korrekt ist (scope monitoring > scope callhome > show expand)
2. Prüfen Sie, ob die Konfiguration des MIO-DNS-Servers korrekt ist, z. B. über die 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. Versuchen Sie, von der Chassis-CLI aus den Ping-Befehl **tools.cisco.com** und prüfen, ob Folgendes aufgelöst wird:

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

4. Versuchen Sie, von der Chassis-CLI aus einen Ping an den DNS-Server zu senden:

```
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. Aktivieren Sie die Erfassung an der Chassis (MIO)-Managementschnittstelle (dies gilt nur für FP41xx/FP93xx), und überprüfen Sie die DNS-Kommunikation, während Sie einen Ping-Test für die **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
```

Registrierungsfehler: Fehler beim Authentifizieren des Servers.

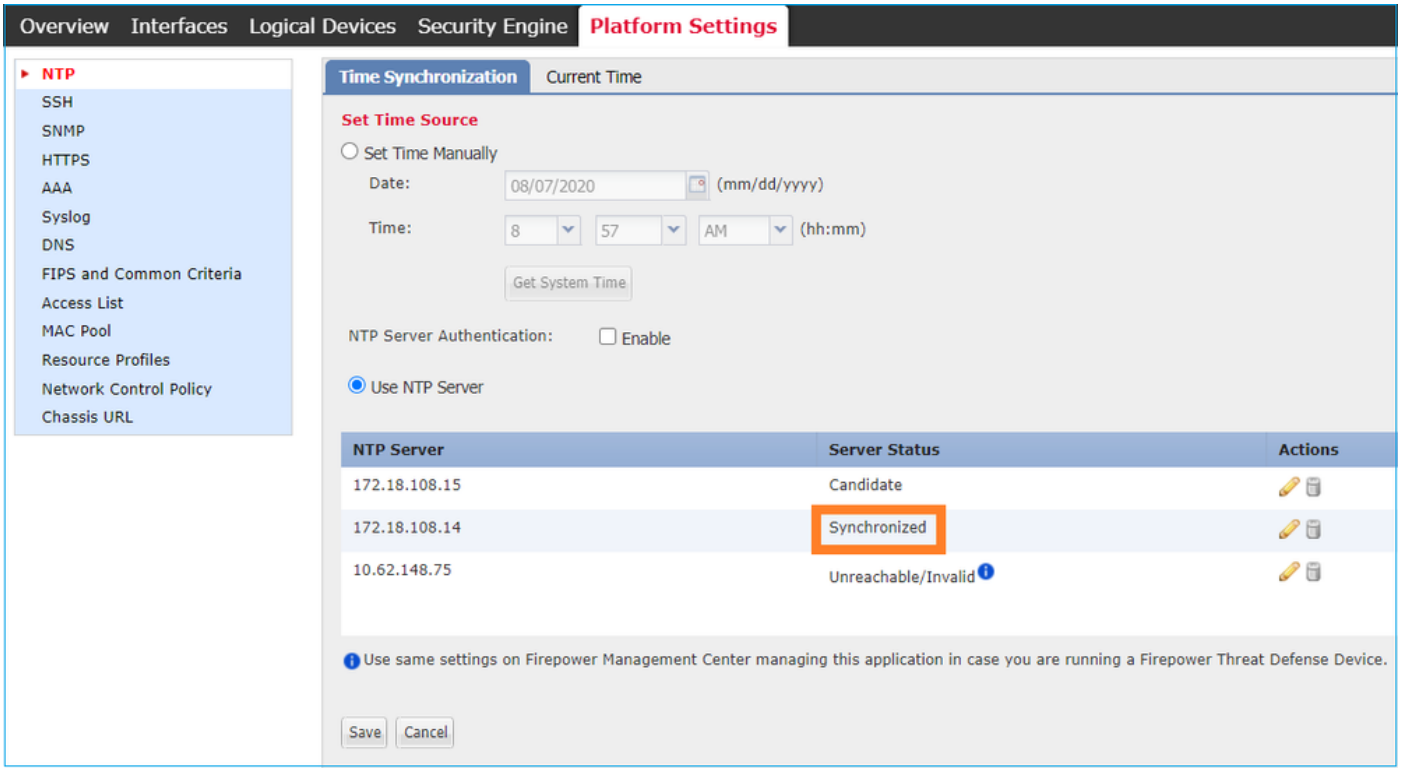
```
FPR4125-1# show license all

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
```

Empfohlene Schritte

1. Überprüfen Sie, ob der MIO-Vertrauenspunkt CHdefault über das richtige Zertifikat verfügt. Beispiel:

```
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. Überprüfen Sie, ob der NTP-Server und die Zeitzone richtig eingestellt sind. Für die Zertifikatsüberprüfung muss die gleiche Zeit zwischen Server und Client verwendet werden. Verwenden Sie dazu NTP, um die Uhrzeit zu synchronisieren. Zum Beispiel FXOS UI Verifizierung:



CLI-Überprüfung

```
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
```

Aktivieren Sie eine Erfassung und überprüfen Sie die TCP-Kommunikation (HTTPS) zwischen der MIO und dem **tools.cisco.com**. Hier haben Sie einige Möglichkeiten:

- Sie können Ihre HTTPS-Sitzung mit der FXOS-Benutzeroberfläche schließen und dann einen Erfassungsfilter in der CLI für HTTPS einrichten. Beispiel:

```
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
```

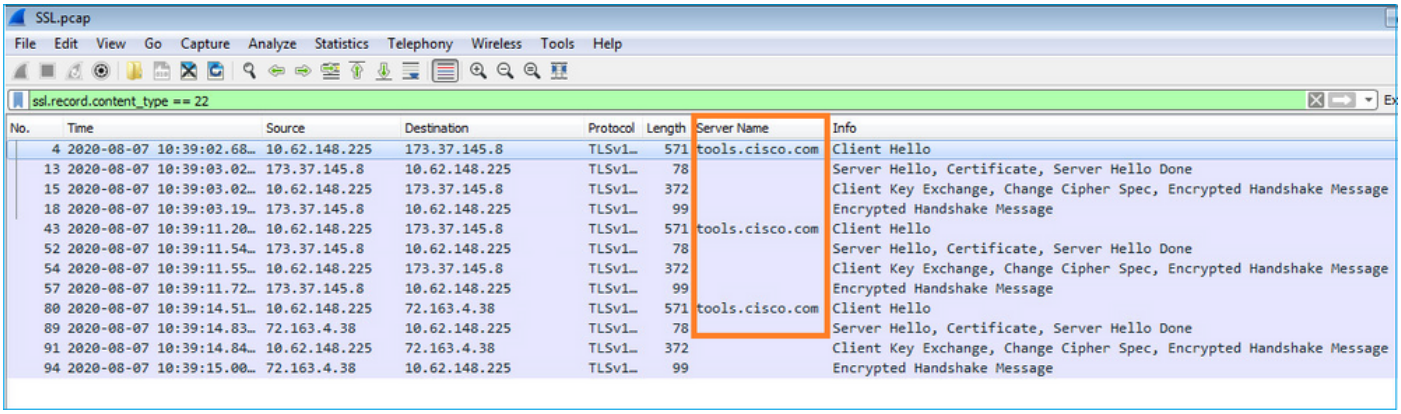
```
2017-01-12 13:09:44.609573  72.163.4.38 -> 10.62.148.37 SSL Continuation Data
2017-01-12 13:09:44.609595 10.62.148.37 -> 72.163.4.38  TCP 43278 > https [ACK] Seq=518 Ack=1369
Win=8208 Len=0 TSV=206433902 TSER=2933962264
2017-01-12 13:09:44.609599  72.163.4.38 -> 10.62.148.37 SSL Continuation Data
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
```

- Wenn Sie die FXOS-Benutzeroberfläche offen halten möchten, können Sie in der Erfassung die Ziel-IPs (72.163.4.38 und 173.37.145.8) als **tools.cisco.com** Server zum Zeitpunkt dieser Veröffentlichung). Es wird außerdem dringend empfohlen, die Aufzeichnung im pcap-Format zu speichern und in Wireshark zu überprüfen. Dies ist ein Beispiel für eine erfolgreiche Registrierung:

```
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
```

- So exportieren Sie die pcap-Datei auf einen FTP-Server:

```
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)#
```



Registrierungsfehler: HTTP-Transport fehlgeschlagen

```
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
```

Empfohlene Schritte

1. Überprüfen Sie, ob die Call-Home-URL korrekt ist. Sie können dies über die FXOS-Benutzeroberfläche oder die CLI (**scope monitoring > show callhome detail expand**).
2. Aktivieren Sie eine Erfassung und überprüfen Sie die TCP-Kommunikation (HTTPS) zwischen der MIO und dem **tools.cisco.com** wie im Abschnitt "Server konnte nicht authentifiziert werden" dieses Dokuments gezeigt.

Registrierungsfehler: Verbindung zum Host konnte nicht hergestellt werden

```
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
```

Empfohlene Schritte

1. Wenn eine Proxy-Konfiguration aktiviert ist, überprüfen Sie, ob die Proxy-URL und der Port richtig konfiguriert sind.
2. Aktivieren Sie eine Erfassung und überprüfen Sie die TCP-Kommunikation (HTTPS) zwischen der MIO und dem **tools.cisco.com** wie im Abschnitt "Server konnte nicht authentifiziert werden" dieses Dokuments gezeigt.

Registrierungsfehler: HTTP-Server gibt Fehlercode zurück >= 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
```

Empfohlene Schritte

1. Wenn eine Proxy-Konfiguration aktiviert ist, wenden Sie sich an den Admin des Proxy-Servers bezüglich der Proxy-Einstellungen.
2. Aktivieren Sie eine Erfassung und überprüfen Sie die TCP-Kommunikation (HTTPS) zwischen der MIO und dem **tools.cisco.com** wie im Abschnitt "Server konnte nicht authentifiziert werden" dieses Dokuments gezeigt. Versuchen Sie, sich erneut über die FXOS-CLI zu registrieren ("force"-Option):

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

Registrierungsfehler: Fehler beim Analysieren der Backend-Antwortmeldung.

```
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
```

Empfohlene Schritte

1. Automatische Wiederholungsversuche zu einem späteren Zeitpunkt Verwenden Sie "renew", um den Vorgang sofort zu wiederholen.

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

2. Überprüfen Sie die Call-Home-URL.

Lizenzprobleme bei ASA der Serie 1xxx/21xx

Registrierungsfehler: Fehler beim Senden der Kommunikationsnachricht

```
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
```

Empfohlene Schritte

1. Überprüfen Sie die DNS-Einstellungen

```
ciscoasa# show run dns
```

2. Versuchen Sie, einen Ping **tools.cisco.com**. In diesem Fall wird die Management-Schnittstelle verwendet:

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

3. Prüfen Sie die Routing-Tabelle:

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

Stellen Sie sicher, dass Sie eine Lizenz aktiviert haben. Beispiel:

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

4. Aktivieren Sie die Erfassung an der Schnittstelle, die zum Router **tools.cisco.com** (Wenn Sie die Erfassung ohne IP-Filter durchführen, stellen Sie sicher, dass bei der Erfassung kein ASDM geöffnet ist, um unnötige Erfassungsgeräusche zu vermeiden.)

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

Warnung: Die Paketerfassung kann sich negativ auf die Leistung auswirken.

5. Aktivieren Sie vorübergehend Syslog-Stufe 7 (debug), und überprüfen Sie die ASA-Syslog-Meldungen während des Registrierungsvorgangs:

```
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
```

Versuchen Sie, sich erneut zu registrieren:

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

Besondere Anforderungen für Zusatzberechtigungen

- Vor der Konfiguration von zusätzlichen Berechtigungen muss eine gültige Berechtigungsstufe erworben werden.
- Alle zusätzlichen Berechtigungen müssen freigegeben werden, bevor Sie die Berechtigung für die Feature-Ebene veröffentlichen.

Berechtigungsstatus während des Neustarts

- Berechtigungsstatus werden im Flash-Speicher gespeichert
- Während des Bootvorgangs werden diese Informationen aus dem Flash-Speicher gelesen, und die Lizenzen werden basierend auf dem gespeicherten Erzwingungsmodus festgelegt.
- Die Startkonfiguration wird basierend auf diesen zwischengespeicherten Berechtigungsinformationen angewendet.
- Ansprüche werden nach jedem Neustart erneut angefordert

Wenden Sie sich an den Cisco TAC Support

FP41xx/FP9300

Wenn alle in diesem Dokument aufgeführten Elemente fehlschlagen, ermitteln Sie die folgenden Ergebnisse über die CLI des Chassis, und wenden Sie sich an das Cisco TAC:

Ausgabe 1:

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

Ausgabe 2:

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

Ausgabe 3:

FXOS-Gehäuse-Supportpaket

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

Ausgabe 4 (sehr empfehlenswert):

Erfassung durch Ethanalyzer über die Chassis-CLI

FP1xxx/FP21xx

Ausgabe 1:

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

Ausgabe 2:

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

Häufig gestellte Fragen (FAQ)

Wo befindet sich beim FP21xx die Registerkarte Licensing (Lizenzierung) auf der Benutzeroberfläche des Chassis (FCM)?
Ab Version 9.13.x unterstützt FP21xx zwei ASA-Modi:

- Appliance
- Plattform

Im Einheitenmodus gibt es keine Chassis-Benutzeroberfläche. Im Plattformmodus ist eine Chassis-Benutzeroberfläche vorhanden, die Lizenz wird jedoch über die ASA CLI oder ASDM konfiguriert.
Andererseits muss auf FPR4100/9300-Plattformen die Lizenz in FCM über GUI oder FXOS CLI konfiguriert werden, und ASA-Berechtigungen müssen von ASA CLI oder ASDM angefordert werden.
Referenzen:

- Lizenzmanagement für die ASA
- Logische Geräte für die Firepower 4100/9300
- Lizenzen: Smart Software-Lizenzierung (ASAv, ASA mit Firepower)
- Bereitstellung im ASA-Plattformmodus mit ASDM und FirePOWER Chassis Manager

Wie können Sie eine Strong Encryption-Lizenz aktivieren?
Diese Funktion wird automatisch aktiviert, wenn für das in der FCM-Registrierung verwendete Token die Option "Ausfuhrkontrollierte Funktionen für die mit diesem Token registrierten Produkte zulassen" aktiviert war.

Wie können Sie eine Strong Encryption-Lizenz aktivieren, wenn die export-gesteuerten Funktionen auf FCM- und die zugehörige Encryption-3DES-AES auf ASA-Ebene deaktiviert sind?
Wenn diese Option für das Token nicht aktiviert ist, heben Sie die Registrierung des FCM auf, und registrieren Sie ihn erneut mit einem Token, für das diese Option aktiviert ist.

Was können Sie tun, wenn beim Generieren des Tokens die Option Exportgesteuerte Funktionalität für die mit diesem Token registrierten Produkte zulassen nicht verfügbar ist?
Wenden Sie sich an Ihr Cisco Account Team.

Muss die Funktion Strong Encryption auf ASA-Ebene konfiguriert werden?

Die Option für starke Verschlüsselung ist nur erforderlich, wenn FCM in einen Satelliten-Server vor 2.3.0 integriert ist. Dies ist nur ein Szenario, in dem Sie diese Funktion konfigurieren müssen.

Welche IPs müssen im Pfad zwischen dem FCM und der Smart Licensing Cloud zulässig sein?
Der FXOS verwendet die Adresse https://tools.cisco.com/ (Port 443) für die Kommunikation mit der Lizenz-Cloud. Die Adresse https://tools.cisco.com/ lautet wie folgt:

- 72.163.4.38
- 173.37.145.8

Warum tritt bei Ihnen der Fehler "Out of Compliance" auf?
In folgenden Fällen kann die Compliance des Geräts aufgehoben werden:

- Überlastung (das Gerät verwendet nicht verfügbare Lizenzen)
- Lizenzablauf - Eine zeitlich begrenzte Lizenz ist abgelaufen.
- Mangel an Kommunikation: Das Gerät kann die Lizenzierungsbehörde nicht erreichen, um eine erneute Autorisierung durchzuführen.

Um zu überprüfen, ob sich Ihr Konto im Status "Out-of-Compliance" befindet oder sich diesem Status nähert, müssen Sie die derzeit von Ihrem FirePOWER-Chassis verwendeten Berechtigungen mit denen in Ihrem Smart Account vergleichen.
In einem nicht konformen Zustand können Sie Konfigurationsänderungen an Funktionen vornehmen, für die spezielle Lizenzen erforderlich sind, ansonsten wird der Betrieb nicht beeinträchtigt. So werden z. B. bereits vorhandene Kontexte mit Standardlizenzlimits weiterhin ausgeführt, und Sie können ihre Konfiguration ändern, Sie können jedoch keinen neuen Kontext hinzufügen.

Warum tritt nach dem Hinzufügen von Lizenzen immer noch der Fehler "Out of compliance" (Out-of-Compliance) auf?
Standardmäßig kommuniziert das Gerät alle 30 Tage mit der Lizenzbehörde, um die Berechtigungen zu überprüfen. Wenn Sie die manuelle Auslösung durchführen möchten, gehen Sie wie folgt vor:

Bei FPR1000/2100-Plattformen muss dies über ASDM oder CLI erfolgen:

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

Bei FPR4100/9300-Plattformen muss dies über die FXOS-CLI erfolgen:

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

Warum wird auf ASA-Ebene keine Lizenz verwendet?
Stellen Sie sicher, dass die ASA-Berechtigung auf ASA-Ebene konfiguriert wurde. Beispiel:

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

Warum werden Lizenzen auch nach der Konfiguration einer ASA-Berechtigung immer noch nicht verwendet?
Dieser Status wird erwartet, wenn Sie ein ASA Active/Standby-Failover-Paar bereitgestellt und die Lizenznutzung auf dem Standby-Gerät überprüft haben.
Wie im Konfigurationsleitfaden beschrieben, wird die Konfiguration auf das Standby-Gerät repliziert, das die Konfiguration jedoch nicht verwendet. Es verbleibt im gecachten Zustand. Nur die aktive Einheit fordert die Lizenzen vom Server an. Die Lizenzen werden in einer einzelnen Failover-Lizenz zusammengefasst, die vom Failover-Paar gemeinsam genutzt wird. Diese zusammengefasste Lizenz wird auch auf der Standby-Einheit zwischengespeichert, um verwendet zu werden, wenn sie in Zukunft zur aktiven Einheit wird. Referenz: Failover- oder ASA-Cluster-Lizenzen.

Was können Sie tun, wenn FCM keinen Zugang zum Internet hat?
Alternativ können Sie Cisco Smart Software Manager On-Prem (ehemals Cisco Smart Software Manager Satellite) bereitstellen. Dies ist eine Komponente von Cisco Smart Licensing, die mit Cisco Smart Software Manager zusammenarbeitet. Sie bietet nahezu Echtzeittransparenz und Reporting-Funktionen für die Cisco Lizenzen, die Sie erwerben und verbrauchen. Außerdem erhalten sicherheitskritische Organisationen die Möglichkeit, zur Verwaltung ihrer vorhandenen Installationen auf einen Teil der Cisco SSM-Funktionen zuzugreifen, ohne eine direkte Internetverbindung nutzen zu müssen.

Wo finden Sie weitere Informationen zu Cisco Smart Software Manager On-Prem?
Diese Informationen finden Sie im FXOS-Konfigurationshandbuch:

- Konfigurieren eines Smart License Satellite Servers für das Firepower 4100/9300 Chassis
- Konfigurieren der FirePOWER Chassis Manager-Registrierung für einen Smart Software Manager vor Ort

Zugehörige Informationen

- Konfigurationsleitfaden für die allgemeine CLI der Cisco ASA-Serie
- Lizenzmanagement für die ASA
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.